## Inhaltsverzeichnis

## Vorwort

Wissen nimmt in der heutigen „Wissensgesellschaft“ einen immer bedeutenderen Stellenwert ein. Gleichzeitig vervielfältigt sich das vorhandene „Wissensgut“ innerhalb von immer kürzer werdenden Perioden. Dadurch wird einerseits eine stetig wachsende Wissensflut ausgelöst, andererseits wird relevantes Wissen jedoch nicht mehr effizient gefunden. Eine Folge davon ist, dass entweder bereits vorhandenes Wissen erneut erzeugt wird oder unverhältnismäßig viel Zeit in die Suche nach relevantem Wissen investiert wird.

An der Landesverteidigungsakademie nehmen die Angehörigen der Abteilung Zentraldokumentation, vorwiegend im Referat „Wissensmanagement“ seit dem Jahr 2008, die Herausforderung, nach einem dem „state of the art“ entsprechenden Lösungsansatz zu suchen, an. In zahlreichen Projekten, insbesondere im Rahmen des österreichischen Sicherheitsforschungsprogramms KIRAS, haben sie ihre ausgezeichnete Kompetenz unter Beweis gestellt und sind sehr begehrte Kooperationspartner, sowohl von Seiten der Universitäten wie auch von führenden Forschungseinrichtungen. In Verbindung mit dem Fokus auf Anwendbarkeit der Forschungsergebnisse ist eine Vielzahl an Unternehmen an der Zusammenarbeit nicht nur interessiert, sondern auch sehr dankbar für die teils einzigartigen erbrachten Leistungen. Viele KIRAS Forschungsprojekte wären ohne die Beteiligung und das hohe Know how der Abteilung Zentraldokumentation gar nicht entstanden; eine *Avantgarde* Rolle kann durchaus bestätigt werden.

Im eigenen Haus, der Landesverteidigungsakademie und anderen Bildungseinrichtungen des ÖBH wird das Prinzip der „forschungsgeleiteten Lehre“ so oft wie möglich und im Fokus der jeweiligen Studiengänge und Fachveranstaltungen umgesetzt. Zusätzlich wird die vorhandene Kompetenz auch direkt bei den Streitkräften im ÖBH immer mehr genutzt, ganz im Sinne der oben erwähnten Eigenheiten von Wissensnutzung im Sinne einer ökonomisch sinnvollen Anwendung.

Der vorliegende Sammelband gibt für den interessierten Leser einen ausgezeichneten Über- und Einblick in die vorgestellten Projektergebnisse. Für die Herausgeber und Autoren soll damit einhergehend ein Ansporn zur

Vertiefung ihrer Kenntnisse und für weitere wichtige Forschungsprojekte gegeben sein. Wissen in den Bildungseinrichtungen wie der Landesverteidigungsakademie wird generiert, vermehrt und begründet und soll darüber hinaus der beruflichen Befähigung, also der Umsetzung des Wissens in praktische Fähig- und Fertigkeiten dienen.

Im Sinne des vom Vorsitzenden des Österreichischen Wissenschaftsrates, Univ. Prof. Dr. Jürgen Mittelstraß, formulierten Wissenschafts- und Forschungsimperativs *„Lass Dich leiten von der Lust auf das Neue und dem Willen zu erkennen, was die Welt im Innersten zusammenhält, aber achte darauf, dass es kein minderes Ziel ist, die Welt mit dem, was Du forschend und entwickelnd tust, zusammenzuhalten!"* darf ich die Hoffnung aussprechen, dass die Lust an neuen Vorhaben und Projekten noch lange nicht gestillt ist und weitere interessante Ergebnisse von den Autoren folgen werden.

***Mag. Klemens Hofmeister, Bgdr***
***Leiter der Abteilung „Wissenschaft, Forschung und Entwicklung"***
***im BMLVS***

## Abstract

Der vorliegende Band beschäftigt sich mit wissenschaftlichen Ergebnissen und Beiträgen aus verschiedenen internen, aber auch externen Forschungsprojekten wie beispielsweise Ergebnissen aus der KIRAS-Forschungslandschaft unter Beteiligung der Zentraldokumentation und insbesondere des Referats Wissensmanagement an der Landesverteidigungsakadamie. Die wissenschaftlichen Papers wurden bei zahlreichen internationalen Konferenzen im Zeitraum 2009-2104 eingereicht, peer-reviewed und präsentiert.

## Abstract

This publication presents scientific papers, which were peer-reviewed and presented on several international conferences from 2009 to 2014. It is based on the results of the scientific work in the Central Documentation – particularly the Section of Knowledge Management – of the National Defence Academy, which is research partner in numerous internal and external research projects and member of the KIRAS Research Program.

# European Meetings on Cybernetics and Systems Research

## EMCSR 2014

*Civilisation at the Crossroads – Response and Responsibility of the Systems Sciences*
*http://www.emcsr.net*

University of Vienna, 22.04.-25.04.2014

Systems terminology has entered any field of society – everyday practice as well as research and development in the sciences, be it in natural, social or engineering sciences or in logics and mathematics or in philosophy. All of those sciences that revolve around systems shall, and do, contribute, in one way or another, more or less, to the thriving of civilisation. But how do they perform now that global challenges beset civilisation as never before? "Best practice" has to be redefined. That's the agenda of the EMCSR 2014.

### Bertalanffy Center for the Study of Systems Science (BCSSS)

The Bertalanffy Center for the Study of Systems Science (BCSSS) is an Austrian independent research institute, accredited by the European Union, inter-nationally acknowledged as an ambassador for the systems science heritage and present state-of-the-art applied systems research. The Bertalanffy Center for the Study of Systems Science focuses on Systems Theory and Systems Philosophy, exploring and explaining the world, and Systems Design, understanding and deploying change in this world. The objective of the BCSSS is to inspire the development of systems science by fostering systems research and supporting systems thinking. Given the global challenges of today, systems science is needed more than ever.

Bertalanffy Center for the Study of Systems Science
Paulanergasse 13
1040 Vienna
http://www.bcsss.org

The following peer-reviewed papers were published in the conference proceedings: J. Wolby, S. Blachfellner, W. Hofkirchner (Eds.), "Civilisation at the Crossroads, Response and Responsibility of the Systems Sciences", Book of Abstracts:

http://emcsr.net/wp-content/uploads/2014/04/BoA-EMCSR-2014.pdf

# Cross-Media Communication during Crises and Disasters

*Gerhard Backfried, Katja Prinz, Johannes Göllner, Christian Meurers, Gerald Quirchmayr, Gerald Czech*

**Abstract:** Traditional and social media are known to be of great benefit for crisis- and disaster communication. In this paper we argue for the combination of these different kinds of media in a cross-media, multi-media and multi-lingual approach, claiming that a combined view will yield superior results to individual media only. We emphasize the importance of analyzing cross-media links to provide valuable insights about the communication structure and -patterns occurring in different stages of a disaster. An approach implementing this combination is presented and the QuOIMA project addressing several of the issues is introduced. After describing the creation of a corpus covering several media in different languages reporting on the Central European floods of 2013, we conclude by presenting some preliminary experiments and findings.

**Keywords:** Multimedia, social media, natural disasters, crisis communication, knowledge development, critical infrastructure

**Acknowledgement:** This work is supported by the Austrian National Security Research Development Program KIRAS.

This extended abstract is available from http://emcsr.net/book-of-abstracts/


Bertalanffy Center for the Study of Systems Science http://www.bcsss.org

## 1 Introduction

Traditional media, such as TV, radio or print-media, have a long history of providing information about crises and disasters (C&D). Media organizations rapidly embraced the Internet as an additional channel for the distribution of information and content producing web-sites, news-feeds or online-media-archives. More recently, the same organizations have also entered the realm of social media platforms, adding yet another dimension to their portfolio of distribution channels. Whereas this diversification of media distribution was driven primarily by commercial aspects, the outcomes equally affect communication aspects during C&D. In spite of the proliferation of new distribution channels, traditional media might still provide the primary source of information for a substantial part of the population even today (depending on disaster type, language-related-, social-, technological- or geographical factors).

Recent years have witnessed a dramatic surge in coverage of C&D on social media platforms. This increase has been accompanied by the extended participation of organizations and individuals and the development and implementation of strategies on how to best combine technological advances with humanitarian and crisis-management objectives (Chan, 2013; International Federation of Red Cross and Red Crescent Societies, 2013). The benefits of using social media to gather, coordinate and disseminate information for supporting supply chains for critical infrastructure during C&D events and C&D management are widely acknowledged by experts as are potential challenges and risks (Antoniou and Ciaramicoli, 2013).

Social media, such as social networking platforms, micro-blogging or photo-sharing sites, interact with traditional media in various ways – as catalysts, sparking off initial coverage, providing different, additional and unfiltered angles or amplifying information – and together produce a broad spectrum of coverage. As examples have shown in the past, this mix of additional and complementary information can lead to substantially improved situational awareness for decision makers and planners and provide the affected public with crucial and transparent information (Kwang-Hoong and Mei-Li, 2012; Tyshchuk, Hui,, Grabowski, and Wallace, 2012).

Frequently, social media may be first to report on an event and play a time-critical role. In certain cases, they have even been found to be the only functioning communication medium (Acar and Muraki, 2011). On other occasions, professional TV stations or journalists may be the first ones to report. The exact role and relevance of media types differs from case to case and changes over time, requiring and prompting continuous research investigating the respective interplay. It is also notable that traditional and social media are increasingly being connected and inter-linked by news providers and individuals alike. Examples include professional journalists tweeting while on air, TV-programs providing links to Facebook accounts or live-discussions listing hashtags to streamline communication pertaining to their program.

Whereas much attention has been paid to the use of social media during C&D, little work has been carried out on the combination of different types of social media with each other and/or with traditional media. Incorporating the different angles and aspects should allow obtaining an even more complete, timely and diverse picture as events unfold. Clearly, the different media channels possess different qualities and advantages and their fusion should yield advantages over each individual one. Technically, this process has to be accompanied by the fusion of processing capabilities for different modalities (textual, audio and visual media) as well as multilingual processing. The latter is indispensable, especially in view of multicultural, international and cross-border C&D settings.

## 2 Existing Work

Social media are known to have played a major role in a series of disasters (Peary, Shaw and Takeuchi, 2012). The authors of (Backfried, Göllner, Quirchmayr, Rainer, Kienast, Thallinger, Schmidt, Pfeiffer, Meurers, Peer, 2013) provide an overview and findings on how different natural disasters have been covered and investigated with regard to media utilization. Relatively little attention has been paid to the actual use and differences of language, terminology and registers in the context of social media and natural disasters: (Mendoza, Poblete, and Castillo, 2010) and (Bryden, Funk and Jansen, 2013) deal with this topic to some extent. (Vieweg, 2012) provides detailed analyses for several disasters (predominantly within the US and in English only). Potential motivations and purposes of social media use have

been investigated and compiled by several studies such as (DHS, 2013) and (Peary et al., 2012). The latter also investigate how various types of media were relied upon during and following the 2011 Japan earthquake and find TV and social media to be on par.

Besides the research-projects in this area, actual use of social media for C&D management is already being practiced by an increasing number of organizations. The use of the @QPSMedia Twitter-account by the Queensland Police during the 2011 floods in Australia provides one of the first accounts of social media use for crisis communication (Bruns, Burgess, Crawford, and Shaw, 2012). The concertation of social media utilization by several US agencies during Hurricane Sandy might signal a marked shift in the use of social media in disasters (DHS, 2013). The establishment of dedicated accounts such as Twitter's @EmergencyTweets and its recent addition of Twitter Alerts point in the same direction. Crisis mapping projects and communities based on crowd-sourcing and emerging technologies, such as Ushahidi, the CrisisMappers network or Google's Crisis Map complement these activities.

## 3 Gaps and Goals

Whereas previous research mostly focused on aspects of C&D communication within a single medium and a single channel only (typically Twitter), little work has been carried out on the investigation of cross-media communication and -patterns during such events. Consequently, individual corpora of data during incidents have been gathered for a single medium (typically a collection of tweets) and for a single language only (typically English). Subsequent processing is often limited to the same single language. On the one hand, these facts may have to do with the availability of media and the corresponding mobile input devices to the population and researchers. On the other hand, these phenomena may simply be due to technical limitations and the lack of processing capabilities for further languages. Furthermore, English has become the de facto lingua franca of social media and may be the natural choice for international participation.

Based on these observations and short-comings, we identify several key issues which merit further attention and investigation. Our interest lies in the communication and -patterns arising before, during and following a

disaster involving the full spectrum of media and diversity of languages and how to best link these to allow for effective and efficient crisis management and communication. In particular, we focus on the gathering of information with the aim of providing improved situational awareness to first responders, linking identified patterns to the different phases of a disaster and to different communities.

Cross-media: both, traditional media as well as social media will continue to play fundamental and complementary roles. Their respective strengths can be capitalized on by combining sources and channels from different media, creating added value and allowing for insights not obtainable by any individual medium alone. Links between different media and their patterns during different disaster stages are expected to yield additional valuable, insights.

Multi-media: multi-media in the form of images and video is becoming more common-place with the ubiquity of portable devices. Individuals carrying such devices will often be on-site, delivering visual content and meta-data associated with short comments swiftly rather than typing lengthy texts. As a consequence, multi-media data and sites storing and accumulating them are becoming more interesting to harvest and process for analysis, interpretation and linking of content. These kinds of media require processing capabilities such as visual processing or speech recognition reaching beyond the purely textual ones often present in today's systems.

Multi-lingual: crises and disasters often take place in multi-national, cross-border, multi-lingual and multi-cultural settings. As a consequence, media in different languages need to be collected and processed. Social media and meta-data created by the crowd can be multi-lingual and include jargon from different domains, linguistic styles and registers. These factors add additional requirements to the technologies and models involved, such as robustness to deviations from (perceived) standards. Outbound communication likewise has to take this diversity of languages and styles into consideration.

Multi-environment: the vocabulary and language-style (or register) used during C&D is likely to differ substantially across the different types of media. Specific, technical terminology and every-day language may overlap

or be misused unintentionally. Messages may be phrased in different manners depending on the medium and are likely to require corresponding phrasing for outbound communication. These differences all require different kinds and levels of processing and robustness of technologies.

## 4 Method and Experiments

The QuOIMA project addressing some of the key issues identified above was launched in November of 2012. In particular, it deals with the use of open-source information and the combination of social and traditional media in the context of natural disasters based on a specific 5-phase disaster model (Backfried, Schmidt, Quirchmayr, Rainer, Kienast, Thallinger, Göllner and Peer, 2013). In collaboration with a first-responder, the Central European Floods of 2013 were selected as the first use-case. However, further data-collection will continue throughout the project duration. Emphasis is placed on cross-media communication and -patterns occurring at different stages of a disaster. Textual processing, audio-processing and visual-processing are combined; an underlying multi-lingual ontology is employed to allow for cross-lingual processing. The architecture is based on the Sail Labs Media Mining System designed for real-time processing of open-sources which will be extended with several technologies and components. Individual components, such as the speech recognition engine are built in a way to make them re-usable in a straight-forward manner regardless of the actual version of the framework. Components, technologies and models will be extended step-by-step according to the findings obtained from analysis of the corpus. This process is envisioned to be performed multiple times, each time integrating existing insights and gathering further data resulting from these insights. The project has a duration of two years, allowing for repeated collection and extension of data-sets.

### *4.1 Corpus creation*

To allow for the analysis of cross-media communication patterns, a parallel corpus spanning various types of media, sources and languages all pertaining to a single event is required. To this end, a corpus covering the 2013 Central European Floods on various types of media has been created. Data-sources and amounts collected are listed in Table 1. The corpus spans the period from 05/20/2013 to 06/23/2013 representing the period caus-

ing the worst floods in 500 years for some of the affected areas in Central Europe (Wikipedia). This first version of the corpus allows examining cross-media/multi-media effects. Further extensions will be addressed in the 2nd round of data collection in 2014. The final goal is to have data available in multiple-languages for all media and modalities covering an event.

| Medium | Amount | Comment |
|---|---|---|
| TV | 218h | 13 TV programs, 9 TV stations, 4 countries, German and English, general and specific news programs |
| Internet (Web) | 3500 | 102 sources, German, English |
| Twitter | 470k tweets | German (mostly) English and Dutch |
| Facebook | 9800 posts / comments | posts and comments from 16 public pages, German and English, involving more than 1000 users |
| Press Agency | 750 | Press-releases, German only |

Table 1: Cross Media Corpus

*4.2 Initial Insights*

Following the first phase of corpus collection, an initial, quantitative evaluation has been taking place, yielding the following preliminary insights:

- Floods were taking place in the South of Germany and in Austria and, with a slight delay, in the East and North of Germany. Both of these regions generate data in German which can only be distinguished by geo-location of items occurring in the text. Direct geo-location is only possible for a subset of the corpus – in line with previous findings, only about 1% of all tweets can be geo-located.
- Internet, Twitter, Facebook and TV coverage of the floods display similar behavior with peaking activity from June 2nd to June 4th and one-day delays between peaks in the order: tweets, TV, Facebook and Internet.
- Two peaks, corresponding to the floods hitting Southern Germany

and Austria and – a few days later – the East of Germany, can be distinguished.

- URLs embedded in tweets do indeed link to other types of media as shown in Figure 2. These are some of the cross-media links identified as meriting further research in our work.

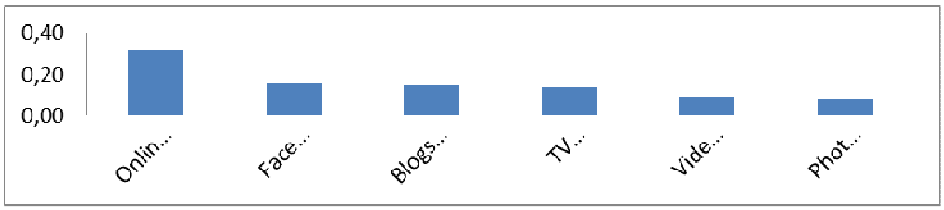



Figure 1: URLs mentioned in tweets by destination type

Downloading and processing the content of the destination documents provides further promising leads for future work employing visual processing technologies. NGOs and first-responders as well as government agencies are conspicuously absent from the set of links. This may be due to their limited participation in the social and new media field during disasters or by the simple lack of visibility of such activities.

A particular finding for Austria is that most public communication on Facebook indeed took place on a private account rather than any account associated with first responders or NGAs. More than 2/3 of all Facebook posts and comments collected were issued on this single account. Upon request by the Austrian Red Cross (personal communication), the FB page's owner refused to cooperate. This puts communication and intervention by first responders and government agencies into a new perspective(further communication on public Facebook-pages corresponded to first responders and media).

Bots may account for a large proportion of flood-related tweets. Automatic bot-detection was implemented as outlined in (Chu, Gianvecchio, Wang and Jajodia, 2012) and shows that approximately 1% of users can be classified as bots. These bots are among the most active users and account for 22% of all flood-related tweets. The type of tweets generated by bots can mostly be classified as noise but may also contain actionable information,

e.g. by providing water-levels at specific locations in 15-minute intervals.

## 5 Conclusion & Outlook

An approach based on the pillars of cross-media, multi-media and multi-lingual processing of diverse data originating from a combination of traditional and social media was motivated and outlined. The project QuOIMA is a first step in the direction of implementing aspects of this framework and establishing a parallel corpus spanning these different media types. Investigation of cross-media links has started yielding some promising preliminary results. The corpus will be extended in a second round of data-gathering, broadening its scope to further languages and extended content. Technologies and components will be integrated into an open-source information system, allowing for rapid deployment. Patterns and links to disaster phases and factors of resilience will be explored in the next phase of the project.

## References


- Acar, A, and Muraki, Y., (2011) Twitter for crisis communication: lessons learned from Japan's tsunami disaster, Int. Journal Web Based Communities, Vol. 7, No. 3, 2011
- Antoniou, N.,and Ciaramicoli, M., (2013) Social Media in the Disaster Cycle – Useful Tools or Mass Distraction, 64th International Astronautical Congress, Beijing, China
- Backfried G., Schmidt C., Quirchmayr G., Rainer K., Kienast G., Thallinger G., Göllner J. and Peer A., (2013) Integration of Media Sources for Situation Analysis in the Different Stages of Disaster Management
- EISIC 2013, European Intelligence and Security Informatics Conference, Uppsala, Sweden
- Backfried, G., Göllner, J., Quirchmayr, G., Rainer, K., Kienast, G., Thallinger, G., Schmidt, C., Pfeiffer, M., Meurers, C., Peer, A., (2013) Cross-Media Analysis for Communication during Natural Disasters, International Conference on Advances in Information Technology, IAIT 2013, Bangkok, Thailand
- Bruns, A., Burgess, J., Crawford, K. and Shaw, F., (2012) #qld-

floods and @QPSMedia: Crisis Communication on Twitter in the 2011 South East Queensland Floods, 2012, Brisbane: ARC Centre of Excellence for Creative Industries and Innovation
- Bryden, J., Funk, S. and Jansen, V., (2013) Word usage mirrors community structure in the online social network Twitter, EPJ Data Science
- Chan, J.C., The Role of Social Media in Crisis Preparedness, Response and Recovery, VANGUARD Report, http://bit.ly/191xdTk on 2013/12/27
- Chu, Z., Gianvecchio, S., Wang, H., and Jajodia, S., (2012) Detecting Automation of Twitter Accounts: Are You a Human, Bot or Cyborg?, IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. X
- DHS, First Responders Group and Virtual Social Media Working Group, Lessons Learned: Social Media and Hurricane Sandy, June 2013
- International Federation of Red Cross and Red Crescent Societies, World Disasters Report 2013
- Kwang-Hoong, L. and Mei-Li, L. (2012) The Fukushima nuclear crisis reemphasizes the need for improved risk communication and better use of social media, Health Physics 103 (3): 307-310
- Mendoza, M., Poblete, B., and Castillo, C., (2010) Twitter Under Crisis: Can we trust what we RT?, SOMA 2010, Washington D.C., USA
- Peary, B., Shaw, R. and Takeuchi, Y., (2012) Utilization of Social Media in the East Japan Earthquake and Tsunami and its Effectiveness, Journal of Natural Disaster Science, Volume 34, Number 1, 2012, pp3-18
- Tyshchuk, Y., Hui, C., Grabowski, M and Wallace, W.A., (2012) Social Media & Warning Response Impacts in Extreme Events: Results from a Naturally Occuring Experiment. 2012 45th International Conference on System Science (HICSS): 818.
- Vieweg, S., (2012), Situational Awareness in Mass Emergency: A Behavioral and Linguistic Analysis of Microblogged Communication, Ph.D. Thesis
- Wikipedia, http://en.wikipedia.org/wiki/2013_European_floods, on 2014/01/02

**Authors**

**Gerhard Backfried** holds a position as head of research at SAIL Labs and is currently part of the core speech recognition engine and toolkit team. His technical expertise includes acoustic and language modelling as well as speech recognition algorithms. More recently he has been focussing on the combination of traditional and social media in the scope of disaster-communication. He holds a degree in computer science (M.Sc.) from the Technical University of Vienna with specialty Artificial Intelligence and Linguistics and is a Ph.D. candidate at the University of Vienna. He has authored several papers and has been contributing to national and international research projects, like CIMWOS, KIRAS/MDL, KIRAS/QuOIMA, M-ECO, VIRTUOSO or iTalk2Learn.

**Katja Prinz** holds a position as Marketing Manager at SAIL LABS. Her main areas of expertise include Strategic Marketing, Communications and Public Relations. She holds a degree in Marketing and Trade from the Vienna University of Economics and Business. She has been contributing to several FP7 and security research projects, like KIRAS/MDL, M-ECO, VIRTUOSO and KIRAS/QUOIMA. As a PhD candidate at Sigmund Freud University, she is specializing in security research and resilience.

**Johannes Göllner, MSc MSc**
Is Head of the Section Knowledge Management of the Department of Central Documentation and Information Service at the National Defence Academy of the Federal Ministry of Defence and Sports, Vienna, since 2011; his research areas and consulting foci include Knowledge Management & -Development, Trend- & Risk Analysis and Scenario Planning & Development, since 2009; former positions include Chairmanship of the Steering Committee of ON Committee 246 "Risk-, Security & Crisis Management" at the Austrian Standards Institute (2003-2008) and national delegate at ISO and CEN, Researcher and Lecturer assignments Risk-, Crisis-, Security Management, Critical Infrastructure and Head of the Section Risk Management and Course Director of the Master of Business Administration (MBA)-Programm "Environmental Threats and Disaster Management" and staff officer at the NBC-Defence School of the AAF and Lecturer assignments at the University of Natural Resources and Life Sciences Vienna and University of Vienna, since 1999; has been further Senior Re-

searcher & Deputy Leader-experience in kind of Inhouse Consultant of the EU-Research-Project "FOCUS-Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenuos EU Roles", 2009-2012.

**Christian Meurers, MSc**
Christian Meurers, MSc, is desk officer in the Multimedia Documentation and Situation Awareness Center and is responsible for multimedia documentation and the administration of the Situation Awareness Center at the Central Documentation at the National Defence Academy of the Ferderal Ministry of Defence and Sports. He graduated in computer sciences at the University of Technology in Vienna and intensively deals with the topics cyber-war, information war, technology and society. He worked for ITP Consulting, the EDVg and the University of Technology in Vienna and has been at the National Defence Academy since 2009, where he has been involved in a number of projects, i.a. KIRAS MDL, KIRAS QuOIMA or KIRAS (SG²), KIRAS MetaRisk, KIRAS LMK-MuSE etc.

**Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr**
Gerald Quirchmayr holds doctors degrees in computer science and law from Johannes Kepler University in Linz (Austria) and currently is Professor at the Department of Distributed and Multimedia Systems at the University of Vienna. In 2001/2002 he held a Chair in Computer and Information Systems at the University of South Australia, where he still holds an adjunct professorship. He first joined the University of Vienna in 1993 from the Institute of Computer Science at Johannes Kepler University in Linz (Austria) where he had previously been teaching.
His major research focus is on information systems in business and government with a special interest in security, applications, formal representations of decision-making and legal issues. His publication record comprises over 150 peer-reviewed papers plus several edited books and conference proceedings as well as nationally and internationally published project reports.

**Gerald Czech**
Gerald Czech is Head of New Media at Austrian Red Cross. He studied Chemistry and Socioeconomics in Vienna and is an senior emergency officer in Austrian Red Cross Disaster management and Civil Protection. He

is trained EU/CP-Expert and lecturer in Emergency Management and Communications.

# Meta Risk Model for Critical Infrastructures

*Christian Meurers, Johannes Göllner, Stefan Schauer, Stefan Schiebeck, Andreas Peer, Martin Stierle*

**Abstract:** In this article we provide an overview on state-of-art risk assessment methodologies and introduce a generic comprehensive approach for the development of a meta risk model, which is further used to build a sensor-driven risk analysis and risk management system. In the course of this, knowledge management as well as risk analysis and risk management disciplines (e.g. the Double Vector Model, meta heuristics, etc.) and their respective application in the strategic and operative context of ICT and critical infrastructures are evaluated and integrated into a meta risk model to guarantee the feature-based organizational development, governance and controlling on an operative level.

**Keywords:** Risk Management, Risk Assessment, Risk Analysis, Decision Support, Heuristics, Critical Infrastructures

**Acknowledgement:** This research is supported by the Austrian Research Promotion Agency (FFG), grant number 840905, within the KIRAS security research program by the Federal Ministry for Transport, Innovation and Technology. The contents of this paper represent the results of the current project work and the submitted proposal (KIRAS 2012).

## 1 Intention & Domain

A comprehensive risk management is the foundation of all management, core and support processes in an organization. Based on a knowledge management system, it represents the background of all measures regarding the feature-based organizational development, governance and controlling. In particular, in the security-relevant area a special emphasis is laid on risk management on a strategic and operative level due to the sensitive tasks and challenges in this area.

There are numerous guidelines and methodologies towards risk assessment and risk management throughout various fields of application (cf. ISO 31000, ISO 31010, ISO 27005, ISO 28000). This includes sectors like the IT security, the telecommunication sector or the financial sector. Nevertheless, the risk management systems used in these sectors are highly domain specific and only valid as long as the assumptions, on which these systems are built, do not change. This includes even well-established approaches like the Business Continuity Framework of the Bank of Japan (Bank of Japan, 2014). Often, these approaches focus on financial risks or IT risks but do not take other influence factors into account. Such an approach might have a huge impact if the respective assumptions it is based on change, as seen in the case of the tsunami in Fukushima, where a total blackout of the power supply was not considered at all.

The intention of the work and the focal point of the underlying R&E project "MetaRisk" is the development of a comprehensive meta risk model based on a generic approach to describe organizational structures and the interconnection between them as well as to increase the quality of scenario development covering potential threats. To achieve that several risk management approaches from different sectors (IT security, financial, logistics, etc.) are evaluated and combined to define the meta risk model.

## 2 State of the Art

It is a common practice to use a well-established risk model from one domain and apply it to other domains than the original one, without considering the adaption of the model due to the different situation in the new domain. This "copy and paste" application of risk models often results in the use of terms from financial risk or IT risk in a new context, which they are not designed for.

In principle, choosing the right method or the right tool to perform risk analysis, risk assessment and risk management turns out to be rather complicated. In this context, a set of concepts, algorithms and tools has been developed over the last few years, which are specifically designed to protect the IT infrastructure and related systems. Based on their historical background in economics, these methods often provide a quantitative approach to risk assessment in terms of monetary values (cf. (Peltier 2001), (Schechter 2004) and the EBIOS method as well as the ISO 27005 standard). Hence, most of the tools and methodologies (cf. (ENISA 2010) for an extensive list of examples) only support the common rule "risk = potential damage x probability of the respective event". Further, depending on the applied methodology, the terms and scales for the assessment of the potential damage and the probability of the respective event are fixed (cf. for example the NIST directives (Stoneburner, Coguen and Feringa 2002) or the MEHARI method (CMC 2004)). Therefore, the selection of a specific tool or method for risk assessment and risk management is often based on practical considerations and depends on how far the present terminology of the application can be mapped on the specific terminology of the respective risk assessment methodology.

In order to structure the process, there already exist various attempts to develop ontologies for generic risk assessments (Kollartis, Wergles, Siegel et al. 2008). For example, the AURUM system (Ekelhart, Fenz S. and Neubauer 2009) provides a graphical tool to build models based on ontologies, using a Bayesian approach for determining threat probabilities. The OCTAVE method (Alberts and Dorofee 2002) is based on subjectively estimated probabilities and can thus be understood as an a priori distribution in the Bayesian approach. It represents a comprehensive collection of

tools and best practice methods for risk management in the field of IT-security.

Although there is a lack of a comprehensive risk assessment and risk management model, most of the models and approaches mentioned above can be reduced to an abstract level and serve as basics for the development of the meta risk model. The challenge of designing and modeling is not only the specification of the generic level but also the granularity of the derivation of the analyzed risk models and approaches in order to guarantee the integration of all relevant factors, processes and methodologies into the meta risk model as well as the suitability for different fields of application.

## 3 Further Work

The topics presented in this article concentrate on the development of a sensor-based risk analysis and risk management system using a comprehensive approach for a generic meta risk model. The aim of the conducting project is not only to model and design the system based on this meta risk model but is also to implement a respective software demonstrator for decision support. In the course of this, results from previous research (Schiebeck 2007, Schiebeck 2013) as well as methodologies, techniques and technologies are integrated into the meta risk model. Furthermore, existing scenario modeling techniques (Pillkahn 2007), classification systems (Göllner, Meurers, Peer et. al. 2014), systems engineering (Göllner, Meurers, Peer et. al. 2010) as well as developed processes, control logics and risk models are combined in the system. To define the correlations between the key performance indicators (KPI) and key risk indicators (KRI), basic sensors, interfaces of analytical instruments (e.g. SNA, Social Network Analysis (Göllner, Meurers, Peer 2011), KIRAS-MDL, etc.) as well as expert knowledge are discussed, formalized and mapped to the system and furthermore integrated into a software demonstrator.

The generic approach and the underlying meta risk model guarantees the possible usage of the system for different domains like supply chain networks, energy sector, finance market etc. and the integration of all relevant knowledge, methods, processes and sensors.

## References


- Alberts, C. J. and Dorofee, A., (2002) "Managing Information Security Risks: The Octave Approach", Addison-Wesley Longman Publishing Co., Inc.
- Bank of Japan (2014) "Business Continuity Planning at the Bank of Japan", http://www.boj.or.jp/en/about/bcp/, last visited 03/2014
- Clusif Methods Commission, (2004) "MEHARI V3 Risk Analysis Guide".
- Dworschak, R., Leitner, A., and Pöttinger, J. (2008), „Evaluierung von Risikoanalysetools", FH-Hagenberg
- Ekelhart, A., Fenz S. and Neubauer, T., (2009)„„Automated Risk and Utility Management," in Proceedings of the Sixth International Conference on Information Technology: New Generations, IEEE Computer Society, pp. 393-398.
- European Network and Information Security Agency, 2010, „Inventory of Risk Management / Risk Assessment Methods,", Available: rm-inv.enisa.europa.eu/rm_ra_methods.html.
- Göllner, J., Meurers, C., Peer, A. et.al. (2010), "Wissensmanagement im ÖBH. Systemdefinition, -beschreibung und –begrenzung zur Szenarioentwicklung und –modellierung. Teil 1: Allgemeine Systemdefinition und Systembeschreibung" in ["Schriftenreihe der Landesverteidigungsakademie 12/2010"], Reprozentrum Wien
- Göllner, J., Meurers, C., Peer, A. [et.al.], (2011) "Wissensmanagement im ÖBH. Systemdefinition, -beschreibung und –begrenzung zur Szenarioentwicklung und –modellierung.:Einführung in die Soziale Netzwerkanalyse und exemplarische Anwendungen " in ["Schriftenreihe der Landesverteidigungsakademie 5/2011/S"], Reprozentrum Wien
- Göllner J., Meurers C., Peer A., Langer, L., Kammerstetter; M.; (2014) „Bedeutung des Risikomanagements für die Sicherheit von Smart Grids", 13. Symposium Energieinnovation, 12.02.-14.02. 2014, Graz
- Kollarits, S., Wergles, N, Siegel H. et al., (2008) „MONITOR - An ontological basis for risk management," Available: http://www.monitor-cadses.org.

- International Standardization Organization, (2011), "ISO 27005: Information security risk management," Geneva, Switzerland
- International Standardization Organization, (2007), "ISO 28000: Specification for security management systems for the supplay chain," Geneva, Switzerland
- International Standardization Organization, (2009), "ISO 31000: Risk Management – Principles and Guidelines", Geneva, Switzerland
- International Standardization Organization, (2009), "ISO 31010: Risk management -- Risk assessment techniques", Geneva, Switzerland
- Peltier, T. R., (2001), "Information security risk analysis", Auerbach Publications
- Pillkahn, (2007), „Trends und Szenarien als Werkzeuge zur Strategieentwicklung"
- Schechter, S. E. (2004), „Computer security strength and risk: a quantitative approach," Harvard University
- Schiebeck, S., (2007), „IT-Risikomanagement – Anforderungen, Vorschriften und Toolevaluierung", Masterthesis, FH Hagenberg
- Schiebeck, S., (2013), „Continuous Information Security Risk Assessment focused on Security Measurements", Forschungsbericht FFG 819952, Universität Wien.
- Stoneburner, G., Goguen, A. and Feringa, A., (2002) „Special Publication 800-30: Risk Management Guide for Information Technology Systems", National Institute of Standards and Technology.

## Authors

**Christian Meurers, MSc**

Christian Meurers, MSc, is desk officer in the Multimedia Documentation and Situation Awareness Center and is responsible for multimedia documentation and the administration of the Situation Awareness Center at the Central Documentation at the National Defence Academy of the Ferderal Ministry of Defence and Sports. He graduated in computer sciences at the University of Technology in Vienna and intensively deals with the topics cyber-war, information war, technology and society. He worked for ITP Consult-

ing, the EDVg and the University of Technology in Vienna and has been at the National Defence Academy since 2009, where he has been involved in a number of projects, i.a. KIRAS MDL, KIRAS QuOIMA or KIRAS (SG²), KIRAS MetaRisk, KIRAS LMK-MuSE etc.

**Johannes Göllner, MSc MSc**
Is Head of the Section Knowledge Management of the Department of Central Documentation and Information Service at the National Defence Academy of the Federal Ministry of Defence and Sports, Vienna, since 2011; his research areas and consulting foci include Knowledge Management & -Development, Trend- & Risk Analysis and Scenario Planning & Development, since 2009; former positions include Chairmanship of the Steering Committee of ON Committee 246 "Risk-, Security & Crisis Management" at the Austrian Standards Institute (2003-2008) and national delegate at ISO and CEN, Researcher and Lecturer assignments Risk-, Crisis-, Security Management, Critical Infrastructure and Head of the Section Risk Management and Course Director of the Master of Business Administration (MBA)-Programm "Environmental Threats and Disaster Management" and staff officer at the NBC-Defence School of the AAF and Lecturer assignments at the University of Natural Resources and Life Sciences Vienna and University of Vienna, since 1999; has been further Senior Researcher & Deputy Leader-experience in kind of Inhouse Consultant of the EU-Research-Project "FOCUS-Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenuos EU Roles", 2009-2012.

**Dipl.-Ing. Dr. Stefan Schauer**
Stefan Schauer is an experienced "Risk Management"-researcher in AIT's the field of risk management at the AIT Austrian Institute of Technology GmbH (Safety & Security Department.). He studied Computer Science at the University of Klagenfurt and received his PhD in Theoretical Physics, working on Quantum Cryptography, at the Technical University Vienna. Since 2005 he is working for the AIT in several projects related to the fields of classical security and risk management. Currently, his main focus lies in the field of risk

management and risk assessment as well as security architectures for critical infrastructures. In this context he is interested in risk assessment using game theoretic approaches and the identification and handling of threats coming from the human factor. He has experience leading medium-sized national research projects funded by the FFG as well as other research promotion agencies.

**Stefan Schiebeck, MSc**
Stefan Schiebeck, MSc is expert on information security and risk management and a scientific researcher at the AIT Austrian Institute of Technology GmbH. While his work focuses on organizational security topics like GRC (governance, risk & compliance), including implementation and audit of information security management systems, he also led and performed many technical security audits using the black box and white box approach, as well as multiple security architecture and concept reviews. During his work he became Certified Ethical Hacker, accredited ISO 27001 Lead and Internal Auditor as well as Certified Risk Manager. From 2007 to 2013 he was employed as Chief Information Security Officer, Internal Auditor and senior security consultant at SEC Consult GmbH. His research interests include many aspects of organizational and technical information security, with strong focus on risk assessment and management. His previous experiences in the context of this project concern a master thesis on the subject of risk management in collaboration with the Federal Ministry of Defence, as well as a subsequent, funded doctoral thesis on the subject of risk, performance indicators and knowledge management (RiskSense, FFG 819952).

**Andreas Peer, MA, MA**
Is a member of the section Knowledge Management of the Department of Central Documentation and Information Service at the National Defence Academy of the Federal Ministry of Defence and Sports in Vienna. He is an expert for risk and crisis management and also knowledge and scenario development. In 2004 he absolved the military academy and became an professional officer and the MA in "military leadership", 2006. Andreas Peer was a participant of the Master of Business Administration "Environmental Threats

and Disaster Management". From 2007 to 2011 he was commanding officer and responsible for the deployment of an NBC-defence company. Experience got Andreas Peer during various trainings and missions mostly after natural disasters, in Austria and abroad. He has further experience in kind of In-house Consultant of the EU-Research-Project "FOCUS-Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles", 2009-2012.

**DI Dr. Martin Stierle, MBA**
Is Head of the Business Unit Optical Quantum Technologies in AIT's Safety & Security Department. He studied Physics at the Technical University Vienna and received his PhD in Theoretical Physics. In addition, he finished the MBA of International Strategic Management at LIMAK. Between 1999 and 2009, he was Head of Network Planning and Network Infrastructure Wireline at Telekom Austria. Since 2010, he is responsible for technology management in the field of disruptive IT security technologies as well as in IT security consulting and risk management at AIT.

# Modelling simulation-based decision support in the last mile of crisis management

*Andreas Peer, Christian Fikar, Patrick Hirsch, Johannes Göllner, Manfred Gronalt, Gerald Quirchmayr*

**Abstract:** The research described in this paper focuses on the development of a cloud-based simulation and operations research toolkit which is integrated in the control information systems for tactical and operative planning support. It provides decision-makers with status reports as well as simulated scenarios and analyses of future developments. In combination with quantitative methods, this should contribute to improving the response to disasters and to providing better support to victims. Moreover, the usage of the toolkit in training helps to identify crucial skills required and can lead to a better understanding of relief processes, especially due to the focus on private and public coordination within this project.

**Keywords:** disaster management, crisis management, model-based simulation, decision support, cloud-based, operations research, interface problem

**Acknowledgement:** This research is supported by the Austrian national KIRAS programme since 2013, and is funded by the Federal Ministry for Transport, Innovation and Technology

This extended abstract is available from http://emcsr.net/book-of-abstracts/


Bertalanffy Center for the Study of Systems Science http://www.bcsss.org

## 1 Motivation

Disasters cause complex scenarios which require coordinated actions of various organisations[1] to reduce resulting damages and to support victims efficiently. Due to the involvement of multiple actors in the relief process, where actors differ in their missions and goals, coordination is essential; however, an efficient and effective coordination is difficult and time-consuming to achieve.[2] As the velocity of decision-making is crucial in such scenarios, a close cooperation between private and public organisations is necessary. In combination with the usage of decision-support tools to simulate and analyse the current situation and expected developments, these factors have a strong impact on the overall effectiveness of the response to disasters.

Due to damaged infrastructures and limited resources, last-mile distribution is especially challenging. Basic goods of daily life, such as food, have to be transported to the location of the disasters by private and public organisations in order to assure the stable operation of communities affected by disasters. The general situation in case of an disaster is shown in Figure 1.

1 Ministry of Interior: Coordination of crisis and disaster management, 2011, Vienna
2 Christensen: Assess your capabilities. Leadership Excellence, 2006

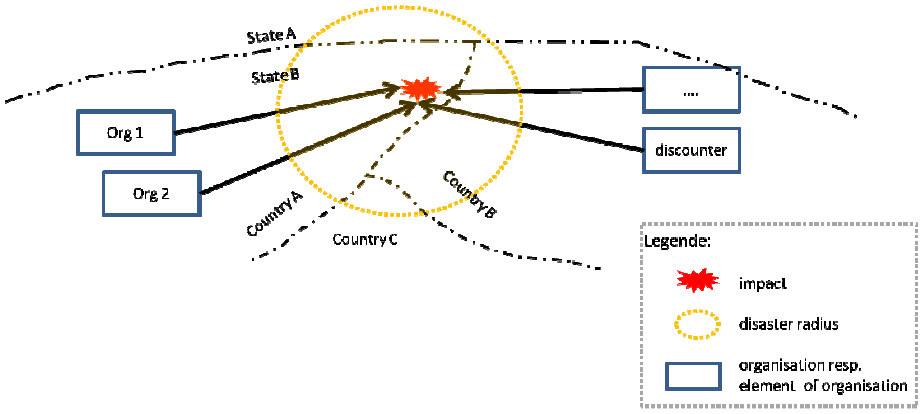



Figure 1: disaster situation[3]

A disaster occurs with or without advanced warning time. So the pre-execution phase may be long or very short. Figure 2 depicts a generic 5-phases model developed at the National Defence Academy of the Austrian MoD.

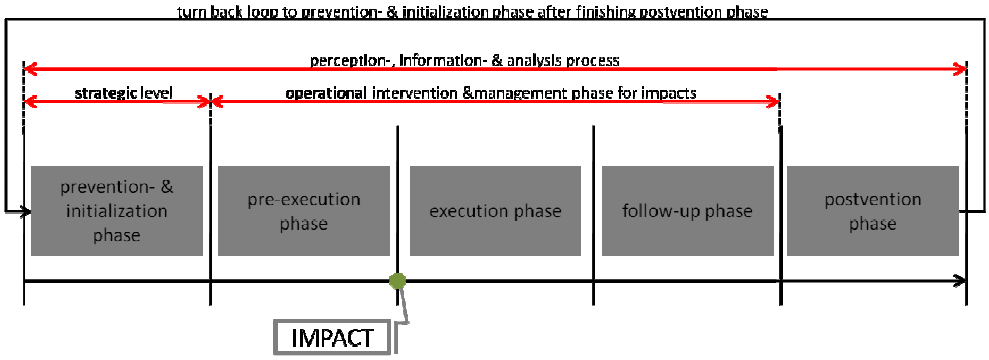



Figure 2: 5-phases disaster model[4]

[3] Born, Fikar, Gatarik, Göllner, Gronalt, Hirsch, Peer, Quirchmayr: Modelling simulation-based decision support in the last mile of crisis management, proposal LMK-MUSE, p. 17, 2013

[4] Backfried, Göllner, Quirchmayr, Rainer, Kienast, Thallinger, Schmidt, Pfeiffer, Meurers, Peer: Cross-Media Analysis for Communication during Natural Disasters, p.7, accepted paper, 2013

According to the above model, first responders or other actors face different challenges and requirements in crisis and disaster management depending on the management / leader-ship level (strategic, operational etc.) as well as the phases themselves.

## 2 Scope of the project

*„No single country is able to tackle today´s complex problems on its own.“*[5]

Within the scope of the research project "Modelling simulation-based decision support in the last mile of crisis management", a common terminology has to be defined to enable better coordinated processes. By development of a cloud-based simulation and operations research toolkit which is integrated in the control information systems for tactical planning support, optimized transshipment points and real-time schedules of relief shipments can be identified. This leads to a faster and more efficient disaster relief. The general interface problem is shown in Figure 3. This generic topic, referred to the "Doppelvektormodell"[6], applies to:

- personnel
- equipment
- facilities
- information and telecommunication systems
- action forces
- mobile vehicles and
- the legal compliance aspect.

[5] EU: European Security Strategy, A Secure Europe in a better World, p.1, Brussels, 2003

[6] Göllner, Meurers, Peer, Langer, Kammerstetter; Bedeutung des Risikomanagements für die Sicherheit von Smart Grids, accepted paper, 13. Symposium Energieinnovation am 12.-14. 2014, Graz

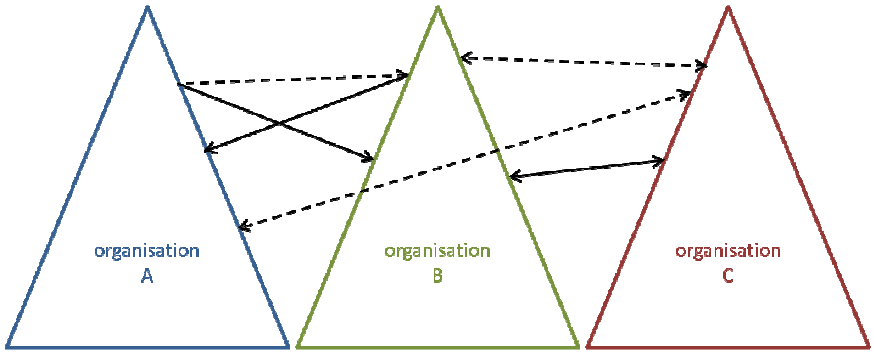



Figure 3: interface problem[7]

Furthermore, decision makers can be supported by a meaningful processing of available data and a detailed overview of the current situation. This is not only provided in a classic two-dimensional way, but three-dimensional, based on topographic features and additional external factors. Additionally, different scenarios can be simulated by an integrated agent-based simulation. By having better knowledge about potential developments, counter-measurements can be initiated and relief process adapted. By providing real-time information of available resources and their current (readiness) status in a common database to various actors, closer cooperation and more efficient mechanisms are facilitated.

[7] Berariu, Peer: Deliverable 4 – interface documentation, p.3, February, 2014

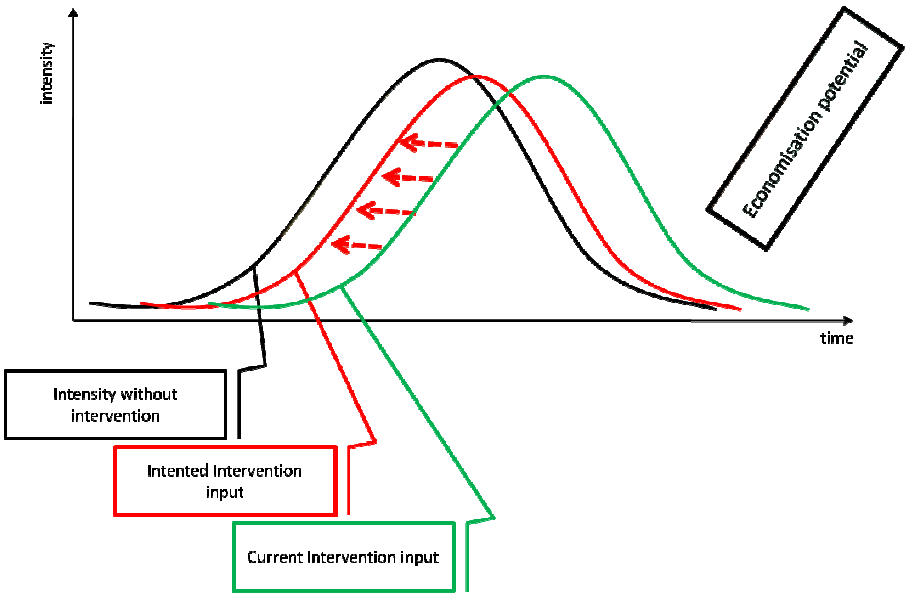



Figure 4: intented economisation potential[8]

As a result, decision-makers are provided with a powerful and integrated toolkit to react to disasters in a fast and efficient manner. Coordination between various actors is supported and various scenarios are considered. Moreover, the usage of the toolkit in training helps to identify crucial skills and can lead to a better understanding of disaster scenarios, their developments and efficient measurements to improve the quality of disaster relief in Austria and in transnational disaster relief efforts.

## References


- Backfried, Göllner, Quirchmayr, Rainer, Kienast, Thallinger, Schmidt, Pfeiffer, Meurers, Peer: Cross-Media Analysis for Communication during Natural Disasters, accepted paper, 2013
- Berariu, Peer: Deliverable 4 – interface documentation, February, 2014


[8] Born, Fikar, Gatarik, Göllner, Gronalt, Hirsch, Peer, Quirchmayr: Modelling simulation-based decision support in the last mile of crisis management, proposal LMK-MUSE, p. 26, 2013

- Christensen: Assess your capabilities. Leadership Excellence, 2006
- EU: European Security Strategy, A Secure Europe in a better World, Brussels, 2003
- Born, Fikar, Gatarik, Göllner, Gronalt, Hirsch, Peer, Quirchmayr: Modelling simulation-based decision support in the last mile of crisis management, proposal LMK-MUSE, 2013
- Göllner, Meurers, Peer, Langer, Kammerstetter; Bedeutung des Risikomanagements für die Sicherheit von Smart Grids, accepted paper, 13. Symposium Energieinnovation am 12.-14. 2014, Graz
- Ministry of Interior: Coordination of crisis and disaster management, 2011, Vienna

**Authors**

**Andreas Peer, MA, MA**
Is a member of the section Knowledge Management of the Department of Central Documentation and Information Service at the National Defence Academy of the Austrian Armed Forces in Vienna. He is an expert for risk and crisis management and also knowledge and scenario development. In 2004 he absolved the military academy and became an professional officer and the MA in "military leadership", 2006. Andreas Peer was a participant of the Master of Business Administration "Environmental Threats and Disaster Management". From 2007 to 2011 he was commanding officer and responsible for the deployment of an NBC-defence company. Experience got Andreas Peer during various trainings and missions mostly after natural disasters, in Austria and abroad. He has further experience in kind of In-house Consultant of the EU-Research-Project "FOCUS-Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles", 2009-2012.

**Christian Fikar, MSc**
Is a research assistant at the Institute of Production and Logistics, University of Natural Resources and Life Sciences, Vienna, Austria. He holds a master degree in supply chain management from Vienna University of Economics and Business, Austria. The main focus of his research is on humanitarian logistics and meta-/matheuristics in the context of innovative and sustainable transport concepts. Currently, he is working on his doctoral

thesis in this field.

**Ass.Prof. Ing. Mag. Dr. Patrick Hirsch**
Is an assistant professor, project manager and vice head of the Institute of Production Economics and Logistics at the University of Natural Resources and Life Sciences Vienna. He is reviewer for several international scientific journals and associate editor of the Journal of Applied Operational Research. His research interests are within transportation logistics, health care logistics and disaster management. He presented his work at several international conferences and published some book chapters as well as scientific journal articles. For his doctoral thesis in the field of timber transport he received two awards.

**Johannes Göllner, MSc MSc**
Is Head of the Section Knowledge Management of the Department of Central Documentation and Information Service at the National Defence Academy of the Austrian Armed Forces, Vienna, since 2011; his research areas and consulting foci include Knowledge Management & -Development, Trend- & Risk Analysis and Scenario Planning & Development, since 1999; is Chairman of the Steering Committee of ON Workshop 1144 "Knowledge Management" at the Austrian Standards Institute, since 2009; former positions include Chairmanship of the Steering Committee of ON Committee 246 "Risk-, Security & Crisis Management" at the Austrian Standards Institute (2003-2008) and national delegate at ISO and CEN, Researcher and Lecturer assignments Risk-, Crisis-, Security Management, Critical Infrastructure and Head of the Section Risk Management and Course Director of the Master of Business Administration (MBA)-Programm "Environmental Threats and Disaster Management" and staff officer at the NBC-Defence School of the AAF and Lecturer assignments at the University of Natural Resources and Life Sciences Vienna and University of Vienna, since 1999; is or has been further Senior Researcher & Deputy Leader-experience in kind of Inhouse Consultant of the EU-Research-Project "FOCUS-Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenuos EU Roles", 2009-2012.

**Univ.Prof. Mag.rer.soc.oec. Dr.rer.soc.oec Manfred Gronalt**
Prof. Gronalt has been a full professor at Boku University Vienna since

2002 and is head of the institute of production economics and logistics. His expertise and research interests comprise simulation based optimization, traffic and logistics research and operations management. He is also member of the Austrian Society for Operations Research and the EURO working group on Agriculture and Forest management and he chairs the working group (5.04.13) on industrial engineering, operations analysis and logistics within IUFRO.
Research at the institute is mainly centered on the topics:

- BioEnergy, Forest based industries and Transportation Logistics,
- Advanced planning in process industries,
- Mobile Health Services and
- Intermodal transport and Traffic systems.

For the research on simulation and capacity analysis of Binnenland Container terminal the Institute was honored with the Austrian State Award for green logistics in 2007.
Prof. Gronalt was member of the department steering comitte from 2004 – 2009 and also member of the university council. He is also member of the executive board of the Austrian Institute for Sustainability and with the german association of logistics (BVL) he is academic member of the jury for awarding the sustainability price 2013 and 2014.

**Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr**
Gerald Quirchmayr holds doctors degrees in computer science and law from Johannes Kepler University in Linz (Austria) and currently is Professor at the Department of Distributed and Multimedia Systems at the University of Vienna. In 2001/2002 he held a Chair in Computer and Information Systems at the University of South Australia, where he still holds an adjunct profesorship. He first joined the University of Vienna in 1993 from the Institute of Computer Science at Johannes Kepler University in Linz (Austria) where he had previously been teaching.
His major research focus is on information systems in business and government with a special interest in security, applications, formal representations of decision-making and legal issues. His publication record comprises over 150 peer-reviewed papers plus several edited books and conference proceedings as well as nationally and internationally published project reports.

# Importance of Risk Management for the Security of Smart Grids[1]

*Lucie Langer, Johannes Göllner, Christian Meurers, Andreas Peer, Markus Kammerstetter, Thomas Bleier*

**Abstract:** Future energy grids will make extensive use of the integration of ICT technologies. Thus, cyber security risks become a threat even for energy suppliers. Numerous security issues are completely unsolved today, because these special environments require novel security mechanisms and processes. The aim of the project (SG)² is therefore a systematic study of smart grid technologies in terms of ICT security issues and the research of countermeasures. Based on a thorough threat and risk analysis from a national perspective and specific security analysis of Smart Grid components, (SG)² explores measures for power grid operators that serve to increase the security of computer systems deployed in the future critical infrastructure of "energy".

**Keywords:** Smart Grids, Security, Risk Management, Energy, Vulnerability, Critical Infrastructure

**Acknowledgement:** This research is supported by the Austrian Research Promotion Agency (FFG) within the KIRAS security research program by the Federal Ministry for Transport, Innovation and Technology.

This extended abstract is available from http://emcsr.net/book-of-abstracts/


[1] The contents of this paper were published for the 13th Symposium for Energy Innovation 2014 (Göllner, Meurers, Peer, Langer, Kammerstetter 2014).

## 1 Existing Approaches

State-of-the-Art Risk Models like the "ISO 27000 Standards" and "IT-Grundschutzkataloge" of the German Federal Office for Information Security (BSI) and the integration of results and different approaches out of several research projects build the foundation of the work on risk models for the security of smart grids. Therefore it is necessary to categorize events and incidents following a categorisation system like the "double vector model" (Göllner, Meurers, Peer, Langer, Kammerstetter 2014), which was developed, evaluated and enhanced in the context of the research project „Szenarioplanung und Wissensmanagement im ÖBH" of the Federal Ministry of Defence and Sports. With this model it is possible to document and provide relevant content concering events and incidents for further analysis and allows the differentiation of events by factors referring the

- organization
- causers/initiators
- type of the event
- timely framework
- dimension/influence and the
- abstractional level.

Every incident or event can be categorized, documented and be related to actors and knowledge role models to recognize correlations and dependencies in order to provide information to analysts or to identify additional demands for information.

## 2 The $(SG)^2$ Risk Catalogue

The purpose of the research project $(SG)^2$ was to develop a risk catalogue for Smart Grid Operators in Austria to support enterprises in the energy supply sector in a comprehensive risk analysis of their systems. Based on the developed high-level reference architecture (*Smart Grid Architecture Model*) of CEN-CENELEC-ETSI (CEN-CENELEC-ETSI, 2012) a ICT-architecture model for Austrian Smart Grids was defined and integrated into a risk catalogue. After linking components and connections of the reference architecture to specified domains (i.e network, metering, enery

production facilities) threats and vulnerabilites were identified following the basic approaches (IT-Grundschutzkataloge, BSI-Schutzprofile) (BSI 2013a, BSI 2013b, BSI 2013c).

These threats were summarized, categorized and mapped to the specific context of Smart Grids producing a list of 31 threats, which were evaluated and reviewed within the scope of the underlying ICT-architecture model. In the next step the risk potential for each threat was determined representing the probability of occurrence and the possible damage. Energy Suppliers can use this list, the $(SG)^2$ Risk Catalogue and the visualization of the risk potential of possible threats for a concrete risk analysis within their implemented systems.

## 3 Evaluation

The ongoing transformation of energy networks to Smart Grids and the following integration of ICT multiply the need for an evaluation and assessment of emerging risks to identify and enable an improved protection of critical infrastructure sectors. However, a risk assessment requires a detailed view on the system landscape of energy suppliers. The often existing lack of risk assessment including the complete architecture confronts energy suppliers and network carriers with the need for proper risk management methods in the field of Smart Grids.

Contrary to analyzed existing methods within the EURACOM FP7 Project (FP7, 2013), the $(SG)^2$-Risk Catalogue follows a comprehensive approach considering the overall architecture and allows the combination of an architectural risk assessment with a detailed, individual risk evaluation in order to identify risk potential and probabilities of occurrence.

## References


- Göllner J., Meurers C., Peer A., Langer L., Kammerstetter M.; (2014) „Bedeutung des Risikomanagements für die Sicherheit von Smart Grids“, 13. Symposium Energieinnovation, 12.02.-14.02. 2014, Graz
- CEN-CENELEC-ETSI, (2012), Smart Grid Coordination Group:

Smart Grid Reference Architecture, Document for the M/490 Mandate, Version 3.0
- BSI, Bundesamt für Sicherheit in der Informationstechnik, (2013a) BSI-Standards 100-1 bis 100-4, 2008, aktuelle Version erhältlich unter https://www.bsi.bund.de/
- BSI, Bundesamt für Sicherheit in der Informationstechnik, (2013b), Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen (BSI-CC-PP-0073), Version 1.2
- BSI, Bundesamt für Sicherheit in der Informationstechnik, (2013c), Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen (BSI-CC-PP-0077), Version 1.0
- FP7 project EURACOM, (2013), URL: http://www.eos-eu.com/?Page=euracom

## Authors

**Lucie Langer**

Dr. Lucie Langer (CISSP) has been with the Safety & Security Department of AIT Austrian Institute of Technology since 2012. She is currently responsible for applied research projects on IT security aspects of critical infrastructures and smart grids, and coordinates the project "Smart Grid Security Guidance – (SG)2".

Before joining AIT she has been working as a Technology Consultant in the private sector for two years, focusing on access rights and infrastructure management in large-scale IT projects. From 2006 to 2010 she was a Research Assistant with the Cryptography & Computer Algebra Group at Technische Universität (TU) Darmstadt, and participated in several security-related research projects, including a security assessment of the German Electronic Identity Card. She received her PhD in 2010 from the Computer Science Department of TU Darmstadt for a dissertation on privacy and verifiability issues of electronic voting systems, and holds a master's degree in Mathematics from TU Darmstadt (2006) and Darmstadt University of Applied Sciences (2004).

**Johannes Göllner, MSc MSc**
Is Head of the Section Knowledge Management of the Department of Central Documentation and Information Service at the National Defence Academy of the Federal Ministry of Defence and Sports, Vienna, since 2011; his research areas and consulting foci include Knowledge Management & -Development, Trend- & Risk Analysis and Scenario Planning & Development, since 2009; former positions include Chairmanship of the Steering Committee of ON Committee 246 "Risk-, Security & Crisis Management" at the Austrian Standards Institute (2003-2008) and national delegate at ISO and CEN, Researcher and Lecturer assignments Risk-, Crisis-, Security Management, Critical Infrastructure and Head of the Section Risk Management and Course Director of the Master of Business Administration (MBA)-Programm "Environmental Threats and Disaster Management" and staff officer at the NBC-Defence School of the AAF and Lecturer assignments at the University of Natural Resources and Life Sciences Vienna and University of Vienna, since 1999; has been further Senior Researcher & Deputy Leader-experience in kind of Inhouse Consultant of the EU-Research-Project "FOCUS-Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenuos EU Roles", 2009-2012.

**Christian Meurers, MSc**
Christian Meurers, MSc, is desk officer in the Multimedia Documentation and Situation Awareness Center and is responsible for multimedia documentation and the administration of the Situation Awareness Center at the Central Documentation at the National Defence Academy of the Ferderal Ministry of Defence and Sports. He graduated in computer sciences at the University of Technology in Vienna and intensively deals with the topics cyber-war, information war, technology and society. He worked for ITP Consulting, the EDVg and the University of Technology in Vienna and has been at the National Defence Academy since 2009, where he has been involved in a number of projects, i.a. KIRAS MDL, KIRAS QuOIMA or KIRAS (SG²), KIRAS MetaRisk, KIRAS LMK-MuSE etc.

**Andreas Peer, MA, MA**
Is a member of the section Knowledge Management of the Department of Central Documentation and Information Service at the National Defence Academy of the Federal Ministry of Defence and Sports in Vienna. He is

an expert for risk and crisis management and also knowledge and scenario development. In 2004 he absolved the military academy and became an professional officer and the MA in "military leadership", 2006. Andreas Peer was a participant of the Master of Business Administration "Environmental Threats and Disaster Management". From 2007 to 2011 he was commanding officer and responsible for the deployment of an NBC-defence company. Experience got Andreas Peer during various trainings and missions mostly after natural disasters, in Austria and abroad. He has further experience in kind of In-house Consultant of the EU-Research-Project "FOCUS-Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles", 2009-2012.

**Markus Kammerstetter**
Markus Kammerstetter is currently working as research assistant, PhD candidate and head of Hardware Security Lab at the Vienna University of Technology, Institute of Computer Aided Automation, Automation Systems Group, International Secure Systems Lab. In the course of his bachelor and master studies "Computer Engineering" and "Computer and Network Security" as well as his ongoing PhD studies, he gained profound knowledge in the fields of Smart Grid security, Soft-and Hardware security, Embedded System security, reverse-engineering and cryptography. Since 2011, he has been actively teaching "Internet Security" and "Advanced Internet Security" at Vienna University of Technology. Besides, he was involved in the FFG funded projects TRUDIE, SeCoverer and several privately funded research projects. Currently, he is working in the field of Smart Grid security through the FFG funded KIRAS project Smart Grid Security Guidance $(SG)^2$. Regarding professional activities, Markus Kammerstetter worked as independent security consultant in the finance sector, since 2005, and acts as director of a Hard- and Software security firm, since 2013. His main research interests include critical infrastructure security, Soft- and Hardware security as well as Embedded System security and high speed cryptography.

**Thomas Bleier**
DI Thomas Bleier, MSc is the program manager for the "ICT Security" research programme at the AIT Austrian Institute of Technology GmbH, Austrias largest non-university research organization. The research programme is focusing on applied research of ICT security aspects in distrib-

uted systems to improve the security of critical infrastructures. Current research interests include secure system design, national cyber defense, secure cloud computing, and security aspects of next generation energy networks (smart grids).
Before joining AIT Thomas Bleier was working in the industry for more than 10 years as a Systems Architect, Project Manager, Software Developer and Technical Consultant. He holds a master's degree in Information Security Management, and a master's degree in Computer Science. Thomas Bleier is a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Ethical Hacker (CEH), Certified Project Manager (IPMA Level C), Certified SCRUM Master, and also holds several technical certifications.

# Evaluation criteria for cloud computing based on the upcoming European data protection regulation

*Manfred Halper, Stefan Fenz, Johannes Göllner, Gerald Quirchmayr*

**Abstract:** The European Union released a proposal on the protection on individuals with regard to the processing of personal data and the free movement of such data. One goal of the Data protection Regulation is to form the statutory framework to facilitate the adoption of cloud technology by Small and Medium Enterprises and mitigate the risks stemming from introducing Cloud Computing Service Providers (CCSP) into their supply chain networks. The developed evaluation criteria stemming from the Regulation should help SMEs to assess CCSPs for compliance and their capability of handling modern security and privacy objectives.

**Keywords:** General Data Protection Regulation; Small and Medium Enterprises; Cloud, Security

**Acknowledgement:** This research is supported by the Austrian Research Promotion Agency (FFG) within the KIRAS security research program by the Federal Ministry for Transport, Innovation and Technology.

This extended abstract is available from http://emcsr.net/book-of-abstracts/


Bertalanffy Center for the Study of Systems Science http://www.bcsss.org

## 1 Introduction

Today cloud computing technology and its various fields of application have reached a momentum and like every other, rather young technology service, the adoption and integration of cloud computing in the existing supply chains faces different problems and risks for small and medium-sized businesses. The European Union has identified cloud computing as a major future technology in the Information- and Communications Technology (ICT) sector and aims at enabling the economy to faster adopt and facilitate cloud computing through all sectors. The utmost important regulation for this cause is the upcoming European Data protection Regulation, as for the moment only available as an evolved proposal.

Information has become one of our utmost important resources in most industry branches, data has become a very liquid good that can easily be transported across sites, cities and borders and this generates a complete new challenge for SME's using or providing cloud computing services. The motivation is to distil evaluation criteria out of the regulation and security guidelines from the European Union to create a framework for SMEs that help them adopting cloud computing in their IT assets in a secure way.

## 2 Results

The first step in the assessment of a CCSP is to identify who holds which role. Regarding the Regulation there are the roles of controller, processor and the joint controller. Each role has its own set of rights and duties therefore the SME has to identify the role of every partner in the supply chain and evaluate their level of compliance in accordance to their role.

The key component of any cloud service nearly always revolves around data. The Regulation gives insight on the different classes of data and how to evaluate the CCSP regarding his implementation of security and organizational measures to protect this data. Especially personal data – any information relating to the data subject – and sensitive data have to be protected to prevent unlawful use.

Another criterion is given by the need of documentation due to the heavy

impact on security. Documentation is important to demonstrate results that originate from selected security measures or controls and makes decisions traceable. In combination with the necessary authorization from the supervisory authority prior to the use of personal data and a detailed data impact assessment the Regulation establishes traceability in the relationship between SME and CCSP.

Every venture working with the personal data of data subjects (an identified natural person or a natural person who can be identified) has to establish procedures that enable the data subject to exercise his/her rights. Due to the new data centric business models the Regulation identifies the collection of personal data as a field that is in need of adjustment and therefore demands the provision of possibilities of rectification, erasure, access and objection for the data subject.

The Regulation also introduces the data protection officer that has to be established by every corporation that employs 250 people or more, that is a public authority or body, or if his core activity requires regular and systematic monitoring of data subjects. The data inspection officer has to be involved in all issues related to the protection of personal data and is responsible to keep the SME informed regarding his obligations to the regulation.

The regulation describes very precisely the circumstances under which data can be lawfully transferred to a third country or an international organization for further processing purposes and thereby reacts to the current uncontrolled cross border flow of data. It states four core scenarios that help to evaluate if a data transfer anywhere in the supply chain is legally.

Another criterion is the encouragement of codes of conduct that include commitments to fair and transparent data processing and to the lawful collection of data and a certification scheme that proves the proper application of the Regulation by the SME or CCSP. The development of certificates, certification mechanism, data protection seals and marks will help elevating the possibilities of the SME, to assess the level of data protection and compliance provided by the CCSP.

The European Union is well aware that especially the adoption of cloud technology by SMEs is a critical success factor to enable the cloud to reach

its full potential and therefore has identified cloud-specific Key Actions in the Europe 2020 plan. One action is to cut through the jungle of standards by identifying and counteracting typical risks and challenges like the Availability of services and data, the current lack of data classification mechanism, integrity issues, confidentiality concerns, regulatory compliance, reputability, lack of forensic readiness, loss of control, responsibility ambiguity, lack of liability, migration problems and lock-in.

Since cloud services have special requirements regarding security and privacy objectives the European Union Agency for Network and Information Security developed a guideline that aims beyond the traditional IT infrastructure and security requirements and developed standards that elevate security and privacy objectives that are regarded major in the field of cloud computing, this includes protection of data from unauthorized access, disclosure and modification, the insurance of isolation, service availability, appropriate security provisions for cloud applications, security of connections and networks, enforcement of privacy policies and incident prevention, detection and response.

Every listed criterion can be used by the SME to assess current or future cloud service providers in his supply chain. The criteria focus on the view of the European Union well aware that there are several nongovernmental guidelines in the field of secure cloud computing.

## 3 Conclusion

There is a major need of regulation in the information market and SMEs are waiting for the upcoming Regulation to align their business strategy appropriately. Nonetheless a firm and solid security strategy pose as a competitive advantage in the fast developing cloud service market. It is beyond all questions that a SME sooner or later has to add cloud services to its infrastructure to stay competitive but the SME can choose how he integrates this technology in his business model and thereby influences if it will be successful or end in disaster. Not every criterion applies to any scenario; the SME has to verify where the criterions are applicable and if they are enforce them. The aggregation of evaluation criteria stemming from the Regulation also helps cloud service providers by identifying criteria that are applicable to their business model and giving them a competitive edge by

implementing the regulatory criterions and thereby facilitating compliance, strengthen security and boosting customer confidence. Since the Regulation is still in progress the final version may change some details of the here presented criteria.

## References


- E. Union, "Regulation of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation)," 01 2012
- ENISA, "Cloud computing. benefits, risks and recommendations for information security," 11 2009.
- N. I. of Standards and Technology, "The NIST definition of cloud computing," 01 2011.
- E. Commission, "Unleashing the potential of cloud computing in Europe," 09 2012.
- E. T. S. Institute, "Cloud standards coordination," 11 2013.
- E. T. S. Institute, "Cloud cloud private-sector user recommendations," 11 2012.


## Authors


**Manfred Halper:** 2008 Bachelor degree in business informatics. Since 2007 working in administration/security of a service provider in the banking, big corporate sector.

**Dr. Stefan Fenz** (CISSP) is a researcher at Vienna University of Technology and SBA Research and founder of Xylem Technologies GmbH. From 2012 to 2015, Stefan is an appointed member of the European Network and Information Security Agency's (ENISA) Permanent Stakeholder Group. In 2010, Stefan worked as a visiting scholar at Stanford Center for Biomedical Informatics Research at Stanford University (USA). From 2008 to 2012, Stefan lectured on information security at Peking University (Beijing, China), Beijing Jiaotong University (Beijing, China), Konkuk University (Seoul, Korea) and University of Applied Sciences Technikum

Wien (Vienna, Austria). His primary research is on information security, with a secondary interest in semantic technologies and energy efficiency. Stefan received an MSc in software engineering & internet computing from Vienna University of Technology, an MSc in political science from University of Vienna, an MSc in business informatics from Vienna University of Technology, and a PhD in computer science from Vienna University of Technology. He is a member of the IFIP WG 11.1 – Information Security Management, the IEEE Systems, Man, and Cybernetics Society and ISC².

**Johannes Göllner, MSc MSc** Is Head of the Section Knowledge Management of the Department of Central Documentation and Information Service at the National Defence Academy of the Austrian Federal Ministry of Defence and Sport, Vienna, since 2011; his research areas and consulting foci include Knowledge Management & -Development, Trend- & Risk Analysis and Scenario Planning & Development, since 2009; former positions include Chairmanship of the Steering Committee of ON Committee 246 "Risk-, Security & Crisis Management" at the Austrian Standards Institute (2003-2008) and national delegate at ISO and CEN, Researcher and Lecturer assignments Risk-, Crisis-, Security Management, Critical Infrastructure and Head of the Section Risk Management and Course Director of the Master of Business Administration (MBA)-Programm "Environmental Threats and Disaster Management" and staff officer at the NBC-Defence School of the AAF and Lecturer assignments at the University of Natural Resources and Life Sciences Vienna and University of Vienna, since 1999; has been further Senior Researcher & Deputy Leader-experience in kind of Inhouse Consultant of the EU-Research-Project "FOCUS-Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenuos EU Roles", 2009-2012.

**Univ. Prof. DDr. Gerald Quirchmayr** holds doctors degrees in computer science and law from Johannes Kepler University in Linz (Austria) and currently is Professor at the Department of Distributed and Multimedia Systems at the University of Vienna. In 2001/2002 he held a Chair in Computer and Information Systems at the University of South Australia. He first joined the University

of Vienna in 1993 from the Institute of Computer Science at Johannes Kepler University in Linz (Austria) where he had previously been teaching. In 1989/1990 he taught at the University of Hamburg (Germany). His wide international experience ranges from the participation in international teaching and research projects, very often UN- and EU-based, several research stays at universities and research centres in the US, Asia and EU Member States to extensive teaching in EU staff exchange programs in the United Kingdom, Sweden, Finland, Germany, Spain, and Greece, as well as teaching stays in the Czech Republic and Poland. International teaching and specialist missions include UN-coordinated activities in Egypt, Russia and the Republic of Korea. He has served as a member of program committees of many international conferences, chaired several of them, has contributed as reviewer to scientific journals and has also served on editorial boards. He is a member of the Austrian and German computer societies and a member of IFIP working groups. For his contributions to the international IT community he was received the IFIP Silver Core Award in 1995. His major research focus is on information systems in business and government with a special interest in security, applications, formal representations of decision making and legal issues. His publication record comprises approximately 150 peer reviewed papers plus several edited books and conference proceedings as well as nationally and internationally published project reports. In July 2002 he was appointed as Adjunct Professor at the School of Computer and Information Science of the University of South Australia. From January 2005 until January December 2010 he headed the Department of Distributed and Multimedia Systems, Faculty of Computer Science, at the University of Vienna and served as Vice Dean of the Faculty of Computer Science from October 2008 until October 2010. Since January 2011 he serves as deputy head of the MIS group.

# Security Strategies towards Mutually Dependent Goals

*Stefan Rass, Stefan Schauer, Johannes Göllner, Andreas Peer*

**Abstract:** Quantitative risk management is a rarely used approach in enterprise security, as it relies on hard to obtain information, whose lack of accuracy or reliability is often inhibiting reasonable conclusions. In restricted cases, however, it is indeed possible to apply game-theoretic techniques to tackle very basic problems of data processing. In this article, we describe a game-theoretic approach to quantitative risk management concerning the security of data transmissions within an enterprise network. Essentially, we outline project efforts towards setting up communication channels similar to a virtual private network, using game-theory and avoiding conventional encryption and hence key-management. Since the latter is most prone to human error, game-theoretic techniques appear interesting and are subject of this article, since they reduce the extent of human responsibility while at the same time providing us with mathematically sound risk estimates.

**Keywords:** Risk Management; Game-Theory; Security

**Acknowledgement:** This research was supported by the Austrian Research Promotion Agency (FFG), under KIRAS research grant 836287.

This extended abstract is available from http://emcsr.net/book-of-abstracts/


Bertalanffy Center for the Study of Systems Science http://www.bcsss.org

## 1 Introduction

Risk management is a core duty of (enterprise) leadership. While qualitative approaches are mostly supported by best-practices and a vast amount of literature, qualitative risk assessment makes cost-benefit analysis somewhat difficult and subjective to a considerable extent. Related literature, such as the ISO standards, the Common Criteria or the guidelines published by the German Bundesamt für Sicherheit in der Informationstechnik (BSI), is an indispensable tool for risk (threat) analysis, yet little is said about how to handle risk in situations where the range of attacks, yet not the adversary's actions, can meaningfully be modeled. It follows that much effort is usually spent on gaining ideas of what the attacker actually intends in order to estimate the most likely spot for a concrete attack. However, taking an alternative view focusing on the best protection against possible damage can spare most of the modeling related to the attacker's behavior. For that sake, we simply assume the attacker's motivation to be causing the maximum possible damage in a system. While this certainly misjudges the attacker's real intentions, it nevertheless is a reasonable worst-case assumption that lets us derive countermeasures against which any possible scenario (within the range of known attack strategies) can cause only less harm than we predicted.

## 2 Secure Transmission as a Mathematical Game

More technically, security can be treated as a mathematical game, in which the prize is the value of secret information (or more generally, the damage that an attack would cause), and the winner is either the honest or evil player (but not both). To model the attacker's worst-case behavior, we define the situation as a zero-sum game, in which the revenue for the honest party and the attacker is the business value that is processed (exchanged over a perhaps partially hostile communication infrastructure, stored at a possibly untrusted location, etc.). This game-theoretic approach is not new, and has been proposed in various preliminary works on secure communication and general quantitative risk management (Alpcan & Başar 2010, Cavusoglu et al. 2008, Lye & Wing 2005). Along the course of the SERIMA project ("IT-Security Risk Management using Decision Theory", funded by the Austrian Research Promotion Agency FFG), the game-theoretic modeling

and analysis has been applied to the rudimentary problem of private communication between two peers in a partially distrusted network. The only assumption made in the game was the attacker having full control over a limited set of nodes in the network, while the system determined the optimal routing strategy to bypass the attacker with maximum probability $u(x,y)$, when $x$ is a transmission configuration and $y$ is an attack strategy. Game-theory allows us to randomly choose both parameters, so as to optimize the revenue for the honest parties, while simultaneously finding the optimal attack profiles. In theory, it could be shown that this enables arbitrarily secure (confidential) communication, provided that there is an (arbitrarily small) chance to circumvent the attacker, while allowing the enemy to be even mobile (it may conquer different parts of the network infrastructure at different times, yet the total range of the hostile area remains bounded at all times). Most importantly, this form of confidential transmission is not based on encryption, thus requires no management of public-keys or secrets for symmetric encryption.

Going one step further, the RSB project ("Risikomanagement für simultane Bedrohungen"; funded by the FFG as a successor project of SERIMA) extends the investigation towards taking more security goals into account. In detail, RSB defines security as comprising confidentiality, authenticity and availability, where the game takes multiple goals for the honest parties into account. While much of the theory used in SERIMA no longer holds in the multivariate case of RSB, the theory could nevertheless be reformulated in this generalized setting, with optimal defenses remaining computable even with respect to multiple inter-dependent security goals. As a neat feature, the modeling does take into account an implicit or hidden interplay between security goals, while it does not require any explicit modeling of such interdependencies. Consequently, even though risks may nontrivially depend on one another, the game-theoretic modeling spares us the need to understand or model such interplay.

More precisely, the RSB approach defines a separate individual indicator variable for each security goal, say confidentiality (captured by the probability function $u_1$), authenticity (captured by the probability function $u_2$), etc., and computes a defense strategy that enjoys two properties (Rass 2012):

1. For each security goal, the optimized indicator average $a$ lower

bounds the likelihood to be successful in the security goal that it refers to.

2. The obtained bounds cannot be uniformly improved by switching to another transmission configuration in the sense that any deviation from the optimal defense will eventually yield a worse than optimal performance in at least one aspect of security.

These two axioms capture the properties that the one-dimensional indicator (used in SERIMA) naturally enjoyed, and are therefore a sound generalization of game-theory to the treatment of multiple and interdependent security goals. As discussed in detail in the SERIMA project, it is easy to analyze a zero-sum competition between two players fighting for a single goal. In that case, it is easy to bound the payoff for the honest player who attempts to maximize his own good, while the enemy tries to minimize the outcome. However, in the multivariate case, we are forced to consider Pareto-optimal behavior instead, where we can only optimize a tradeoff between what is achievable, if we cannot optimize all aspects of interest individually. This makes the obtained defenses necessarily ambiguous, as well as the optimal attack strategies. The latter have a particularly interesting interpretation, as these show possible scenarios of worst-case incidents, alas, the identification of such is in no way exhausting. Nevertheless, fixing the defense against one scenario and running the analysis again will eventually dig up further threats against which further countermeasures can be installed. In this iterative fashion, game-theory helps to create a comprehensive defense by repeatedly playing the game (which is simulating optimal attacks) and deriving countermeasures from it.

Basically, any network provisioning is compatible with the game-theoretic modeling, provided that there are degrees of freedom that a sender of secret information can use to introduce randomness for an attacker. In our case, this network provisioning is based on source routing that can be done on OSI layers 2, 3 or even 7 (to gain maximal flexibility and ease of use). For secret transmission, we randomly switch paths to prevent a (static) attacker to eavesdrop on all parts of the message. By choosing a proper encoding, the missing parts of the message act like encryption keys, however, without requiring any explicit key-management. For authenticity, we apply a reputation-based technique (Rass & Schartner (2010)), that is, we let the sender attach a message authentication code, whose verification is up to

designated parties in the network, with whom the sender shares some secret knowledge (this application of symmetric cryptographic techniques is the only case where key-management is required).

## 3 Ongoing Works and Outlook

Open issues with the technique concern its applicability to other security goals like non-repudiation or anonymity. This is subject of follow-up research. Ongoing work concerns the evaluation of efficiency and scalability of the methods. While for SERIMA, we have been able to analyze and provision hierarchically structured networks (wide-area networks that connect smaller local area networks) of a total of 10.000 nodes (SERIMA Consortium 2012), similar benchmarks for the RSB method are not yet ready. To this end, we defined a virtual enterprise infrastructure, in which we will set up a demonstrator and run experiments. The testbed is a generic model of an international holding. This corporation with a pharmaceutical background employs more than 18.000 personnel and besides the headquarters there are 18 independent branches dislocated in all continents. Three product lines (tablets, liquids and crown caps) and distribution branches are part of the holding. Every organizational element is structured to identify the relevant internal (e.g. communication lines between offices) and external (e.g. relevant lines to distributers) gateways for the further testing. This hypothetical pharmaceutical corporation can easily be replaced by a consisting organization to switch from the laboratory situation into real situation. More importantly, the simulation testbed provides realistic communication scenarios and traffic loads, to evaluate the usability of the RSB techniques in a large-scale setting.

## References


- Alpcan, T. & Başar, T. (2010) *Network Security: A Decision and Game Theoretic Approach*, Cambridge University Press.
- Cavusoglu, H.; Raghunathan, S. & Yue, W. T. (2008) Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment, In: *J. of Management Inf. Sys.*, Vol. 25, (pp. 281-304).
- Lye, K.-W. & Wing, J. M. (2005) Game strategies in network security, In: *Int. J. of Inf. Sec.*, Vol. 4 (pp. 71-86)

- Rass, S. (2012). On Game-Theoretic Network Security Provisioning, In: *Journal of Network and Systems Management*, Vol. 21 (pp. 47-64), Springer
- Rass, S. & Schartner, P. (2010) Multipath Authentication without shared Secrets and with Applications in Quantum Networks, In: *Int. Conf. on Security and Management*, CSREA, 2010, 1, (pp. 111-115)
- SERIMA Consortium (2012) *Bericht über System-Verifikation*, Technical Report D-WP4.1.

**Authors**

**Dipl.-Ing. Dipl.-Ing. Dr. Stefan Rass**
Stefan Rass studied technical mathematics (with a focus on statistics), and computer science at the Klagenfurt University and graduated with a double degree in 2005. He gained a PhD degree in mathematics in 2009 for a dissertation about information-theoretic security. His research interests include (among others) general system security, complexity theory, decision theory, statistics and applied cryptography. His research activities cover new cryptographic primitives in the context of cloud computing, about which he co-authored a textbook published by ArtechHouse. Besides theoretical aspects of security, he is investigating design and analysis techniques for practical general (critical) security infrastructures, with the aid of game-theory, and provides consultancy services for the industry. He has been participating in EU projects, as well as several national research projects, and is currently a member of the system security research group at the Alpen-Adria Universität Klagenfurt, led by Prof. Dr. Patrick Horster.

**Dipl.-Ing. Dr. Stefan Schauer**
Stefan Schauer is an experienced researcher in the field of risk management at the AIT Austrian Institute of Technology GmbH (Safety & Security Department). He studied Computer Science at the University of Klagenfurt and received his PhD in Theoretical Physics, working on Quantum Cryptography, at the Technical University Vienna. Since 2005 he is working for the AIT in several projects related to the fields of classical security and risk management. Currently, his main focus lies in the field of risk management and risk assessment as well as security architectures for critical infrastructures. In this context he is interested in risk assessment using game theoret-

ic approaches and the identification and handling of threats coming from the human factor. He has experience leading medium-sized national research projects funded by the FFG as well as other research promotion agencies.

**Andreas Peer, MA, MA**
Is a member of the section Knowledge Management of the Department of Central Documentation and Information Service at the National Defence Academy of the Federal Ministry of Defence in Vienna. He is an expert for risk and crisis management and also knowledge and scenario development. In 2004 he absolved the military academy and became a professional officer and the MA in "military leadership", 2006. Andreas Peer was a participant of the Master of Business Administration "Environmental Threats and Disaster Management". From 2007 to 2011 he was commanding officer and responsible for the deployment of an NBC-defence company. Experience got Andreas Peer during various trainings and missions mostly after natural disasters, in Austria and abroad. He has further experience in kind of In-house Consultant of the EU-Research-Project "FOCUS-Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles", 2009-2012.

**Johannes Göllner, MSc MSc**
Is Head of the Section Knowledge Management of the Department of Central Documentation and Information Service at the National Defence Academy of the Federal Ministry of Defence, Vienna, since 2011; his research areas and consulting foci include Knowledge Management & -Development, Trend- & Risk Analysis and Scenario Planning & Development, since 2009; former positions include Chairmanship of the Steering Committee of ON Committee 246 "Risk-, Security & Crisis Management" at the Austrian Standards Institute (2003-2008) and national delegate at ISO and CEN, Researcher and Lecturer assignments Risk-, Crisis-, Security Management, Critical Infrastructure and Head of the Section Risk Management and Course Director of the Master of Business Administration (MBA)-Programm "Environmental Threats and Disaster Management" and staff officer at the NBC-Defence School of the AAF and Lecturer assignments at the University of Natural Resources and Life Sciences Vienna and University of Vienna, since 1999; has been further Senior Researcher & Deputy Leader-experience in kind of Inhouse Consultant of the EU-

Research-Project "FOCUS-Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenuos EU Roles", 2009-2012.

# Risk analysis for "Schutz 14"

*Andreas Peer, Johannes Göllner, Christian Haberfellner, Herbert Bauer*

**Abstract:** The internal research described in this paper focuses on the identification of a risk index for the critical infrastructure railroad in Tyrol. The result is used for the further planning and decision making process for the military training exercise "Schutz 14" in June 2014. The risk analysis was done in autumn 2013 from an expert team consist of members of the Military Command of the Tyrol and the National Defense Academy. The result of the research should be the basis for further researches[1] to handle the complexity of various critical infrastructures as a support for the ongoing decision making process.

**Keywords:** supply chain, railroad, risk analysis, decision support, critical infrastructure, risk index, system thinking, scenario development

**Acknowledgement:** This internal research was supported and funded by the Federal Ministry of Defense and Sports.

This extended abstract is available from http://emcsr.net/book-of-abstracts/


Bertalanffy Center for the Study of Systems Science http://www.bcsss.org



[1] Submitted proposal for the Austrian national KIRAS program in 2014

## 1 Motivation

In June 2014 takes a national military training place in Tyrol with the focus on protection of critical infrastructures with military and civil organizations and institutions. Beside the ongoing decision making, General Bauer, the Commanding Officer (CO) of the Military Command of the Tyrol and responsible for all territorial aspects, decided to start a parallel risk assessment of the railroad as one of the critical infrastructures in Tyrol. The risk analysis was done in autumn 2013 from members of the Military Command of the Tyrol and the Section for Knowledge Development in the Department of Central Documentation and Information from the National Defense Academy of the Federal Ministry of Defence and Sports.
The motivation was to identify a risk index for the railroad based on the generic "Doppelvektormodell"[2] which was developed at the Department of Central Documentation and Information in 2011 and the previous researches in the topic of critical infrastructure[3].

## 2 Process

The research followed the identified process which is shown in Figure 1.

---

[2] Göllner, Meurers, Peer, Langer, Kammerstetter; Bedeutung des Risikomanagements für die Sicherheit von Smart Grids, accepted paper, 13. Symposium Energieinnovation am 12.-14. 2014, Graz

[3] Göllner, Kienesberger, Peer, Schönbacher, Weiler, Wurzer: Analyse und Betrachtung von Kritischen Infrastrukturen; Wissensmanagement im ÖBH-Systemdefinition, -beschreibung und –begrenzung zur Szenarioentwicklung und –modellierung, Supplement im Rahmen der Reihe „Grundlagen zum Wissensmanagement im ÖBH", Schriftenreihe der Landesverteidigungsakademie, 2010, Wien

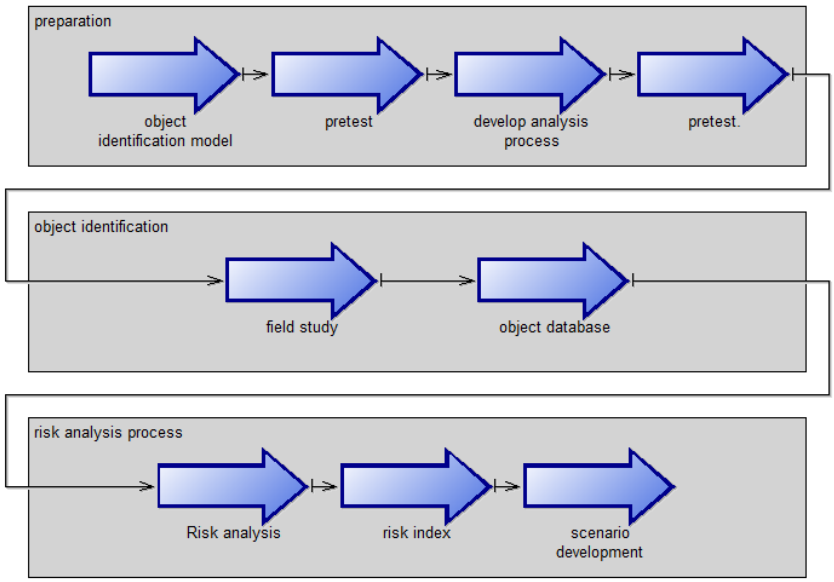



Figure 1: meta process[4]

During the preparation phase a model to categorize objects and other relevant parameters was generated and pretested on site. Also the further steps for the analyzing process were generated and tested in this phase.

In the object identification phase a team of at least two persons filled all objects and relevant parameter in prepared sheets. In another step the information of the field study were transmitted in specific database.
Referred to the "Doppelvektormodell" various models to attribute the identified parameters were generated in the risk analysis process phase. Of course the results of the singular models must be connected together to represent the complex situation of the evaluated system.[5] An abstract of one Model is shown in Figure 2.

[4] Created by Peer, Göllner, Haberfellner, 2013

[5] Göllner, Meurers, Peer, Povoden: Einführung in die Soziale Netzwerkanalyse und exemplarische Anwendung, Wissensmanagement im ÖBH-Systemdefinition, -beschreibung, und –begrenzung zur Szeanrioentwicklung und –modellierung, Supplement im Rahmen der Reihe „Grundlagen zum Wissensmanagement im ÖBH", Schriftenreihe der Landesverteidigungsakademie, 2011, Wien

| Hier sind die unterschiedlichen identifizierten Infrastrukturen/Objekte hinsichtlich der spezifischen Parameter (x-Achse) zu bewerten. | Kritisch !! | ÖBB | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Betriebsunterbrechung | | | | Ressourceneinsatz | | | | |
| | | keine | kurz | mittel | lang | keiner | gering | mittel | hoch | keine |
| Gewichtungsfaktor | | 25 | | | | 25 | | | | |
| Multiplikator | | 1 | 3 | 6 | 10 | 1 | 3 | 6 | 10 | 1 |
| Mauer | | 1 | | | | 1 | | | | |
| Unterführung | | 10 | | | | 3 | | | | |
| Nebengleise | | 1 | | | | 3 | | | | |

Figure 2: rating specific parameter (abstract)[6]

The necessary Models are generated like the identified objects attribute to identified parameters on the y-axis. An extract of these parameters on the y-axis were:

- Austrian Armed Forces (AAF)
  - resource management equipment
  - resource management personnel
- Austrian Federal Railway (ÖBB)
  - business interruption
  - resource management personnel/equipment
  - costs
- event orientation
  - technical threats
  - environmental threats
  - civil threats
  - legal compliance
  - political threats
  - socio-economic threats

These models were categorized in various layers and the last one is exactly characterized to allow the relation of an at least 4-step scale.

[6] Created by Peer, Göllner, 2013

The use of the "Doppelvektorenmodell" ensured that the analyzing steps were done under a widespread view to gaze at the independent influence. So for instance the effect of the general and the specific energy supply took influence as the impact of the identified threats on the different identified objects. For this the model connect the identified topics for

- event orientation,
- time orientation,
- organizational orientation,
- space orientation,
- trigger orientation and the
- level of abstraction orientation.

## 3 Aim/result of the research

In this research the critical objects were identificated specific for the distance scale and the two demand carriers, the Federal Ministry of Defence and Sports and the Austrian Federal Railway.

The most important result of the research was to create a risk index for, in this specific case, two demand carrier to support the decision making process for the preparation of the exercise "Schutz 14". Another result was to create demand carrier specific scenarios based on the risk analyzing process. So the comparison with existing results of further analysis was done as the comparison with the military analyzing process. Of course there was a lot of added relevant information like the risk index with combine the complex situation of one supply chain as critical infrastructure in the area of Tyrol.

As an example the identified critical objects in the evaluated system are visualized in maps for the planning process and the use for the various military and civil elements on site.

The generic risk analyzing process model can easily be used for other supply chains, supply chain networks or other demand carriers to indentify critical infrastructure elements or objects and of course the interdependent influence.

**References**


- Göllner, Meurers, Peer, Langer, Kammerstetter; Bedeutung des Risikomanagements für die Sicherheit von Smart Grids, accepted paper, 13. Symposium Energieinnovation am 12.-14. 2014, Graz
- Göllner, Meurers, Peer, Povoden: Einführung in die Soziale Netzwerkanalyse und exemplarische Anwendung, Wissensmanagement im ÖBH-Systemdefinition, -beschreibung, und –begrenzung zur Szeanrioentwicklung und –modellierung, Supplement im Rahmen der Reihe „Grundlagen zum Wissensmanagement im ÖBH", Schriftenreihe der Landesverteidigungsakademie, 2011, Wien, IS70-56-4
- Göllner, Kienesberger, Peer, Schönbacher, Weiler, Wurzer: Analyse und Betrachtung von Kritischen Infrastrukturen; Wissensmanagement im ÖBH-Systemdefinition, -beschreibung und –begrenzung zur Szenarioentwicklung und –modellierung, Supplement im Rahmen der Reihe „Grundlagen zum Wissensmanagement im ÖBH", Schriftenreihe der Landesverteidigungsakademie, 2010, Wien, ISBN: 978-3-902670-64-9
- Haberfellner, Ch. (2011): Leitlinien zur Stärkung der Wirtschaftskraft am Beispiel Eisacktal. Verlag Effekt. Nachhaltige Regionalentwicklung durch Innovation. Hrsg. Amt für Innovation (2009), Verlag Weger.
- Haberfellner, Ch. (2005): Erfolgsfaktoren im Clustermanagement. In: Kongress net'swork. Bielefeld.
- Haberfellner, Ch. (2005): Die Struktur der IT Branche in Südtirol und die Methode zur Clusterentwicklung. In: Succi, G., Hrsg., (2005 im Druck) Clusterentwicklung am Beispiel des Clusters Information Technology und Software Engineering. Mailand.
- Haberfellner, Ch. (1999) Leben an der Armutsgrenze. Alltag der kleinbäuerlichen Bevölkerung Kamwalas in Nordmalawi. Innsbruck, 1999. In: Innsbrucker Geographische Gesellschaft. Innsbrucker Jahresbericht 1997/1998. Innsbruck.

**Authors**

**Andreas Peer, MA, MA**
Is a member of the section Knowledge Management of the Department of Central Documentation and Information Service at the National Defence Academy of the Federal Ministry of Defence and Sports in Vienna. He is an expert for risk and crisis management and also knowledge and scenario development. In 2004 he absolved the military academy and became an professional officer and the MA in "military leadership", 2006. Andreas Peer was a participant of the Master of Business Administration "Environmental Threats and Disaster Management". From 2007 to 2011 he was commanding officer and responsible for the deployment of an NBC-defence company. Experience got Andreas Peer during various trainings and missions mostly after natural disasters, in Austria and abroad. He has further experience in kind of In-house Consultant of the EU-Research-Project "FOCUS-Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles", 2009-2012.

**Johannes Göllner, MSc MSc**
Is Head of the Section Knowledge Management of the Department of Central Documentation and Information Service at the National Defence Academy of the Federal Ministry of Defence and Sports, Vienna, since 2011; his research areas and consulting foci include Knowledge Management & -Development, Trend- & Risk Analysis and Scenario Planning & Development, since 2009; former positions include Chairmanship of the Steering Committee of ON Committee 246 "Risk-, Security & Crisis Management" at the Austrian Standards Institute (2003-2008) and national delegate at ISO and CEN, Researcher and Lecturer assignments Risk-, Crisis-, Security Management, Critical Infrastructure and Head of the Section Risk Management and Course Director of the Master of Business Administration (MBA)-Programm "Environmental Threats and Disaster Management" and staff officer at the NBC-Defence School of the AAF and Lecturer assignments at the University of Natural Resources and Life Sciences Vienna and University of Vienna, since 1999; has been further Senior Researcher & Deputy Leader-experience in kind of Inhouse Consultant of the EU-Research-Project "FOCUS-Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenuos EU Roles", 2009-

2012.

**Christian Haberfellner, MA MIM**
Is head of the department innovation and marketing within the Red Cross Austria – Ambulance Innsbruck. He studied Geography at the University of Innsbruck and did an Executive Master in Management. Since several years he is involved in development of regions in Europe and Africa.
In the Austrian Army Haberfellner works in the department of military geography. He was over 20 years management consultant and teaches at the University of Salzburg, the Management Business school Salzburg and the Management Center Innsbruck management topics with a strong focus on Innovation, Marketing, Change- and strategic Management.
He developed and lead various European projects in Austria and Italy over the last years. He is lecturer at many occasions in Europe.
Haberfellner is an expert of economic development of regions. He is a volunteer paramedic and an international search and rescue dog handler within the Red Cross.

**Herbert Bauer, MA**
Is Commanding Officer of the Military Command of the Tyrol of the Federal Ministry of Defense and Sports. He is in tactical lead during the exercise "Schutz 14" and in this function also responsible for inner state CIMIC with federal government, police, railway-association or press media. He was CO of Austrian Special Forces from 1995 to 1997, completed training in USA, Turkey, Portugal and Swiss and was sent on disaster assessment mission in Malawi/Africa as member of United Nation Disaster Assessment and Coordination Team (UNDAC) by department of Humanitarian Affairs in Geneva in 1997. He was CO of the 6th (Mountainous) Infantry Brigade in western Austria from 1999 to 2002 and is lector and board member to the UNESCO-Chair of Master of Arts Program in Peace, Development, Security and International Conflict Transformation on the University of Innsbruck/Tyrol. He also was chief of cabinet to the minister of defense from 2003 to 2005, during this time he accompanied the minster on visits to Austrian troops in Afghanistan, Syria, Bosnia and Kosovo. Since 2006 he is CO of the Military Command of the Tyrol and responsible for territorial defense and military disaster relief operations within the Federal State Tyrol.

# Horizon Scanning for emerging risks in supply chain systems

*Joachim Klerx, Johannes Göllner, Klaus Mak*

**Abstract**: Existing foresights studies produce expectations about mid-term and long-term trends. These expectations tend to change accidently, caused by external disruptive events. For reliable long-term strategic planning it is necessary to understand the dynamics of these changes. Our horizon scanning method is developed to address social needs, as well as scientific capabilities and technical solutions and will produce reliable knowledge about weak signals for threats, disruptive events and long-term trends. The goal of this extended abstract is, to present a consistent horizon scanning method, developed in the security domain, to deal with expectations about future trends in a rational manner. Rational in this context means that the expectations are formed, based on evidence

**Keywords:** Horizon scanning, foresight, strategic long term planning, research agenda setting, critical infrastructure, supply chain protection, cyber security

**Acknowledgement:** As the results, presented in this extended abstract rely on research activities in the FP7 projects SESTI, UNCOVER and ETTIS, we would like to express my special thanks of gratitude to all partners in these projects.

Transparent, public knowledge about long-term trends is very important for the efficiency of each strategic long term planning activity in all supply chain networks. Each stakeholder has their own expectations about future trends and behaves in accordance to these expectations. Misleading expectations can cause flawed investments and political strategies. To have reliable information about future social needs and possible technological solutions is a win-win situation for all stakeholders of each supply chain system. However traditionally each stakeholder tends to produce his own knowledge is often has no intention to share his knowledge. We will present a method for automatic knowledge creation and sharing to increase the public knowledge in the system.

## 1. Methodical concept

Knowledge about future developments, about future social needs, about future research and technologies is regularly created in large scale foresight and road mapping projects. However, these foresight and road mapping activities are very expensive and often resource intensive. In this paper, we present a method to collect this information from internet sources and to build semi automatic a knowledge base for strategic long term planning with measures for trustfulness and reliability out of these internet data.

The supply chain system usually is a very complex system. However for simplicity we asume, that there are three layers. First the actual infrastructure layer with different logistic infrastructures, like transport infrastructure, storage infrastructure and e.g. cooling infrastructure. Second the operating organizations of the infrastructure layer form a network structure of stakeholder and actors. Third, some of these stakeholders are involved in discussion about the future of this sector, about threats, road maps and possible structural changes in the future. The following figure shows the interaction of these layers.

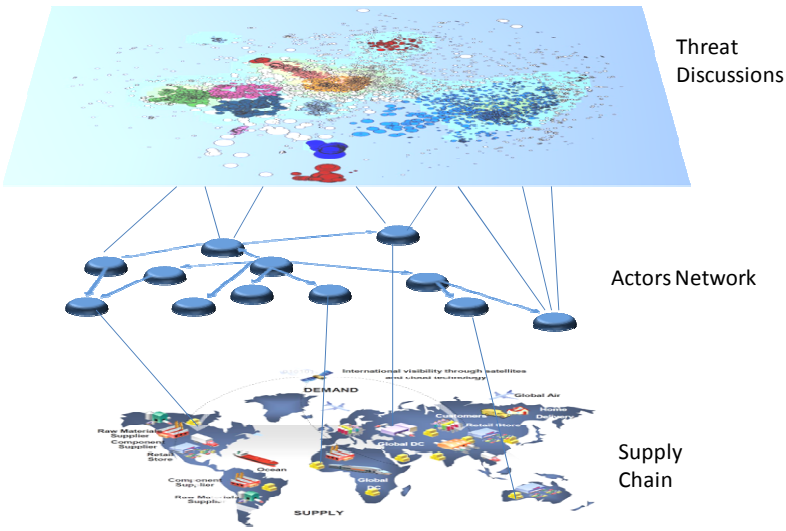



Figure 3: Different layer of supply chain networks (Source AIT, 2014)

Our measures for trust and reliability are based on the core concept of long term learning in future research. They are typically developed in large scale planning and foresight processes. However there is a remarkable probability that after a few years there are disruptive events, which causes structural changes and undermines trust and reliability of these planning processes. Therefore we developed a software for automatic scanning internet sources for weak signals of potential future disruptive events.

Finding potential new threats and disruptive events on the internet is notoriously difficult for an automated scanning process. Humans usually use semantic judgments to decide whether there is a threat in an internet discussion or not. Whether this threat is new, emerging or of declining importance is even more difficult for humans to find out. It is specific to our method, that we will not try to copy the human approach but use statistics to identify potential weak signals. In an initial crawling stage our agent loads search results from a search engine like Google, which are considered as relevant for the search, i.e. in our case for threat identification. The agent then follows each of the links extracted by the search engine to a result list and downloads the corresponding text information. If this text contains the search string, our threat identification agent (TIA), developed in ETTIS extracts title, keywords and main text, and notes the results in the site re-

pository. It then extracts all links from this "relevant" site and adds them to the link repository.

In a second and final stage of data acquisition, the agent iteratively follows all extracted links, again extracts the site attributes and once more tests whether the main text of the site contains the search string. To prevent the agent from being drawn into "black holes" for internet crawlers the agent will not download more than about 1000 documents from a single domain. All text results are grouped by domain, so that there is a consistent domain –text/date relation in the database. This database forms our data source for a topic map analysis.

Based on the downloaded dataset, the threat identification agent (TIA) uses hyperlinks from already identified community sites to find new community sites. By using hyperlinks, the agent makes use of wisdom of the crowds in a way that it uses links as expressions of trust from the source site to the link target site. As our potential text corpus on the internet contains hyperlinks, the text corpus can be thought of as a directed network, with authorities and hubs, in which an authority node is a site with a lot of inbound links, and a hub is a site with a lot of outbound links. Each node in the network has some text online, which can be used to form topic clusters.

## 2. Results

As a result, we receive topic cluster out of threat discussions on the internet. The clusters give an overview of the topics discussed in the community. As the whole text corpus is about future threats, the identified topics sum up the discussions about future threats.

For a detailed analysis the identified discussions are manually analyzed to identify the potential for a weak signal. Weak signals are small and therefore often early signs to events, which point to future threats, opportunities, needs or wild cards. In particular, the weak signals with a potential to be a wild card often points to future strategic discontinuity. Therefore they have a high analytical value for strategic long term planning.

**Threats** can be a warning that one is going to hurt or punish someone, they can be a sign of something dangerous or unpleasant which may be, or

is, about to happen, or they can be a source of danger.[1] In each meaning, the following 3 essential elements are part of a threat:

- a harmful event
- a cause of this event (either accidently or by intention)
- a effect of this event

Based on the wide geographic distribution of threat discussion on the internet, identified by TIA, it became obvious in the analytical work, that a threat is a subjective interpretation of a specific event. If this event is harmful to a person or a group, this event is considered as a threat from all group members. This opinion is not necessary shared by other groups and all other humans. In particular, there might be another group, who takes advantage from this event. The group will not usually consider this event as a threat. Therefore, threats are always subjective expression of values shared within the group. The same applies to opportunity. An **opportunity** might either be a favourable or advantageous circumstance, occasion or time, or a chance for progress or advancement. The advantage is usually related to a specific group. Thus this group will consider the favourable event as opportunity.

**Wild Cards** are high-impact events that seem too incredible to believe.. Therefore they tend to be overlooked in long term strategic planning. Often it leads even to a decrease in reputation in the peer group, if a member of this peer group starts to discuss a wild card seriously. In futurology, "wild cards" refer to low-probability, high-impact events, as introduced by John Petersen author of 'Out of The Blue - How to Anticipate Big Future Surprises'.[2] However more important than probability is, that these topics are not well known and not part of the mainstream discussion. Often these disruptive events are still too incomplete to permit an accurate estimation of their impact and to determine possible reactions. However for strategic long term planning and scenario development they are very important, as they increase the ability in scenario planning, to adapt to surprises arising in turbulent chaotic environments. In trend analysis, they point to trend breaks and tipping points.

---

[1] http://www.thefreedictionary.com

[2] Petersen, J. (2000) 'Out of The Blue - How to Anticipate Big Future Surprises' Madison Books

**Trend** as a future oriented concept is misleading. It is a well-known fact that it is easy to discover a trend based on historical data on the stock exchange. However it is nearly impossible to learn something about the share price of tomorrow from this. A trend in general is a direction, derived from past data. It is usually based on linear pattern, which only work in a specific context. Trends are usually described by time horizon, impact and geographical coverage. Here in this report, a trend is in a way the opposite of a wild card. Trends are expected events and wild cards are surprising events.

The result of the weak signal scan was a list of about 70 weak signals for either harmful events, threats, trends, wild cards or social needs. Topics out of this list where later on used in the human threat identification.

The following table presents a selection of weak signals, which are relevant for supply chain security.

Table 2: List of weak signals

| Title of weak signal | Domain | Source | Threat | Social Need | Potential for wild card |
|---|---|---|---|---|---|
| Stuxnet as first SCADA attack software platform | Nuclear, Environment, Cyber | TIA | x | x | 7 |
| Advanced persistent threats (APT), like Ghostnet | Nuclear, Environviron-ment, Cyber | TIA | x | x | 6 |
| Black Market prices explosion of Zero day exploits | Cyber | TIA | x | x | 8 |
| Military cyber attack unites | Nuclear, Environviron-ment, Cyber | TIA | x | x | 9 |

| | | | | | |
|---|---|---|---|---|---|
| Modular botnet development platforms | Cyber | TIA | x | x | 6 |
| Trojan horse software service industry | Cyber | TIA | x | x | 6 |
| Globalisation, strategic sourcing and cloude services | Cyber | TIA | x | x | 8 |
| Global advertising networks and private data exchange | Cyber | TIA | x | x | 10 |
| Dark nets and cryptographic peer to peer nets for anonymous publishing and whistleblowing | Cyber | TIA | x | x | 9 |
| Global black hacker industry and black markets | Cyber | TIA | x | x | 7 |
| Epistemic networks for knowledge exchange in organised crime | Cyber | TIA | x | 0 | 7 |

Source: D 4.4 ETTIS, AIT

### 3. Consequence

As a consequence from our experience with internet scanning, the scanning is very much driven by the definition of the search issue, which is reflected in the search strategy. Scanning activities will become better when expert experience in a specific domain is used to define the search strategy and a domain specific knowledge management is used to cluster the results. In general this implies, that repeated scanning can and should be used for iterative improvements in scanning activities.

In principle the internet is a suitable source for such a broad scanning.

However, the finding from internet sources needs additional human reasoning and interpretation in order to extract more consistent and accurate insights. In the process of sense making all categories of future issues (threats, needs, wild cards, disruptive events and so on) became more accurate. The precise knowledge about these different types of issues was not available at the beginning of the project. Taking into account, that this knowledge is helpful in scanning the internet, a repeated scan would lead to more precise results. This is a strong argument for setting up a horizon scanning center with a proper knowledge management.

**References**


- Bun, Khoo Khyou and Ishizuka, Mitsuru, Emerging topic tracking system in WWW, Knowledge-Based Systems 19 (2006) 164-171, Elsvier, 2006
- Butter, Maurits, et al., Early warning scanning; dealing with the unexpected, An operational framework for the identification and assessment of unexpected future developments, SESTI working paper, 13. December 2009
- Dillard, Logan, Valence-Shifted Sentences in Sentiment Classification, University of Washington, Institute of Technology - Tacoma, 2007
- Esuliand, Andrea and Sebastiani, Fabrizio, Page Ranking WordNet Synsets: An Application to Opinion Mining, Proceedings of the 45th Annual Meeting of the Association of Computational Linguistics, pages424–431, Prague, Czech Republic, June 2007
- Feinerer, Ingo, A Text Mining Framework in R and Its Applications, Wirtschaftsuniversität Wien, Department of Statistics and Mathematics, Vienna, Austria, 2008
- Hiltunen, Elina, Good Sources of Weak Signals: A Global Study of Where Futurists Look For Weak Signals, in Journal of Futures Studies, May 2008, 12(4): 21 – 44, Finland Futures Research Centre, Finland, 2008
- Lee, Changki, Lee, Gary Geunbae and Jang, Myunggil, Use of place information for improved event tracking, Information Processing and Management 43 (2007) 365–378, Elsevier, 2007

- Manu Aery, Naveen Ramamurthy, Y. Alp Aslandogan, Topic Identification of Textual Data, Technical Report CSE-2003-25, Department of Computer Science and Engineering, University of Texas at Arlington, Arlington, TX 76019, 2003
- Roth, Camille and Bourgine, Paul, Epistemic communities: description and hierarchic categorization, Center for Research in Applied Epistemology, CNRS/EcolePolytechnique, 1 rue Descartes, 75005 Paris, France, Dec. 2004
- Russell, Stuart & Norvig, Peter, Artificial Intelligence, A Modern Approach, Prentice Hall Series in Artificial Intelligence, Pearson Education, 2003, USA
- Surowiecki, James, The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations, Anchor, New York, 2004
- Taleb, Nassim, The black swan: the impact of the highly improbable, Random House, New York, USA, 2007
- Wooldridge, Michael & Jennings, Nicholas R., Pitfalls of Agent-Oriented Development, Department of Electronic Engineering, Queen Mary & Westfield College, University of London, London E1 4NS, United Kingdom, fM.J.Wooldridge@qmw.ac.uk; N.R.Jenningsg@qmw.ac.uk, 1998
- Zdravko Markov and Daniel T.Larose, Datamining the WEB, Uncovering Patterns in Web Content,Structure and Usage, Central Connecticut State University, New Britain, CT, Wiley-Interscience, 2007
- Amanatidou, E. et al. (2011). On Concepts and Methods in Horizon Scanning: Lessons from Initiating Policy Dialogues on Emerging Issues. Submitted paper for the FTA 2011 conference, Seville.
- Ansoff, H.I. (1975). Managing Strategic Surprise by Response to Weak Signals, Califonia Management Review XVIII(2), 21–33.
- Botterhuis, L., van der Duin, P., de Ruijter, P., van Wijck, P. (2010). Monitoring the Future. Building an Early Warning System for the Dutch Ministry of Justice, Futures 42, 454–465.
- DEFRA (2002). Horizon Scanning & Futues Home. http://horizonscanning.defra.gov.uk/ (15.7.2011)

- Georghiou, L. (2007). "Future of Foresighting for Economic Development." UNIDO, Vienna (Available at: https://www.unido.org/foresight/rwp/dokums_pres/tf_plenary_georghiou_201.pdf, 15.7.2011)
- Könnölä, T. et al. (2011). Facing the Future: Scanning, Synthesizing and Sense-Making in Horizon Scanning. Submitted paper for the FTA 2011 conference, Seville.
- Loveridge, D. (2009). "Foresight: The Art and Science of Anticipating the Future." Routledge, London.
- RAHS (2004). Risk Assessment and Horizon Scanning programme of Singapore. http://app.hsc.gov.sg/public/www/home.aspx (15.7.2011)
- Schultz, W.L. (2006). The Cultural Contradictions of Managing Change: Using Horizon Scanning in an Evidence-based Policy Context, Foresight 8(4), 3–12.

**Authors**

**Dr. Joachim Klerx**
workes at AIT Foresight & Policy Development Department for 14 years in different fields of research- and innovation policy. As philosopher and economist by education, his main focus is currently the exploration of innovative groups and their issue management. He uses methods from the field of data mining, artificial intelligence and agent programming. His special achievement in recent years was the development of a political information systems for the analysis of the innovation system of the Vienna region, the development of ISA (Intelligent screening agent) an agent who is looking for weak signals of emerging issues on the Internet, financed by SESTI an EU project about identification of weak signals developed for emerging issues. In the EU project ETTIS Joachim Klerx works an a system for threat-identification and political agenda setting and in EFP, he did the engineering for a global knowledge exchange platform for the world foresight community.

**Johannes Göllner, MSc MSc**
Is Head of the Section Knowledge Management of the Department of

Central Documentation and Information Service at the National Defence Academy of the Federal Ministry of Defence and Sports, Vienna, since 2011; his research areas and consulting foci include Knowledge Management & -Development, Trend- & Risk Analysis and Scenario Planning & Development, since 1999; former positions include Chairmanship of the Steering Committee of ON Committee 246 "Risk-, Security & Crisis Management" at the Austrian Standards Institute (2003-2008) and national delegate at ISO and CEN, Researcher and Lecturer assignments Risk-, Crisis-, Security Management, Critical Infrastructure and Head of the Section Risk Management and Course Director of the Master of Business Administration (MBA)-Programm "Environmental Threats and Disaster Management" and staff officer at the NBC-Defence School of the Austrian Armed Forces (since 1999) and Lecturer assignments for Risk & Crises Management and Leadership at the University of Natural Resources and Life Sciences Vienna and University of Vienna, since 2008 ; has been further Senior Researcher & Deputy Leader-experience in kind of Inhouse Consultant of the EU-Research-Project "FOCUS-Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenuos EU Roles", 2009-2012.

**Klaus Mak, MA**
Is Head of the Department of Central Documentation and Information Service at the National Defence Academy (NDA) of the Federal Ministry of Defence and Sports, Vienna; 1982 - 1985 Theresian Military Academy, Austria and served 6 years in a Mechanized Brigade, keeps a Masters degree in Political Science and Communication Science at the University of Vienna; since 1993 Head of the Department of Central Documentation and Information Service at the NDA and since 2004 responsible for main tasks in the field of "Knowledge Management" in the Austrian Armed Forces. Responsible for Concept Development, the R&D field "KM" and operational tasks.

# 13. Symposium Energieinnovation

## EnInnov 2014

*Innehalten und Ausblick: Effektivität und Effizienz für die Energiewende*
Technische Universität Graz, 12.02.-14.02.2014

In den letzten Jahren wurden große Fortschritte im Bereich der Nutzung erneuerbarer Energien erzielt, wobei die Entwicklungen in den Bereichen Windkraftnutzung und Photovoltaik besonders hervorzuheben sind. Diese Entwicklungen haben unter anderem dazu geführt, dass einerseits die Preise an den europäischen Strombörsen zum Teil massiv eingebrochen sind und andererseits das Fördervolumen für die Nutzung erneuerbarer Energien stark zugenommen hat. Im Falle der stark zunehmenden intermittierenden Stromerzeugung betreffen künftige Aufgabenstellungen vor allem die Bereiche Stromtransport, die Integration in das Gesamtsystem sowie Lösungen hinsichtlich des zunehmenden Speicherbedarfes. Parallel dazu findet eine Flexibilisierung des gesamten Energie-systems von der Erzeugung über die Verteilung bis hin zum Verbraucher statt.

Darüber hinaus wurde bisher der Fokus primär auf aufbringungsseitige Fragestellungen gelegt und nachfrageseitige Aspekte tendenziell geringer beachtet. Aktuelle Bestrebungen der Europäischen Union erfordern künftig die stärkere Berücksichtigung von Energieeffizienz und -management, beispielsweise durch Umsetzung der Energieeffizienz-Richtlinie.

Diesen Gegebenheiten muss das Marktsystem bzw. die Aufbau- und Ablauforganisation entsprechend Rechnung tragen, um auch künftig das Funktionieren des Gesamtsystems sicherzustellen. Es ist daher erforderlich, die bisherigen Lösungsansätze zu überdenken und an die geänderten Rahmenbedingungen anzupassen: Machen wir die richtigen Dinge (im Sinne der Effektivität) und machen wir die Dinge richtig (im Sinne der Effizienz)?

### Ziel des Symposiums

Die Lösungsansätze müssen neben der Ausgestaltung der europäischen Wirtschaftsordnung inkl. regulatorischer Fragestellungen, die Energieaufbringung (Erneuerbare Energien, Innovative Energietechnologien), Energieverteilungssysteme aber vor allem auch nachfrageseitige Maßnahmen

(Energiesparen, Energieeffizienz, Energiemanagement) betreffen.

Wissenschaft, Wirtschaft sowie Politik und Verwaltung sind daher gefordert, entsprechende Beiträge für die gedeihliche Entwicklung der europäischen Energiewirtschaft und Gesellschaft zu leisten und deren Beiträge werden im Rahmen des 13. Symposium Energieinnovation präsentiert und diskutiert.

Technische Universität Graz
Institut für Elektrizitätswirtschaft und Energieinnovation
Inffeldgasse 18
A-8010 Graz
http://portal.tugraz.at/portal/page/portal/TU_Graz/Einrichtungen/Institute/Homepages/i4340/veranstaltungen/eninnov2014/

Das folgende peer-reviewed Paper liegt in der Langfassung vor. Es wurde in der Kurzfassung in den Conference Proceedings mit der Langfassung als Beilage veröffentlicht. Die freundliche Genehmigung zur Veröffentlichung in diesem Band wurde durch Hr. Assoc.Prof. Dipl.-Ing. Dr.techn. Udo Bachhiesl am 26.06.2014 erteilt.

# Bedeutung des Risikomanagements für die Sicherheit von Smart Grids

*Johannes Göllner, Christian Meurers, Andreas Peer, Lucie Langer, Markus Kammerstetter*

**Abstract:** Die Energieversorgung der Zukunft wird sich fundamental auf den Einsatz von IKT-Systemen stützen. Die damit verbundenen Risiken wirken sich unmittelbar auf die Sicherheit der Energieversorgung aus und stellen neue Bedrohungsbilder in diesem Bereich dar. Im Rahmen des KIRAS-Sicherheitsforschungsprogramms beschäftigt sich das Projekt *Smart Grid Security Guidance (SG)²*, basierend auf einer fundierten Bedrohungs- und Risikoanalyse aus einer gesamtstaatlichen Sicht sowie auf Sicherheitsanalysen von Smart-Grid-Komponenten, mit einer systematischen Untersuchung von Smart-Grid-Technologien in Bezug auf IKT-Aspekte und der Erforschung von entsprechenden Gegenmaßnahmen zur Erhöhung der Sicherheit von IKT-Systemen in der kritischen Infrastruktur „Energie".

**Keywords:** Energie, Bedrohung, Sicherheit, Kritische Infrastruktur, Smart Grid

**Kurzfassung:**
http://portal.tugraz.at/portal/page/portal/Files/i4340/eninnov2014/files/kf/KF_Meurers.pdf

**Langfassung:**
http://portal.tugraz.at/portal/page/portal/Files/i4340/eninnov2014/files/lf/LF_Meurers.pdf

**Präsentation:**
http://portal.tugraz.at/portal/page/portal/Files/i4340/eninnov2014/files/pr/PR_Goellner.pdf

## 1 Einleitung

Die immer rasantere Entwicklung neuer Technologien am Sektor der Energieversorgung sowie der zunehmende Energiebedarf unserer Gesellschaft lassen grundlegende Veränderungen in der Bereitstellung von Energie und den Energienetzen erwarten. Konventionelle Ansätze und Technologien werden in Zukunft die steigenden Anforderungen nicht mehr decken können, daher werden zunehmend Informations- und Kommunikationstechnologien (IKT) angewendet, um Energie effizienter verteilen, aber auch die Integration von Wind-, Solar- oder Biomasse-Energieerzeugern in das vorhandene Stromnetz sicherstellen zu können. Diese Integration von Energie-Anbietern, Verbrauchern, Erzeugern und Netzbetreibern mittels IKT bildet die Basis für *Smart Grids*.

Es entsteht mit den zunehmenden Einsatz dieser Smart Grid Technologien parallel zum Stromnetz ein neues, umfassendes IKT-Netz, das aber den gleichen Risiken und Gefahren ausgesetzt sein wird, wie wir sie beispielsweise von herkömmlichen IKT-Netzen wie dem Internet kennen. Die große Ausdehnung, die große Anzahl an Teilnehmern und Zugangspunkten, vor allem aber die starke zukünftige Abhängigkeit der Energieversorgung von diesen IKT-Systemen machen die Notwendigkeit einer umfassenden Risikoanalyse und –bewertung deutlich, um bereits jetzt Maßnahmen zur Gefahrenabwehr ableiten und treffen zu können. Energiediebstahl durch Stromzählermanipulation, Angriffe auf Kontrollelemente der Netzbetreiber zur Störung des Betriebes oder großräumige Abschaltungen des nationalen Stromnetzes zählen hier unter anderem zu den möglichen Bedrohungsbildern, die aber fatale Folgen hätten. Daher haben intelligente Stromnetze (Smart Grids) nur dann Zukunft, wenn die Sicherheit der kritischen Infrastrukturen durch entsprechende Maßnahmen gewährleistet werden kann.

Im Rahmen des Sicherheitsforschungsprogrammes KIRAS wird daher das Projekt *Smart Grid Security Guidance - (SG)²* durchgeführt, das solche Maßnahmen auf Basis einer umfassenden Risiko- und Bedrohungsanalyse erforscht und Methoden, Konzepte und Modelle zur Risikominimierung, aber auch begleitende Softwarewerkzeuge, entwickelt. Neue Ansätze zur Modellierung komplexer IKT-gestützter Smart Grid Architekturen bilden dabei die Grundlage für die Analyse primärer Angriffsformen und An-

griffsflächen und der Abschätzung von Folgewirkungen. Auf Basis dieser Modelle werden Schutzmaßnahmen und –strategien gegen mögliche im Rahmen von Sicherheits- und Risikoanalysen identifizierten und bewerteten Bedrohungen und Verwundbarkeiten entwickelt. Ein wesentliches Ergebnis des Projektes ist daher auch ein Katalog von Schutzmaßnahmen, die notwendig sind, um einerseits die Sicherheit von Smart Grids gegen Angriffe auf das IKT-Netz gewährleisten zu können, andererseits aber die entstehenden Bedrohungen in den Fokus der Netzbetreiber zu rücken. Außerdem werden im Rahmen des Projektes neue Software-Werkzeuge entwickelt, um die Umsetzung der angesprochenen Maßnahmen, der erforschten Richtlinien und Methoden im komplexen Umfeld der IKT-Sicherheit zu unterstützen.

Das KIRAS-Projekt *Smart Grid Security Guidance – (SG)²* trägt der zunehmenden Bedeutung von IKT-Systemen und deren Einsatz in der Energieversorgung Rechnung und vereint Energienetzbetreiber, staatliche Stellen, die mit dem Schutz kritischer Infrastrukturen betraut sind, Smart Grid Produkthersteller aus der Industrie sowie Experten im Bereich Informationssicherheit aus dem akademischen und privatwirtschaftlichen Umfeld, um auf möglichst breiter Basis neuartige, auf nationale Verhältnisse zugeschnittene Maßnahmen zur Realisierung eines zukünftigen sicheren und intelligenten Stromnetzes in Österreich zu erforschen.

## 2 Das Doppel-Vektoren Modell

Im Rahmen des KIRAS-Projekts *Smart Grid Security Guidance – (SG)²* wurde ein Risikokatalog für Smart Grids in Österreich entwickelt, welcher Energieversorgungsunternehmen dabei unterstützen soll, eine Risikoanalyse für ihr System durchzuführen. Als Basis für die Bedrohungs- und Risikoanalyse dienen zunächst State-of-the-Art-Risikomodelle wie die BSI-Standards und IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik, die in den Bereichen der Informationstechnik und Risikoanalyse bereits ein weites Spektrum an Gefährdungen abdecken. Weiters werden Ergebnisse und Ansätze aus bereits durchgeführten Forschungsprojekten, wie beispielsweise das Doppelvektorenmodell, berücksichtigt.

Die Komplexität von Systemen und die Etablierung einer gemeinsamen Terminologie machen Kategorisierungsmodelle erforderlich, um System-

komponenten und –elemente klassifizieren zu können. Dieser Ansatz garantiert einen normierten und analytischen Prozess, um Ergebnisse und verschiedene Elemente und Komponenten miteinander vergleichen zu können. Dazu wurde das sogenannte Doppelvektorenmodell auf Basis einer ersten Kategorisierungsebene (Metakategorisierungsebene) im Rahmen des BMLVS-internen Forschungsprojektes „Szenarioplanung und Wissensmanagement im ÖBH“ im Zeitraum 2010 – 2013 durch Johannes GÖLLNER, Klaus MAK, Christian MEURERS, Andreas PEER und Günther POVODEN entwickelt.

Die Kategorisierungs-Systematik des Doppelvektorenmodells ist in der nachfolgenden Abbildung dargestellt

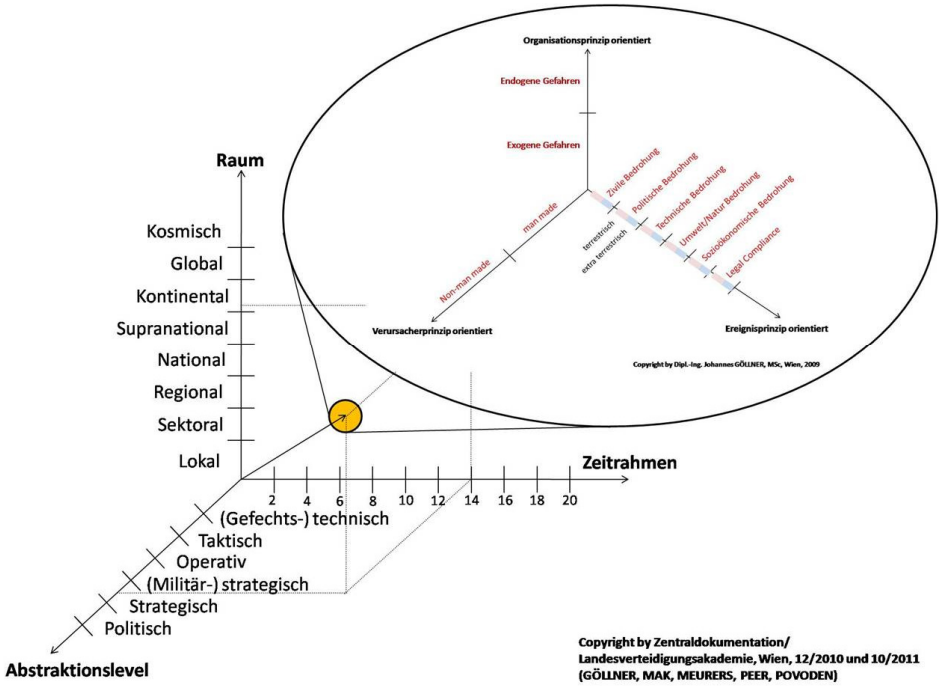



Abb. 1: Doppelvektorenmodell

Das Doppelvektorenmodell stellt ein dreidimensionales, mehrstufiges Meta-Klassifikationssystem dar, in dem jedes Element über die vektorale Zuordnung von definierten Eigenschaften und Attributen dargestellt und be-

schrieben werden kann.

Die erste Ebene unterscheidet die Ordinaten nach zeitlichen und räumlichen Aspekten und bietet einen organisations- bzw. ebenenspezifischen Abstraktionslevel an (politisch, strategisch, militärstrategisch, operativ, taktisch, gefechtstechnisch).

In der zweiten Ebenen wird das Ereignis kategorisiert hinsichtlich des Verursachers und ob Organisationsimmanente Gefahren einwirken oder resultieren. Zusätzlich kann/muss das Ereignis im Rahmen der Ereignisprinzip-Achse, auch unter Berücksichtigung des Ursprunges (terrestrisch, extraterrestrisch), weiter kategorisiert werden.
Das Doppelvektorenmodel bietet somit eine normierte Basis für weitere Analysen.

Nachfolgend sind die einzelnen Vektoren detailliert beschrieben:

- Vektor 1[1,2,3,4,5,6,,,,,,]:

[1] Göllner, Johannes/Meurers, Christian/Peer, Andreas/Povoden, Günter: Systemdefinition, Systembeschreibung und Systembegren-zung zur Szenarioentwicklung und Szenariomodellierung - Teil 2: Darstellung von ausgewählten Methoden und möglichen Teilsyste-men, Schriftenreihe der National Defence Academy 13/2010, S.7, Vienna, Austria, Feber 2011, ISBN: 978-3-902670-53-3.

[2] Göllner, Johannes/Meurers, Christian/Peer, Andreas/Povoden, Günter: Wissensmanagement im ÖBH, Systemdefinition, System-beschreibung und Systembegrenzung zur Szenarioentwicklung und Szenariomodellierung - Teil 3.A: Einführung in Szenarioentwick-lung und Szenariomanagement-Grundlagen, Szenariotechnik und Szenarioplanung, Schriftenreihe der National Defence Academy 15/2010, S.37, Vienna, Austria, September 2011, ISBN: 978-3-902670-55-7.

[3] Vortrag: Hybridisation of Social Network Analysis in Contxt with other Methods for a Scenario Based Risk Analysis-Case Study: Critical Infrastructure for Energy Security in Austria (Johannes GOLLNER, Christian MEURERS, Andreas PEER, Guenter POVODEN), accepted paper at the 7th Social Network Confer-ence 2011 at the University of Greenwich, London, United King-dom, accepted: 13.05.2011 by Programme Committee, ppt.-presentation at the Conference 07.07.2011

[4] Vortrag: „Staatliche Sicherheit und Versorgungssicherheit am Bei-spiel Energie“: Beispiel- und modellhafte Darstellung Kritischer Infrastrukturen und deren Inter-aktionen mit Fokus Energie (Jo-hannes GOLLNER, Andreas PEER), ppt.-Präsentation (Seite 33) iRd World Energy Council-Landesverteidigungsakademie- Sympo-sion am 13.10.2011 an der Landesverteidigungsakademie, Wien.

- Raum
    - Lokal
    - Sektoral
    - Regional
    - National
    - Supranational
    - Kontinental
    - Global
    - Kosmisch
- Abstraktionslevel
    - (Gefechts-)technisch
    - Taktisch
    - Operativ
    - (Militär-)strategisch
    - Strategisch
    - Politisch
- Zeitrahmen
    - Sekunde
    - Minute
    - Stunde
    - Tage
    - Wochen
    - Monate
    - Jahre
    - Jahrzehnte
    - Jahrhunderte

---

[5] Vortrag: Soziale Netzwerkanalyse –SNA iRd Wissensmanagement- Forschungsprojektes „Szenarienplanung und WM“ des ÖBH: Bei-spiel- und modellhafte Darstellung Kritischer Infrastrukturen unter Berücksichtigung der SNA (Klaus MAK, Johannes GOLLNER), ppt.-Präsentation (Seite 17+18) iRe geladenen Vortrages Bundeskriminalamt des BMI, November 2011, Wien.

[6] Vortrag/Briefing: Beispiel- und modellhafte Darstellung einer Risi-koanalyse (Johannes GOLLNER), ppt.-Präsentation (Seite 16) iRd Raiffeisen Akademie-LG für Bankmanager an der Landesverteidi-gungsakademie Wien, 27.02.2012, Wien.

- Vektor 2[7]:
  - Organisationsprinzip-orientiert
    - Exogene Gefahren
    - Endogene Gefahren
  - Verursacherprinzip-orientiert
    - Man-made
    - Non-man-made
  - Ereignisprinzip-orientiert (terrestrisch/extraterrestrisch)
    - Zivile Bedrohung
    - Politische Bedrohung
    - Technische Bedrohung
    - Umwelt/Natur Bedrohung
    - Sozioökonomische Bedrohung
    - Legal Compliance

Das Doppelvektorenmodell wurde in mehreren Anwendungsfällen erarbeitet, weiterentwickelt sowie getestet und stellt die Möglichkeit dar, ereignisrelevanten Inhalt zu dokumentieren und für weitere Analysen abrufbar zu Verfügung zu stellen. Auch lassen sich Muster zu diversen Ereignissen in spezifischen Kategorien damit erkennen, was einen weiteren Mehrwert im Rahmen dieses KIRAS Forschungsprojektes $(SG)^2$ darstellt.

## 3 Der $(SG)^2$-Risikokatalog

Ausgehend von der durch CEN-CENELEC-ETSI entwickelten Referenzarchitektur (Smart Grid Architecture Model)[8] [8] wurde zunächst ein IKT-Architekturmodell für österreichische Smart Grids definiert, welches als Grundlage für den Risikokatalog diente.

Dazu wurden die IKT-Architekturen ausgewählter nationaler sowie internationaler Smart-Grid-Projekte auf SGAM abgebildet. In den meisten Fällen wurde bei Einordnung in das SGAM-Modell vorwiegend derjenige Teil

[7] Göllner, Johannes, Eigendefinition von 06/2009, Vorlesungsprä-sentation an der Donau Universität Krems iRd LVA Risikoma-nagement; Integraler Bestandteil der internen Publikationen und Vortragsreihen der LVAk [3]-[6]

[8] CEN-CENELEC-ETSI Smart Grid Coordination Group: Smart Grid Reference Architecture, Document for the M/490 Mandate, Version 3.0, 2012

des SGAM-Modells belegt, welcher den Domains Distribution, DER und Customer Premises, sowie den Zonen Process, Field und Station entspricht. Die Auswirkungen der Einführung von Smart Grids zeigen sich somit deutlicher im Mittel- und Niederspannungsnetz sowie bei der verteilten Erzeugung, da diese Bereiche bisher einen niedrigen Automatisierungsgrad aufweisen. Ergänzend zu den ausgewählten Pilotprojekten wurden auch Systemarchitekturen nationaler Energieversorgungsunternehmen betrachtet und auf SGAM abgebildet, wobei neben dem aktuellen Stand der Technik auch bereits kurz- bis mittelfristig absehbare Entwicklungen berücksichtigt wurden. Ergebnis dieser Auswertungen war schließlich ein IKT-Architekturmodell, welches die verschiedenen IKT-Komponenten und Kommunikationsverbindungen zwischen diesen aufzeigt. Dieses diente anschließend als Grundlage für den Bedrohungs- und Risikokatalog.

Um die Bedrohungs- und Risikoanalyse nicht allzu komplex werden zu lassen, wurden die im Architekturmodell dargestellten Komponenten und Kommunikationsverbindungen zu den folgenden Domänen gebündelt:

- Funktionale Gebäude
- E-Mobilität
- Haushalte
- Erzeugungsanlage Niederspannung
- Erzeugungsanlage Mittelspannung
- Messstellen
- Umspannwerk (Hoch-/Mittelspannung)
- Umspannwerk (Mittel-/Niederspannung)
- Netzbetrieb
- Metering
- Energiehandel

Anschließend wurden, ausgehend von den IT-Grundschutz-Bedrohungskatalogen[9] sowie ergänzenden Dokumenten wie z.B. den ein-

[9] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standards 100-1 bis 100-4, 2008, aktuelle Version erhältlich unter https://www.bsi.bund.de/

schlägigen BSI-Schutzprofilen[10],[11], relevante Bedrohungen identifiziert. Auf diese Weise entstand eine Liste von etwa 250 Bedrohungen, die jedoch zum Teil unterschiedliche Detaillierungsgrade aufwiesen. Um eine konsistente Darstellung zu erreichen, wurden diese Bedrohungen in weiteren Iterationen teils zusammengefasst und auf den Smart-Grid-spezifischen Kontext zugeschnitten. So entstand letztendlich ein Katalog von 31 Bedrohungen, welche verschiedenen Kategorien zugeordnet wurden. Diese Bedrohungen wurden anschließend im Rahmen des vorhandenen IKT-Architekturmodells evaluiert, d.h. es wurde untersucht, inwieweit die Bedrohungen auf die einzelnen Domänen zutreffen.

Anschließend wurde das Risikopotential dieser Bedrohungen bewertet, indem die Eintrittswahrscheinlichkeit und die Auswirkungen eines erfolgreichen Angriffs geschätzt wurden. Die Einschätzung erfolgte jeweils auf einer Skala von 1 (sehr gering) bis 5 (sehr hoch). Durch Multiplikation der beiden Werte ergibt sich das zu der jeweiligen Gefährdung gehörige Risikopotential. Dabei wurde das Risikopotential bei Werten <5 als „niedrig", zwischen 5 und 12 als „mittel" und ab 12 als „hoch" eingestuft. Insgesamt lässt sich sagen, dass erfolgreiche Angriffe auf die dezentralen Komponenten beim Kunden (d.h. einzelne Haushalte) eine hohe Wahrscheinlichkeit und eher geringe Auswirkungen haben, während es sich bei den zentralen Komponenten v.a. im Netzbetrieb umgekehrt verhält. Zieht man jedoch in Betracht, dass erfolgreiche Angriffsmethoden beispielsweise auf Smart Meter öffentlich werden und sich entsprechend rasch verbreiten, so können die Auswirkungen auch hier gravierend sein und die Stabilität des Energienetzes maßgeblich negativ beeinflussen.

Der $(SG)^2$-Risikokatalog vermag keine individuelle Risikoanalyse eines konkret implementierten Systems zu ersetzen, kann jedoch Energieversorgern als Hilfestellung dienen, um Bereiche mit hohem Risikopotential zu identifizieren und ihre Gegenmaßnahmen hierauf zu fokussieren. Vorschläge zu geeigneten Sicherheitsmaßnahmen werden derzeit im Projekt $(SG)^2$ erarbei-

[10] Bundesamt für Sicherheit in der Informationstechnik: Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen (BSI-CC-PP-0073), Version 1.2, 2013

[11] Bundesamt für Sicherheit in der Informationstechnik: Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen (BSI-CC-PP-0077), Version 1.0, 2013

tet.

## 4 Auswertung & Ausblick

Vor allem durch die fortschreitende Transformation bestehender Energienetze zu Smart Grids und der damit verbundenen massiven Integration von Informations- und Kommunikationstechnologien (IKT) stehen Netzbetreiber heute vor der Herausforderung die dadurch entstehenden Risiken adäquat zu bewerten. Erst durch die Risikobewertung können kritische Bereiche identifiziert und in weiterer Folge besser geschützt werden. Diese Risikobewertung kann allerdings nur mittels Detailbetrachtung der bei den Netzbetreibern umgesetzten Systemlandschaft erfolgen. Eine auf die Gesamtarchitektur bezogene Risikobewertung fehlt jedoch häufig. Viele Netzbetreiber stehen daher heute vor dem Problem, zum einen auf keine geeigneten Risikomanagement Methoden im Smart Grid Bereich zurückgreifen zu können und, zum anderen, Risiken in der Smart Grid Gesamtarchitektur nicht erfassen zu können.

Im Gegensatz zu den im EURACOM FP7 Projekt analysierten bestehenden Methoden [13], verfolgt der im KIRAS-Projekt *Smart Grid Security Guidance – (SG)²* entstandene Risikokatalog einen durch die Gesamtarchitektur getriebenen Ansatz. Durch die architekturelle Bewertung in Bezug auf Risikopotential und Eintrittswahrscheinlichkeit erfolgt für die Netzbetreiber eine innerhalb des Smart Grids architekturbezogene Vorauswahl der bestehenden Risiken.

Durch Kombination der Gesamtarchitektur Risikobewertung mit der detailbezogenen individuellen Risikobewertung ermöglicht die Anwendung des (SG)² Risikokatalogs einen gesamtheitlichen Ansatz.

Sowohl die Gesamtarchitektur wie auch der (SG)² Risikokatalog wurden nicht nur in Abstimmung mit führenden Netzbetreibern und Herstellern entwickelt, sondern auch in mehreren Feedbackrunden mit den Mitgliedern des (SG)² Konsortiums evaluiert und kontinuierlich erweitert. Dadurch kann ein hoher praktischer Nutzungsfaktor gewährleistet werden. Der Hauptnutzen liegt dabei in der Möglichkeit Fragestellungen aus unterschiedlichen Expertendomänen klar formulieren und mittels einzelner Elemente des Architekturmodells gezielt beantworten zu können.

Im Spezifischen fanden folgende Evaluierungsschritte statt:

1. Evaluierung des Gefahrenkatalogs: Um den Gefahrenkatalog zu evaluieren und in Bezug auf seine Praktikabilität und Nähe zu realen Smart Grid Umgebungen zu evaluieren, wurden mehrere Workshops mit Experten aus den Bereichen Netzbetreiber, Hersteller sowie akademischer Forschungseinrichtungen durchgeführt. Im Zuge dieser Workshops wurden weitere Gefahren zum Gefahrenkatalog hinzugefügt, die besonders für die Smart Grid Domäne relevant sind.
2. Evaluierung der Gefahren: Um die jeweiligen Gefahren im Gefahrenkatalog zu evaluieren, wurden diese innerhalb des Architekturmodell von einem Expertenteam aus Netzbetreibern, Herstellern und akademischen Forschungspartnern in Bezug auf deren Kritikalität sowie der Abhängigkeitsverhältnisse geprüft. Die Ergebnisse wurden erneut innerhalb des Konsortiums diskutiert und gemeinsam mit den Netzbetreiben in Enduser-Workshops präzisiert.
3.

Evaluierung in Bezug auf Eintrittswahrscheinlichkeiten und Auswirkungen: Im letzten Schritt fand in Bezug auf den Gefahrenkatalog eine Evaluierung der Eintrittswahrscheinlichkeiten und der Auswirkungen statt. Diese Evaluierung wurde im unabhängig von einer durch Experten aus den Bereichen Netzbetreiber, Hersteller und akademischen Forschungspartnern durchgeführt und widerspiegelt jeweils deren Einschätzungen. In einem gemeinsamen Workshop wurden die Ergebnisse schließlich konsolidiert und gemeinsam diskutiert sodass ein breiter Einsatzbereich des resultierenden Gefahren- und Risikokatalogs sicherzustellen.

## Danksagung

Diese Arbeit wurde durch das Österreichische Förderungsprogramm für Sicherheitsforschung KIRAS und das Bundesministerium für Verkehr, Innovation und Technologie (BMVIT) im Rahmen des Projekts Smart Grid Security Guidance (SG)² gefördert.

## 5 Referenzen


[1] Göllner, Johannes/Meurers, Christian/Peer, Andreas/Povoden, Günter: Systemdefinition, Systembeschreibung und Systembegrenzung zur Szenarioentwicklung und Szenariomodellierung - Teil 2: Darstellung von ausgewählten Methoden und möglichen Teilsystemen, Schriftenreihe der National Defence Academy 13/2010, S.7, Vienna, Austria, Feber 2011, ISBN: 978-3-902670-53-3.

[2] Göllner, Johannes/Meurers, Christian/Peer, Andreas/Povoden, Günter: Wissensmanagement im ÖBH, Systemdefinition, Systembeschreibung und Systembegrenzung zur Szenarioentwicklung und Szenariomodellierung - Teil 3.A: Einführung in Szenarioentwicklung und Szenariomanagement-Grundlagen, Szenariotechnik und Szenarioplanung, Schriftenreihe der National Defence Academy 15/2010, S.37, Vienna, Austria, September 2011, ISBN: 978-3-902670-55-7.

[3] Vortrag: Hybridisation of Social Network Analysis in Contxt with other Methods for a Scenario Based Risk Analysis-Case Study: Critical Infrastructure for Energy Security in Austria (Johannes GOLLNER, Christian MEURERS, Andreas PEER, Guenter POVODEN), accepted paper at the 7th Social Network Conference 2011 at the University of Greenwich, London, United Kingdom, accepted: 13.05.2011 by Programme Committee, ppt.-presentation at the Conference 07.07.2011

[4] Vortrag: „Staatliche Sicherheit und Versorgungssicherheit am Beispiel Energie“: Beispiel- und modellhafte Darstellung Kritischer Infrastrukturen und deren Inter-aktionen mit Fokus Energie (Johannes GOLLNER, Andreas PEER), ppt.-Präsentation (Seite 33) iRd World Energy Council-Landesverteidigungsakademie- Symposion am 13.10.2011 an der Landesverteidigungsakademie, Wien.

[5] Vortrag: Soziale Netzwerkanalyse –SNA iRd Wissensmanagement-Forschungsprojektes „Szenarienplanung und WM“ des ÖBH: Beispiel- und modellhafte Darstellung Kritischer Infrastrukturen unter Berücksichtigung der SNA (Klaus MAK, Johannes GOLLNER),

ppt.-Präsentation (Seite 17+18) iRe geladenen Vortrages Bundeskriminalamt des BMI, November 2011, Wien.

[6] Vortrag/Briefing: Beispiel- und modellhafte Darstellung einer Risikoanalyse (Johannes GOLLNER), ppt.-Präsentation (Seite 16) iRd Raiffeisen Akademie-LG für Bankmanager an der Landesverteidigungsakademie Wien, 27.02.2012, Wien.

[7] Göllner, Johannes, Eigendefinition von 06/2009, Vorlesungspräsentation an der Donau Universität Krems iRd LVA Risikomanagement; Integraler Bestandteil der internen Publikationen und Vortragsreihen der LVAk [3]-[6]

[8] CEN-CENELEC-ETSI Smart Grid Coordination Group: Smart Grid Reference Architecture, Document for the M/490 Mandate, Version 3.0, 2012

[9] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standards 100-1 bis 100-4, 2008, aktuelle Version erhältlich unter https://www.bsi.bund.de/

[10] Bundesamt für Sicherheit in der Informationstechnik: Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen (BSI-CC-PP-0073), Version 1.2, 2013

[11] Bundesamt für Sicherheit in der Informationstechnik: Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen (BSI-CC-PP-0077), Version 1.0, 2013

FP7 project EURACOM, http://www.eos-eu.com/?Page=euracom

**Autoren**

**Johannes Göllner, Christian Meurers, Andreas Peer**
Bundesministerium für Landesverteidigung und Sport, Roßauer Lände 1, 1090 Wien

**Lucie Langer**
AIT Austrian Institute of Technology GmbH, Safety & Security Department, Donau-City-Straße 1, 1220 Wien

**Markus Kammerstetter**
Technische Universität Wien, Institute of Computer Aided Automation, Treitlstraße 1-3, 1040 Wien

# 3. DGI-Konferenz und 66. Jahrestagung der DGI

## 3. DGI-Konferenz und 66. Jahrestagung der DGI

*Informationsqualität und Wissensgenerierung*
Frankfurt am Main, 08.08.-09.05.2014

Die 3. DGI-Konferenz trägt den Titel "Informationsqualität und Wissensgenerierung". Thema sind die rasanten Veränderungen durch neue innovative Verfahren und Werkzeuge in den offenen Informationsarchitekturen des WWW und die immer dringlicher werdenden Fragen nach dem Nutzen dieser Innovationen, ihre Auswirkungen auf Qualität und die dabei maßgeblichen Standards. Bieten sie tatsächlich auch einen qualitativen Mehrwert oder kompensieren sie ihre leichte Verfügbarkeit und Erzeugbarkeit mit deutlichen Schwächen in der Qualität der Dienstleistungen und Produkte? Tragen Sie dazu bei, aus Informationen Wissen zu generieren, oder reduzieren Sie den Informationsgehalt zugunsten verkürzter oder subjektiv pointierter Darstellung? Welche Verfahren stehen uns zur Verfügung, diese Fragen anzugehen? Welche Kriterien und Maßstäbe sind angemessen, qualitative Aspekte zu bewerten? Können unterschiedliche Evaluationskriterien zugelassen werden, um unterschiedlichen Informations-, Kommunikations- und Wissensquellen gerecht zu werden?

Deutsche Gesellschaft für Information und Wissen e.V. (DGI)
Windmühlstraße 3
60329 Frankfurt am Main
Telefon: +49 (0)69 4303-13
Telefax: +49 (0)69 4909096
E-Mail: mail@dgi-info.de
http://www.dgi-info.de

Das folgende peer-reviewed Paper wurde im Tagungsband veröffentlicht:

Ockenfeld, Marlies (Hrsg.): Informationsqualität und Wissensgenerierung, 3. DGI-Konferenz / 66.Jahrestagung der DGI, Frankfurt am Main, 8. - 9. Mai 2014, Proceedings,DGI: Frankfurt am Main,2014, S. 65-84. ISBN 978-3-925474-73-6

Die freundliche Genehmigung zur Veröffentlichung in diesem Band wurde durch die DGI am 06.08.2014 erteilt.

# Von der Dokumentation zum organisationalen Wissens-PerformanceSystem

*Klaus Mak, Christian Meurers, Johannes Göllner, Robert Woitsch*

**Abstract:** „Von der Dokumentation zum organisationalen WissensPerformanceSystem" beschreibt die Entwicklung einer Dokumentationseinrichtung und ihren Hauptaufgaben in Zusammenhang mit den notwendigen Schritten zu einem operativen Unterstützungselement für ein Unternehmen. Die Steuerung durch Wissen als „Idee" im Hintergrund leitete mehrere Jahre Entwicklungs- und Forschungstätigkeit im Bereich des Dokumentations- und Fachinformationswesens und des Wissensmanagements in der Zentraldokumentation („ZentDok") der Landesverteidigungsakademie. Neben den durchzuführenden Arbeiten des praktischen Dokumentations- und Fachinformationswesens im gesamten Unternehmen, wurde auch ein F&E-Bereich kontinuierlich in der Organisation aufgebaut und etabliert.

Die Ergebnisse dieses Beitrages entstanden somit aus mehr als vierzig Jahren praktischer Erfahrung in der Organisation, wie auch aus unterschiedlichsten Projekten mit Partnern aus der Industrie und der Forschung[1].

Der Beitrag beschäftigt sich zunächst mit dem organisatorischen Hintergrund und der zugrundeliegenden WM-Strategie im ÖBH. In weiterer Folge wird der konzeptuelle Hintergrund und der theoretische Ansatz sowie das entwickelte Referenzarchitekturmodell vorgestellt, bevor anhand eines durchgeführten Projektes zur Erstellung einer Forschungsbilanz für das ÖBH die praktische Umsetzung beschrieben wird.

**Keywords:** Dokumentation Wissensmanagement Wissensperformancesystem Wissensbilanz Fachinformation Wissensentwicklung Prozessmanagement Referenzarchitektur

[1] Die detaillierten Inhalte des Papers sind im Rahmen der Schriftenreihe der Landesverteidigungsakademie publiziert worden und bei Bedarf verfügbar. (Woitsch, Mak & Göllner 2010; Woitsch et.al. 2010a)

## 1. Einleitung

Organisatorisch entwickelte sich die ZentDok bis 2013 zu einem Instrument für Unterstützungs- und Dienstleistungen sowie Anwendungsentwicklungen für das Österreichische Bundesheer (ÖBH) in den Bereichen: Dokumentation, Fachinformation, Wissensmanagement und Wissensentwicklung.

Diese Aufgaben sind für alle Unternehmensbereiche abzudecken und mit Erstellung von Konzepten, Bereitstellung von Open Source Content, Entwicklung von Verfahren und Methoden, sowie Werkzeugen zur Wissensentwicklung, aber auch bei der Fähigkeitenentwicklung der Mitarbeiter, sicherzustellen.

Ausgangspunkt dabei ist nicht nur ein pragmatischer Zugang zu den Begrifflichkeiten sondern parallel dazu die Entwicklung von anwendbaren Vorgangsweisen, Methoden und Werkzeugen, die in Pilotprojekten in unterschiedlichsten Unternehmensdomains entwickelt und getestet sowie bereits in Teilorganisationen eingeführt wurden.

Nachfolgend wird der Begriff Wissen als erforderlicher „Wert" in allen Ausprägungsformen implizit oder explizit als eine zentrale Ressource definiert und durch heuristische Modelle für die jeweiligen Anforderungen in den Geschäftsprozessen analysiert, modelliert und dokumentiert.

Wissen ist die Voraussetzung für eine Handlung oder Nichthandlung in einem System oder einer Domain. Wissen sind somit „interpretierte Daten oder Informationen", die in einem Entscheidungsprozess „Gewissheit" gleichzeitig schaffen müssen. Daten und Information sind in sich nicht zu Interpretation fähig.

Die Grenzen der Vollständigkeit und Richtigkeit der Informationen sind neben mangelhafter Interpretationsleistung und Zeitmangel bestimmend für die Höhe des Risikos, der Chancen und der (Un-)Sicherheit der (Nicht-)Entscheidung!

Die erforderliche „Interpretationsleistung" oder „Relevanzprüfung" muss

von einer „Entscheidungsinstanz“ geleistet werden. Diese „Entscheidungsinstanz“ kann ein Mensch oder eine Maschine sein, wobei „implizites Wissen“ durch Fähigkeiten des Menschen/der Rolle überprüft werden und unter anderem aus Daten, Informationen, Dokumenten, Intuition, Erfahrung, Erkenntnissen usw. generiert worden sein kann.
„Explizites Wissen“ muss ebenfalls geprüft in das System gebracht werden und Content muss durch Context-Informationen mit Mehrwert zum „Dokument“ transformiert werden.

Das „Dokument“ ist damit das system- oder domainrelevante Wissensobjekt. Dabei kann es sich um Text, Ton-, Bild-, Multimedia-, u. a. -inhalte und deren Beziehungen und Muster (Systeme, Domains, Lagebilder, etc.…) handeln.

In der Wissensentwicklung stellen alle unternehmerischen Entscheidungsprozesse ähnliche Herausforderungen in unterschiedlichsten Konstellationen und Intensitäten für die Mitarbeiter der ZentDok dar. Nachfolgende Darstellung stellt dies generisch - ohne Anspruch auf Vollzähligkeit - dar.


Abbildung 1 – Generischer Blick auf die Wissensentwicklung

Ziel ist es, durch Fachinformation, Dokumentation, Wissensmanagement und Wissensentwicklung eine kontinuierliche Steigerung der Potentiale zur Erhöhung der Handlungsfähigkeit des gesamten Unternehmens zu erreichen. Der Rahmen der Fähigkeiten des ursprünglichen „Dokumentars" erweiterte sich in den letzten Jahren rasant und dieser entstand aus dem Bedarf der zu unterstützenden Unternehmensbereiche.

## 2. Voraussetzungen im Unternehmen

Alle Voraussetzungen zur Steuerung eines unternehmensweiten WM-Systems sind fundierte theoretische Grundlagen sowie ein generisches Rahmenwerk. Dies wird mit dem Konzept „Wissensmanagement im ÖBH" (BMLVS 2008), einem operativen Querschnittskonzept, auch dezidiert ausgewiesen.

Dadurch ergibt sich die Bedeutung für alle organisatorischen Hauptgeschäftsfelder wie Einsatz, Lehre und Forschung einschließlich der Betriebsführung in allen Ebenen und Teilbereichen der Organisation.

Der Fokus liegt dabei auf den Einsatzerfordernissen, die zielgerichtet durch WM-Tätigkeiten unterstützt werden. Ein besonderes Augenmerk muss daher auf die Verknüpfungsmöglichkeiten zwischen allen entscheidenden Organisationsbereichen und deren Abhängigkeiten gelegt werden. Wissensmanagement als Enabler (vgl. Cuviello 2009) von „Interoperabilität" nimmt dabei eine wesentliche einsatzrelevante Unterstützungsaufgabe wahr.

Die Wissensmanagement Vorgehensweise basiert auf dem BPMS Paradigma (vgl. Karagiannis 1995). Genau wie im BPMS Paradigma werden fünf Phasen für modellunterstütztes Wissensmanagement definiert und vier Anwendungsszenarien realisiert, die zur unterschiedlichen Zielerreichung beitragen.

(1) Die Wissensbasierte Produktstrategie ermöglicht die Steuerung des Wissensmanagementsystems aus einer strategischen Produktsicht mit Werkzeugen ähnlich der Balanced Scorecard oder der Wissensbilanz.

(2) Die Wissensbasierten Geschäftsprozesse ermöglichen die Ausrichtung des Wissensmanagements auf die Geschäftsprozesse hin, um diese direkt oder indirekt zu unterstützen. Dabei werden Werkzeuge wie Workflows, Process-Steppers oder Geschäftsregeln verwendet.

(3) Die Wissensbasierte Organisation ermöglicht die Ausrichtung des Wissensmanagements auf die Mitarbeiter und die Organisation hin. Dabei werden Werkzeuge wie Skill-Management, Skill-Profile und Ausbildungsszenarien eingesetzt.

(4) Die Wissensbasierte Infrastruktur verbindet Wissensprodukte mit den Bedarfsträgern, indem die Infrastruktur wie Internet, Datenbanken oder Dokumentenmanagement-Systeme mittels Wissensmanagementprozessen verbunden werden.

## 3. WM-Strategie

In Anlehnung an den Begriff der Strategie in einer Organisation kann die WM-Strategie wie folgt definiert werden:

Eine WM-Strategie verfolgt das Ziel, Wissensmanagement in einer Organisation dauerhaft lebensfähig und auf die Geschäftsziele ausgerichtet zu integrieren. Ziel ist es, bestehendes Wissen so lange wie möglich nutzbar zu machen, zu erhalten sowie rechtzeitig zukünftige Potentiale aufzubauen.

Dazu werden fünf Dimensionen als Grundgerüst für die Erstellung einer unternehmensbezogenen WM-Strategie angenommen. (vgl. PROMOTE 2001; vgl. Knowledge Research 2002)

**Dimension 1**: Wissensstrategie als Geschäftsstrategie (vgl. WIEM 2009)
Dieser Blickwinkel konzentriert sich auf das Bereitstellen von qualitätsgesichertem und zeitgerechtem Wissen in der täglichen Arbeit des Wissensarbeiters. Durch die Kopplung von Geschäftsprozessen – die ja die Unternehmensziele unmittelbar ermöglichen – und dem Wissensmanagement, wird der Output des Wissens direkt oder indirekt an den Ergebnissen des Geschäftsprozesses gemessen. Daher werden folgende WM-Aktivitäten besonders gefördert: das Erzeugen, Verteilen, Dokumentieren, Speichern,

Erneuern und Nutzen von geschäftsprozessrelevantem Wissen. Dieser Blickwinkel betrachtet daher die Effektivität des Wissensmanagements.

**Dimension 2**: Immaterielles Vermögen (vgl. Nemetz 2006)
Dieser Blickwinkel legt das Schwergewicht auf das Wissen in Form von immateriellem Vermögen in einer Organisation. Das immaterielle Vermögen kann explizit in Form von Patenten, Technologien, Methoden, Beziehungen oder anderen strukturieren Wissensformen auftreten. Dadurch wird der Wert des Wissens im Unternehmen gesichert und ermöglicht eine Marktdifferenzierung. Daher werden folgende WM-Aktivitäten besonders gefördert: das Erkennen, Schützen, Dokumentieren, Speichern und Vermarkten von Wissen. Dieser Blickwinkel betrachtet daher die Sicherstellung des Wissens.

**Dimension 3**: Persönliches Wissensmanagement (vgl. PKM 2009)
Dieser Blickwinkel fokussiert auf den eigentlichen Wissensträger, den Mitarbeiter, der für die Generierung, Erneuerung und Nutzung des Wissens in den Anwendungsbereichen verantwortlich ist. Ziel ist die Entwicklung und Unterstützung von unternehmensrelevanten
Wissensträgern, indem Eigenverantwortung, Arbeitsklima, Weiterentwicklung sowie die individuelle Vernetzung gefördert werden. Dabei stehen folgende WM-Aktivitäten besonders im Mittelpunkt: das Fördern und die Weiterbildung von Mitarbeitern, Übertragen von Eigenverantwortung, geeignete Team- und Gruppenbildung, sowie das Fördern von Netzwerken. Dieser Blickwinkel betrachtet daher den Wissensträger und seine Entwicklung als zentrale Wertschöpfung.

**Dimension 4**: Innovationsstrategie
Dieser Blickwinkel betrachtet die ständige Weiterentwicklung eines Unternehmens durch die Erzeugung von neuem Wissen. Dabei werden eine Technologiefrüherkennung sowie eine Technologieführerschaft angestrebt, um diesen Technologievorsprung in weiterer Folge durch Differenzierung zu einem Wettbewerbsvorteil umzuwandeln. Daher werden folgenden WM-Aktivitäten besonders berücksichtigt: die Grundlagenforschung, die angewandte Forschung, die experimentelle Entwicklung, das ständige Prototyping sowie die Weiterentwicklung aufgrund von Lessons Learned oder ähnlicher Instrumente. Dieser Blickwinkel betrachtet vor allem die zukünftige Wettbewerbsfähigkeit des Unternehmens.

**Dimension 5**: Wissenstransfer
Dieser Blickwinkel beobachtet den Wissenstransfer sowie die Dokumentation und Archivierung von Wissen. Im Zentrum der Aktivitäten stehen die zielgerichtete Verteilung und die dafür notwendige Transformierung des Wissens in eine Form, die für Adressaten notwendig ist. Daher werden folgende WM-Aktivitäten besonders berücksichtigt: das Organisieren, Umstrukturieren, Dokumentieren, Verteilen, Übersetzen und Anwenden des Wissens. Dieser Blickwinkel betrachtet daher die Effizienz des Wissensmanagements.

In Abhängigkeit der Gesamtunternehmensstrategie, die zuerst expliziert in Vision, Mission und Strategie sowie weiterführender Strategiewerkzeuge abgebildet werden sollte, können obige fünf Dimensionen entweder für sich alleine oder in unterschiedlich gewichteten Kombinationsmöglichkeiten verwendet werden, um eine für das Unternehmen relevante WM-Strategie zu definieren.

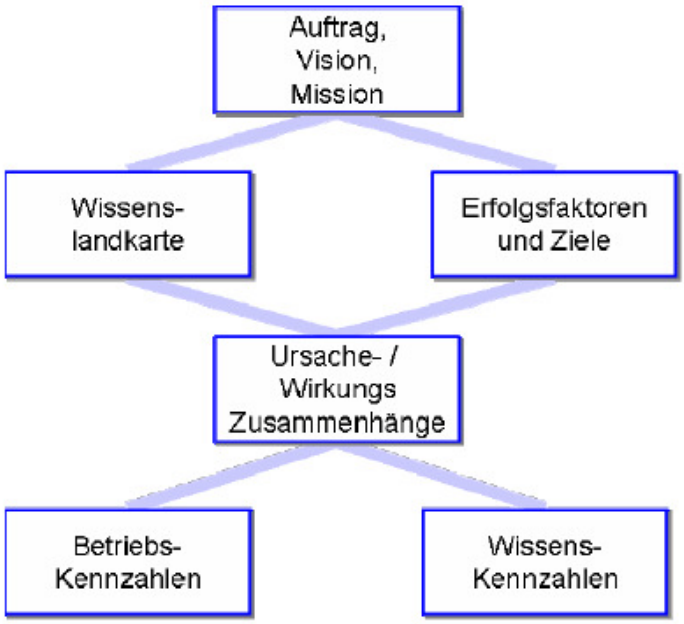



Abbildung 2 – Kernelemente der WM-Strategie

Strategisches Wissensmanagement ist daher ein Prozess, welcher

1) die Formulierung der Ziele,
2) deren Umsetzung sowie
3) laufende Überprüfung und Anpassung des WM-Systems liefert.

Es gilt dabei, sowohl externe Chancen und Risiken als auch interne Stärken und Schwächen zu berücksichtigen und Entscheidungen mit Zukunftswirkung zu treffen.

Kernfragen sind daher:

4) Welches Wissen ist für den heutigen Geschäftserfolg relevant?
5) Wie kann das Wissen für den zukünftigen Geschäftserfolg zur Verfügung gestellt werden?
6) Wie muss sich die Organisation weiterentwickeln, damit sie auch in Zukunft über das erforderliche Wissen verfügt, um lebensfähig und profitabel zu bleiben?

Um diese Fragen konkret und detailliert beantworten zu können, muss sich eine strategische Analyse regelmäßig mit dem Umfeld der Organisation auseinandersetzen, also insbesondere mit

a) den Bedürfnissen der Bedarfsträger
b) mit dem Umfeld, welches das Wissen für die Organisation maßgeblich bestimmt.

## 4. Konzeptueller Hintergrund

Das Konzept einer Wissensbilanz muss abgestimmt auf das vorhandene Betriebs- Organisations-Modell entwickelt werden. Alle in Anwendung stehenden betriebswirtschaftlichen Methoden und Instrumente müssen in der Erstellung der Wissensbilanz nicht nur berücksichtigt, sondern auch integriert werden.

Die Prozessqualität spielt dabei eine zentrale Rolle. Dadurch wird das Zusammenwirken von Auftrag, den geforderten Fähigkeiten der Organisation, ihrer organisatorischen und strukturellen Entwicklung, den Kosten sowie Qualitäten der Leistungserbringung über konkrete Ergebnisse abbildbar.

Aus der Mission, Vision und den strategischen Zielen sowie ergänzenden strategischen Dokumenten wie Leitbild, Konzept oder SOLL-Profil können konkrete Fähigkeiten der Organisation und Kompetenzen der Mitarbeiter samt den dazu notwendigen Produkten abgebildet werden.

Um konkret Daten aus der jeweiligen Organisation zu generieren, können alle zur Verfügung stehenden betriebswirtschaftlichen Methoden und Instrumente des Controllings und des Qualitätsmanagements angewendet werden.

Zum Beispiel:

- Prozessmanagement
- Balanced Scorecard
- Qualitätsmanagement
- Assessment Frameworks
- Kosten- und Leistungsrechnung
- Kontinuierlicher Verbesserungsprozess (KVP)
- Produktlandkarte
- Wissensprozesslandkarte

Als Darstellungsform der Organisationsumgebung in den vier Sichtweisen des Wissensbilanzrahmenwerkes ergibt sich die „Idee“ eines generischen Performance-Frameworks.

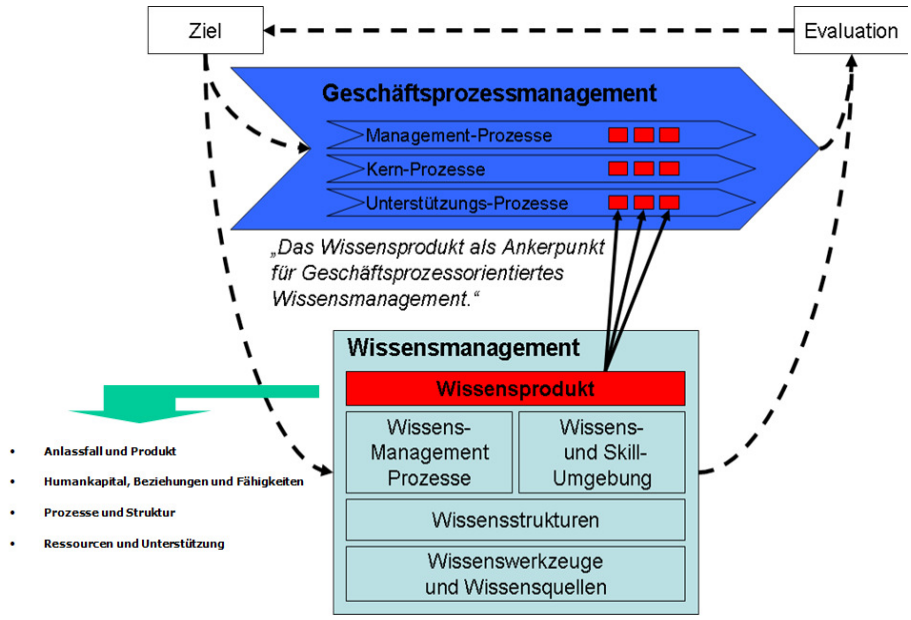



Abbildung 3 – „Idee" einens generischen Performance-Frameworks

Eine Wissensbilanz ist ein Instrument zur gezielten Darstellung sowie Entwicklung des Intellektuellen Kapitals (IK) (Woitsch et.al. 2010b) einer Organisation. Sie zeigt die Zusammenhänge zwischen den organisationalen Zielen, den Geschäftsprozessen, dem Intellektuellen Kapital und dem Geschäftserfolg einer Organisation auf und beschreibt diese Elemente mittels Indikatoren (vgl. BMWA 2008).

Mit der Wissensbilanz werden folgende direkte Nutzenkategorien erreicht (Bornemann&Reinhardt 2008):

1. Höhere Wettbewerbsfähigkeit und weniger Risiko,
2. Bessere Nutzung der immateriellen Vermögenswerte,
3. Klare strategische Ausrichtung.

Die Wissensbilanz zeigt einerseits die Zusammenhänge zwischen den organisationalen Zielen, den Prozessen, dem Intellektuellen Kapital und dem

Erfolg von wissensbasierten Organisationen auf. Andererseits generiert die Wissensbilanz auch Kenngrößen für strategische Entscheidungen und Potentiale. Diese Indikatoren werden, besonders wenn sie sensible Informationen und Daten enthalten, vorrangig für interne Organisationszielgruppen verwendet.

### *4.1 Referenzmodell/-architektur*

Das Referenzmodell basiert auf der Analyse von existierenden Wissensbilanzen, dem Balanced Scorecard Ansatz sowie vorhandenen Instrumenten der Betriebsorganisation.
Dieses Referenzmodell unterscheidet vier Perspektiven:

1. Anlassfall und Produkt Perspektive: Ziele, Kennzahlen, Vorgaben und Maßnahmen in Bezug auf Anlassfälle, Produkte sowie das wahrgenommene Ergebnis
2. Prozesse und Struktur Perspektive: Ziele, Kennzahlen, Vorgaben und Maßnahmen in Bezug auf Kernprozesse, qualitätsrelevante Prozesse sowie führungs- und qualitätsrelevante Prozesse.
3. Humankapital, Beziehungen und Fähigkeiten-Perspektive: Ziele, Kennzahlen, Vorgaben und Maßnahmen in Bezug auf Personen (Humankapital), sowie Fähigkeiten und Beziehungen (Beziehungskapital).

Ressourcen und Unterstützungs-Perspektive: Ziele, Kennzahlen, Vorgaben und Maßnahmen in Bezug auf Budget, Infrastruktur (Strukturkapital), Material und Gerät, sowie Information und Kommunikation. (vgl. HESIG 2008)

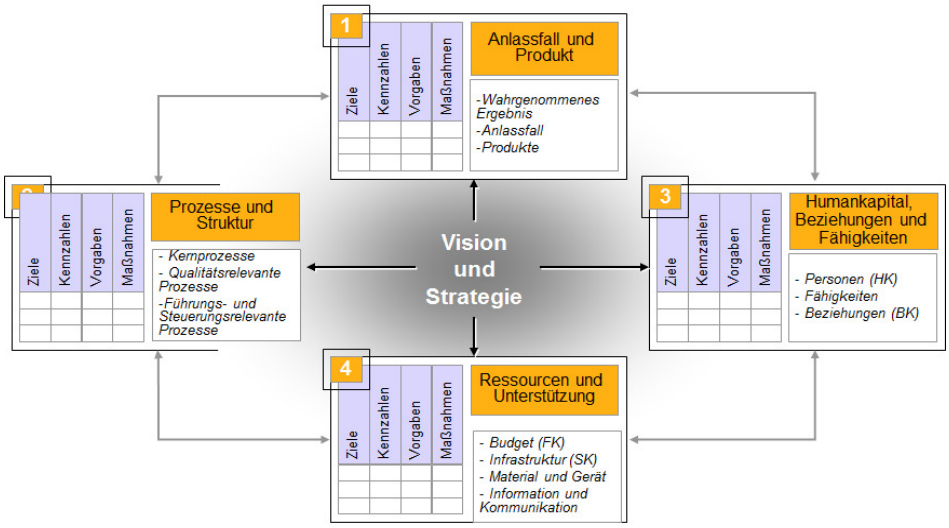


Abbildung 4 - PROMOTE®-Sichtweisen einer Wissensbilanz

Zur verfahrenstechnischen und somit nachvollziehbaren und qualitätsgesicherten Umsetzung von Wissensmanagement haben sich modellorientierte Ansätze als vorteilhaft erwiesen.

Ziel dieses Abschnittes ist es die Modellierung von Wissensmanagement vorzustellen und das PROMOTE® Referenzmodell (Mak, Göllner, Meurers & Utz 2010; Hinkelmann, Karagiannis & Telesko 2002) anzubieten. Nachdem die Strategie des Wissensmanagements definiert worden ist und die Veränderung des derzeitigen Systems vorgegeben ist, wird das WM-System geplant.

Das Wissensmanagement hat den Geschäftsprozess direkt oder indirekt zu unterstützen. Um ein eindeutiges und in der Praxis handhabbares Werkzeug für die Kopplung von Geschäftsprozessen und Wissensmanagement zur Verfügung zu haben, wird hier der Begriff „Wissensprodukt“ eingeführt.

Wissensprodukte sind die Ergebnisse aus dem Wissensmanagement, die im Geschäftsprozess verwendet werden. Das hier vorgestellte Referenzmodell beschreibt, wie Wissensprodukte hergestellt werden.

Die Wissensprodukte werden vom WM-System aus an das Unternehmen angeboten. Sie werden in Informationsprodukte, Beratungsprodukte und Anwendungsprodukte unterteilt. Sie werden zum Triggern von Prozessen, bei der Durchführung von Aktivitäten oder beim Treffen von Entscheidungen von den Wissensarbeitern genutzt.

Informationsprodukte stellen explizite Informationen zur Verfügung, die von einem Mitarbeiter verarbeitet wird. Darunter fallen Handlungsanleitungen, Dokumente, Bücher, Richtlinien, Protokolle, schriftlich festgehaltene Regeln, Präsentationen, Filme, Datenbankabfragen oder ähnliches.

Beratungsprodukte stellen implizites Wissen zur Verfügung und können daher nur von einem Mitarbeiter zu einem anderen Mitarbeiter weitergegeben werden. Darunter fallen Auskünfte, Beratungen, Moderationen, das Abhalten von Kursen, periodische Besprechungen oder ähnliches.

Anwendungsprodukte stellen explizites Wissen zur Verfügung, die von Softwareprogrammen verarbeitet werden. Darunter fallen Entscheidungsunterstützungssysteme, Workflowsysteme, automatische Textanalysesysteme, Suchmaschinen oder Ähnliches.

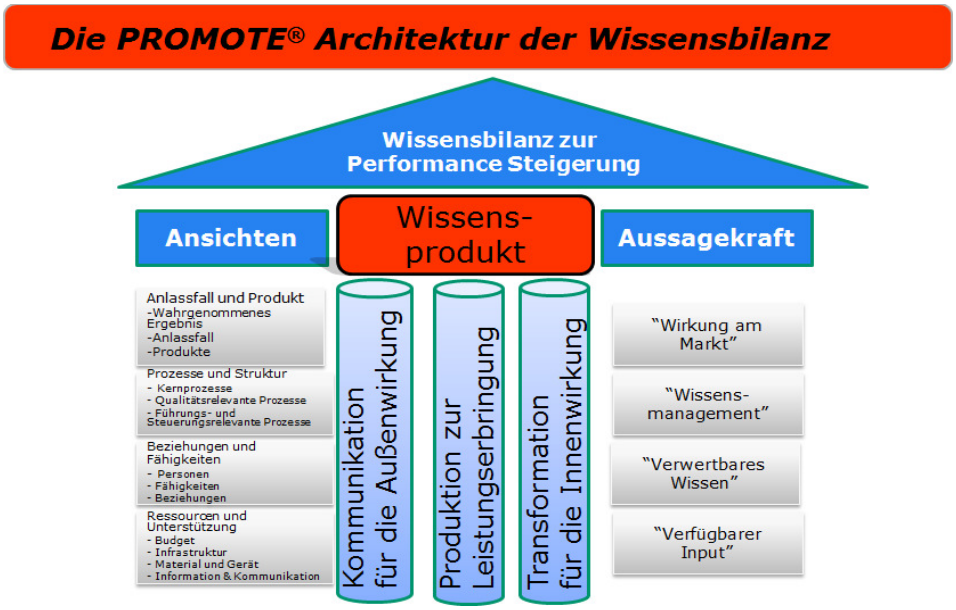


Abbildung 5 - PROMOTE® Referenzarchitektur einer Wissensbilanz

Das WM-System baut im Wesentlichen auf den drei Säulen

a) Kommunikation,
b) Produktion und
c) Transformation

auf.

Die Kommunikation bezieht sich dabei auf die Außenwirkung am Markt, Produktion bezieht sich auf die Leistungserbringung und Transformation auf die Innenwirkung. Diese drei Säulen werden in vier unterschiedlichen Sichtweisen (Perspektiven) betrachtet.

Ausgangspunkt für die erste Sichtweise ist das Produkt selbst und die Analyse seiner Wirkung am Markt. Die zweite Sichtweise sind Prozesse und Strukturen, somit wird das Wissensmanagement der Organisation analysiert. Die dritte Perspektive bilden Humankapital, Beziehungen und Fähigkeiten der Organisation, somit wird das verwertbare Wissen analysiert. Die vierte Sichtweise sind Ressourcen und Unterstützungen wie Kapital, Infra-

struktur, Material und Gerät sowie Information und Kommunikation, somit wird der verfügbare Input analysiert. Anhaltspunkte für das Referenzmodell liefern die so genannten Wissenscodes aus dem EU-Projekt MATURE (MATURE 2010). Codes sind Beschreibungen von Wissenstätigkeiten, welche der Referenzarchitektur für das Wissensmanagementsystem zugeordnet werden können, wobei kein Anspruch auf Vollzähligkeit besteht. Sie bieten Anhaltspunkte in der Referenzarchitektur um Wissensarbeit beschreiben zu können und haben somit beispielhaften Charakter.

Die Wissensarbeit in Kommunikation, Produktion und Transformation in der Produktebene ist abhängig vom jeweiligen Unternehmensziel und individuell anzupassen.

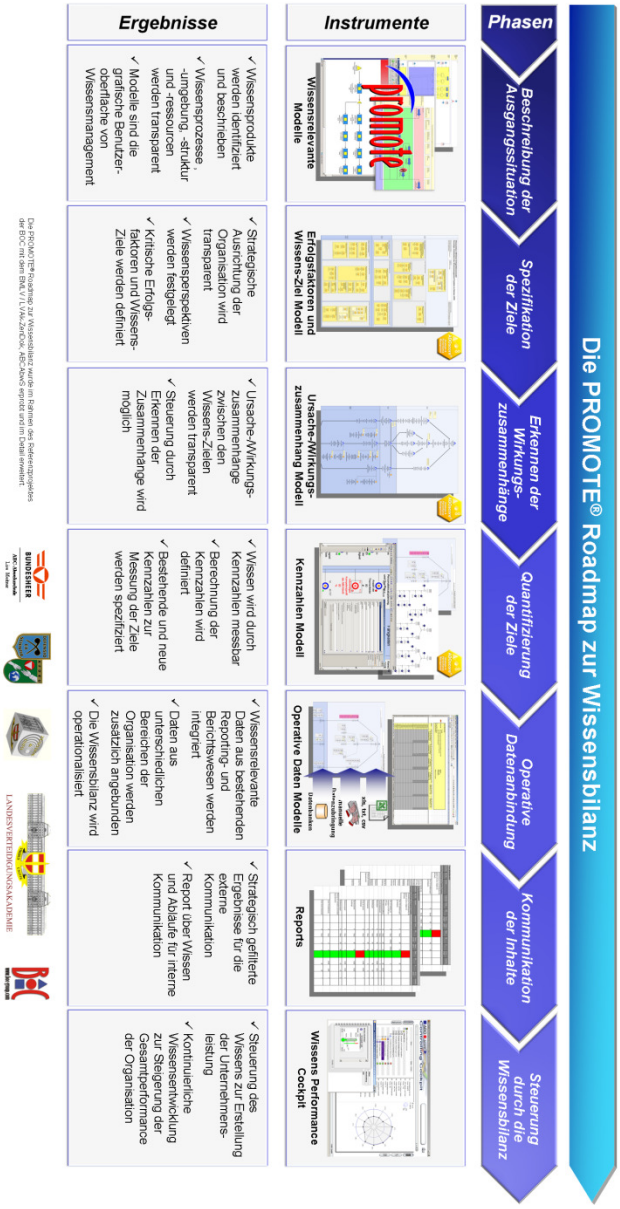



Abbildung 6 - RoadMap zur Erstellung der Wissensbilanz

**Beschreibung der Ausgangslage**
Bevor mit der Erstellung der Wissensbilanz begonnen werden kann, muss im ersten Schritt die Ausgangssituation beschrieben werden. Dabei gilt es die Wissensorganisation zu analysieren und die für die Steuerung relevanten Teile der Organisation zu spezifizieren. Die Abbildung mittels Modellen ermöglicht nicht nur komplexe Zusammenhänge durch die Modellsprache einfach und graphisch darzustellen, sondern unterstützt auch die Analyse einer Wissensorganisation durch ein formales und strukturiertes Vorgehen. Es muss zuerst ein Überblick über das vorhandene Wissensmanagement gegeben werden, um anschließend im Detail verschiedene Wissensaspekte genauer analysieren zu können.

**Spezifikation der Ziele**
Zur Ableitung der Ziele werden zuerst die Zielgruppen der Wissensbilanz erhoben. Pro Zielgruppe werden der Zweck der Wissensbilanz, die Qualität der Berichte, sowie der Berichtszyklus festgelegt. Eine Tabelle ermöglicht einen Überblick über die Zielgruppen, den Zweck der Wissensbilanz für die jeweilige Zielgruppe sowie den Berichts- und Steuerzyklus. In einem weiteren Schritt werden die Einflussfakturen der Instrumente auf die Wissensbilanz identifiziert.

**Erkennen der Wirkungszusammenhänge**
Nachdem die kritischen Erfolgsfaktoren erarbeitet und zu Wissenszielen zusammengefasst wurden, erfolgt eine Analyse der Ursachen-Wirkungszusammenhänge. Die Ziele können in übergeordnete (strategische) und untergeordnete (operative) Ziele aufgeteilt werden. Ein untergeordnetes (operative) Ziel dient als Zwischenschritt zu einem übergeordneten (strategischen) Ziel. Die Aufteilung in übergeordnete und untergeordnete Ziele erfolgt daher aufgrund des zeitlichen Horizonts des Zieles, die direkte oder indirekte Auswirkung auf das Wissensprodukt oder die Anzahl der beeinflussenden Erfolgsfaktoren. Danach werden die Abhängigkeiten der Ziele basierend auf der Einschätzung von Experten definiert.

**Quantifizierung der Ziele**
Effektive Unternehmensdaten werden in Kennzahlen hinterlegt bzw. an Datenquellen angebunden. Kennzahlen beinhalten die aktuellen Werte, sowie Vergleichswerte (Soll-Werte) und Toleranzgrenzen. Die Plausibilität jeder Kennzahl wird durch kritisches Hinterfragen sichergestellt. Jede

Kennzahl wird durch den Bezugszeitraum, Maßeinheit, Begrenzungsart, Toleranzgrenzen, ihrer Funktion sowie der Art des Periodenwertes beschrieben. Großteils werden die Kennzahlen von bestehenden Systemen bereitgestellt, sodass eine plausible Integration bestehender Sichtweisen mit neuen Kennzahlen erarbeitet werden kann.

**Operative Datenanbindung**
Die Verknüpfung von Daten mit der Wissensbilanz erfolgt durch die Anbindung externer Datenquellen wie Datenbanken, DataWarehouse oder manuellen Dateneingaben mittels Excel an die jeweiligen Kennzahlen. Die verwendeten komplexeren Kennzahlen werden erst im Werkzeug auf Basis der verknüpften elementaren Daten berechnet. Diese werden zur Simulation der Kennzahlen vor der eigentlichen Cockpit-Generierung herangezogen, um die Plausibilität auf Indikatoren-Ebene überprüfen zu können.

**Kommunikation der Inhalte**
Nach der Modellierung der Wissensbilanz, der Anbindung der Daten sowie der Simulation können das Wissens-Performance-Cockpit sowie die Wissensbilanz-Berichte generiert werden. Das eingerichtete „Wissens-Performance-Cockpit" bietet weitreichende Controlling- und Analyse-Funktionen. Die Inhalte können anhand vielfältiger Darstellungs- und Filteroptionen aufbereitet werden. Zur Aufbereitung der Werte, der Ziele sowie der Kennzahlen, kann dabei das „traffic-light-coding" verwendet werden. Durch die Signalwirkung der Ampelfarben können positive und negative Entwicklungen frühzeitig erkannt und entsprechende Maßnahmen gesetzt werden. Über einen Navigationsbaum wird die Auswahl der gewünschten Perspektiven, Ziele oder Kennzahlen ermöglicht.

**Steuerung der Wissensbilanz**
Die Berichtsformen des Performance-Cockpits einer Wissensbilanz listen die Kennzahlen, ihre Zugehörigkeit zu den Sichten (Perspektiven), sowie die Wirkung auf Zielvorgaben auf. Neben einer Ampeldarstellung kann der Trend, sowie ein normierter Zielerreichungsgrad – Score – ausgerechnet und neben den wichtigsten Kennzahlenwerten dargestellt werden. Ein Performance-Cockpit ermöglicht ebenfalls umfangreiches recherchieren in den Detailbeschreibungen sowie in der Kennzahl-Zielabhängigkeit. Somit können Schwachstellen frühzeitig erkannt und die Auswirkungen auf die Ziele rechtzeitig beeinflusst werden.

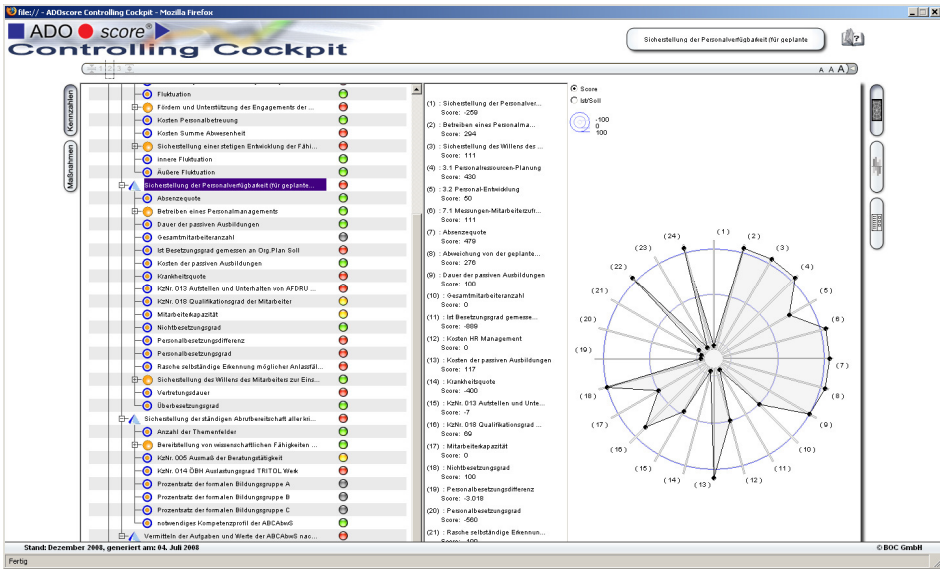



Abbildung 7 - Performance Cockpit

## 5. Umsetzung des Modells im Rahmen des Aufbaus eines Forschungsmanagementsystems

Auf Basis der oben vorgestellten entwickelten Referenzarchitektur wurde den konzeptionellen und strategischen Vorgaben, sowie dem Konzept „Forschung im ÖBH“ und dem operativen Querschnittskonzept „WM im ÖBH“ folgend im Rahmen eines internen Projektes die Wissensbilanz für das Forschungsmanagementsystem (FMS) im ÖBH erstellt (BMLVS 2010). Die dabei benötigten Ressourcen, Fähigkeiten, Prozesse, Strukturen für den Anlassfall „Forschungsbedarf“ wurden abgebildet und mit den verfügbaren „Forschungsressourcen“ verglichen. Dieses Monitoring gab einen Überblick über die Verfügbarkeit der Forschungsmanagement- und Forschungsdurchführungskompetenz in einer bestimmten Zeitperiode.

Zunächst wurde ein Übersichtsmodell in Form einer Wissenslandkarte generiert, in der die „Inputgeber“ und „Konsumenten“ der Forschung im ÖBH mit ihren Schnittstellen zum FMS abgegrenzt und die steuerungsrelevanten Teile der Organisation abgebildet wurden. Der Vision/Mission sowie den aus den strategischen Vorgaben für Forschung im ÖBH folgen-

den Strategie und Zielen wurde eine Forschungsprozesslandkarte entwickelt, die alle Kern- und Unterstützungsprozesse sowohl in Bereich der Steuerung und Management aber auch bei den forschungsdurchführenden Stellen abbildet.

Zur Spezifikation der Ziele wurden zuerst die Zielgruppen der Wissensbilanz erhoben. Pro Zielgruppe konnte dann der Zweck der Wissensbilanz, die Qualität der Berichte, sowie der Berichtszyklus festgelegt werden. Nach der Spezifikation der Ziele wurden die kritischen Erfolgsfaktoren identifiziert. Die Erfolgsfaktoren wurden im Zuge von Workshop-Sitzungen gesammelt und in weiterer Folge auf Plausibilität überprüft und angepasst. Bekannte Erfolgsfaktoren aus Referenzmodellen wurden dabei ergänzend zur Verfügung gestellt und integriert. Die Erfolgsfaktoren wurden den Perspektiven der Wissensbilanz (Anlassfall und Produkt- Perspektive, Prozesse und Struktur-Perspektive, Humankapital, Beziehungen und Fähigkeiten – Perspektive, Ressourcen und Unterstützungs-Perspektive), sowie den Säulen der Wissensbilanz (Kommunikation, Produktion, Transformation), zugeordnet. Durch diese Zuordnung ergab sich eine erste Gruppierung der Erfolgsfaktoren. Ähnliche Faktoren wurden zu strategischen Zielen aggregiert.

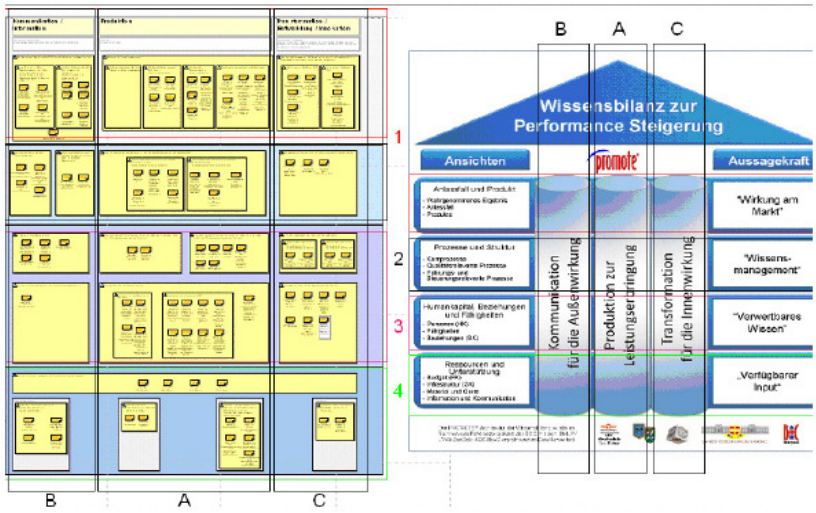



Abbildung 8 - Erfolgsfaktoren und deren Zuordnung zu den Säulen der Wissensbilanz

Auf Basis der erarbeiteten Ergebnisse wurden Ursachen- und Wirkungszu-

sammenhänge identifiziert und dargestellt und den strategischen Zielen operative Ziele zugeordnet. Die Erreichung eines Ziels wird dabei durch eine oder mehrere Kennzahlen gemessen. Anhand der Abhängigkeiten von Zielen sowie Kennzahlen, konnten Einflüsse zwischen den Faktoren aufgezeigt werden. Die folgende Abbildung zeigt einen Auszug aus dem Ursache- Wirkungsmodell:

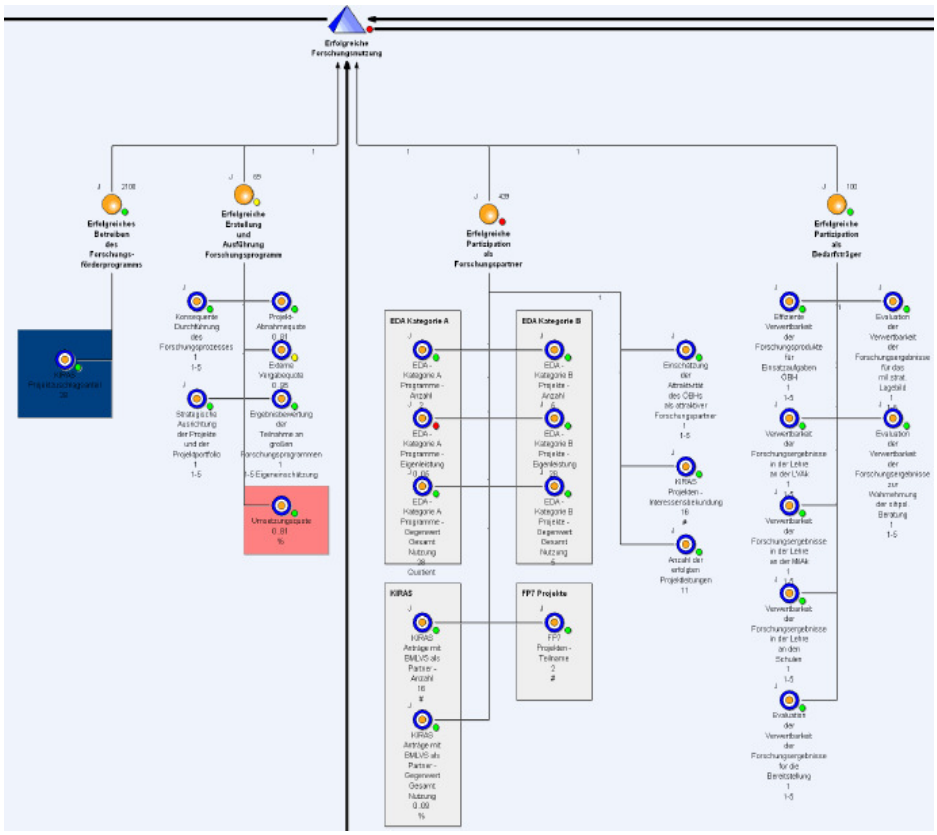



Abbildung 9 - Auszug aus dem Ursache-Wirkungsmodell

Gemäß der Roadmap wurden die Ziele quantifiziert und mit Kennzahlen hinterlegt. Die Kennzahlen wurden mit effektive Unternehmensdaten hinterlegt bzw. an Datenquellen angebunden. Kennzahlen beinhalten die aktuellen Werte, sowie Vergleichswerte (Soll-Werte) und Toleranzgrenzen. Die Plausibilität jeder Kennzahl wurde durch Bereitstellung und Analyse von Daten sowie kritisches Hinterfragen sichergestellt.

| Name | Bezugszeit-raum | Messgröße | Tolleranz-art | Begrenzungs-art | Toleranz grün / gelb | Toleranz gelb / rot | FDS / FMS |
|---|---|---|---|---|---|---|---|
| Abnahmequote Forschungsprojekte | Jahr | % | absolut | von unten | 0.2 | 0.28 | |
| Anpassungsmöglichkeit des FDS an den tatsächlich erkannten Bec | Jahr | 1-5 | absolut | von oben | 2 | 3 | |
| Anzahl der am FMS teilnehmenden Dienststellen | Halbjahr | % | absolut | von unten | 0 | 0.2 | |
| Anzahl der an FDS teilnehmenden Dienststellen | Halbjahr | % | absolut | von unten | 0 | 0.2 | |
| Anzahl der erfolgten Projektleitungen | Jahr | | absolut | von unten | 0 | 4 | |
| Anzahl der Informationsveranstaltungen für Externe | Jahr | # | absolut | von unten | 0 | 0 | |
| Anzahl der Informationsveranstaltungen für Interne | Jahr | # | absolut | von unten | 0 | 0 | |
| Anzahl der Kommunikationsprodukte | Quartal | # | absolut | von unten | 0 | 9 | |
| EDA - Kategorie A Programme - Anzahl | Jahr | # | absolut | von unten | 0 | 1 | |
| EDA - Kategorie A Programme - Eigenleistung | Jahr | % | absolut | beidseitig | 0 | 0.01 | |
| EDA - Kategorie A Programme - Gegenwert Gesamt Nutzung | Jahr | Quotient | absolut | von unten | 13 | 20 | |
| EDA - Kategorie B Projekte - Anzahl | Jahr | # | absolut | von unten | 0 | 1 | |
| EDA - Kategorie B Projekte - Eigenleistung | Jahr | € | absolut | von unten | 0 | 0 | |
| EDA - Kategorie B Projekte - Gegenwert Gesamt Nutzung | Jahr | | absolut | von unten | 0 | 0.06 | |
| Effiziente Verwertbarkeit der Forschungsprodukte für Einsatzaufga | Jahr | 1-5 | absolut | von oben | 2 | 3 | |
| Einschätzung der Attraktivität des ÖBHs als attraktiver Forschungs | Jahr | 1-5 | absolut | von oben | 1 | 3 | |
| Erfüllung aller Kennzeichen des funktionierenden Systems | Jahr | 1-5 | absolut | von oben | 2 | 3 | |
| Ergebnisbewertung der Teilnahme an großen Forschungsprogram | Jahr | 1-5 | absolut | von oben | 1 | 3 | |
| Evaluation der Mitwirkung an int. Forschungsprogramme | Jahr | 1-5 | absolut | von oben | 2 | 4 | |
| Evaluation der Mitwirkung an int. und nationalen. Forschungsgremi | Jahr | 1-5 | absolut | von oben | 2 | 3 | |
| Evaluation der Verwertbarkeit der Forschungsergebnisse für das m | Jahr | 1-5 | absolut | von oben | 2 | 3 | |

Abbildung 10 - Kennzahlen (Auszug)

Jede Kennzahl, sowohl quantitativ als auch qualitativ, wird durch den Bezugszeitraum, Maßeinheit, Begrenzungsart, Toleranzgrenzen, ihrer Funktion sowie der Art des Periodenwertes beschrieben. Großteils waren die Kennzahlen von bestehenden Systemen bereitgestellt, sodass eine plausible Integration bestehender Sichtweisen mit neuen Kennzahlen erarbeitet werden konnte.

Nach der Operativen Datenanbindung erfolgte die Kommunikation der Inhalte sowie die Steuerung durch die Wissensbilanz durch die Implementierung eines Wissens-Performance-Cockpits, das weitreichende Controlling- und Analyse-Funktionen bietet. Die Inhalte, Werte, Ziele und Kennzahlen können anhand vielfältiger Darstellungs- und Filteroptionen aufbereitet werden. Dazu wird beispielsweise das „traffic-light-coding" verwendet, das über die Darstellung von Ampelfarben und der damit verbundenen Signalwirkung positive und negative Entwicklungen frühzeitig erkennen lässt, sodass entsprechende Maßnahmen gesetzt werden können.

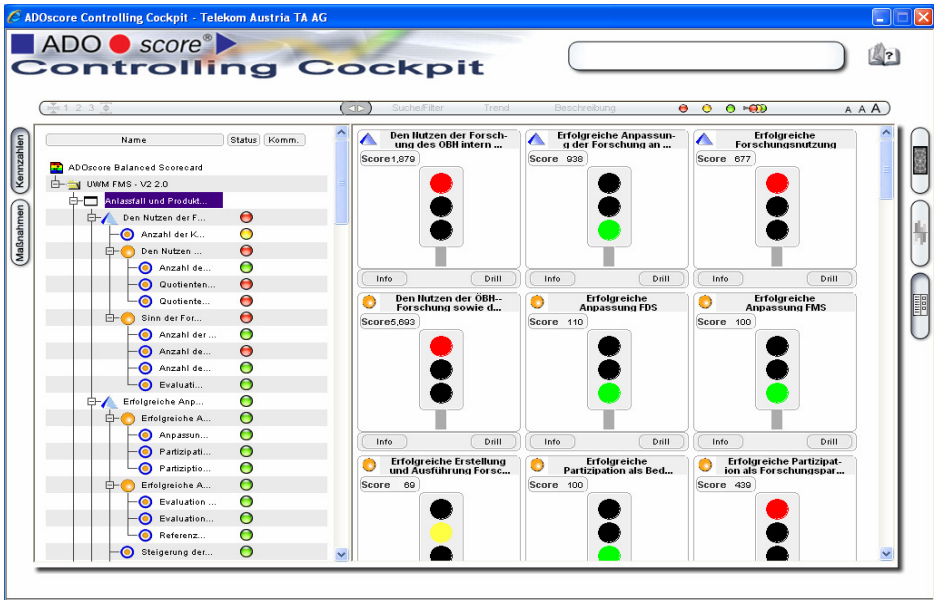



Abbildung 11 - Ampeldarstellung im Wissens-Performance-Cockpits

Der Navigationsbaum auf der linken Seite des Cockpits ermöglicht die Auswahl der gewünschten Perspektiven, Ziele oder Kennzahlen. Die Berichtsformen im Performance-Cockpit der Wissensbilanz listen die Kennzahlen, ihre Zugehörigkeit zu den Sichten (Perspektiven), sowie die Wirkung auf Zielvorgaben auf. Neben der Ampeldarstellung wird der Trend, sowie ein normierter Zielerreichungsgrad – Score – ausgerechnet und neben den wichtigsten Kennzahlenwerten dargestellt. Das Performance-Cockpit ermöglicht umfangreiches recherchieren in den Detailbeschreibungen sowie in der Kennzahl-Zielabhängigkeit. Somit können Schwachstellen frühzeitig erkannt und die Auswirkungen auf Ziele rechtzeitig beeinflusst werden.

| Kennzahlenübersicht | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Pers-pektive | Strat. Ziel | Kennzahl | Verantwortlich | Einheit | BZR | Toleranz grün/gelb | Toleranz gelb/rot | Status | Soll | Ist | Ist Vor-periode | Kommentar |
| Anlassfall und Produkt Perspektive | | | | | | | | | | | | |
| | Sinn der Forschung für das Unternehmen BH transparent, nachvollziehaber und Nutzbringend zu kommunizieren (OZ) | | | | | | | | | | | |
| | | Anzahl der Informationsveranstaltungen für Interne | | # | Jahr | 0..00 | 0..00 | | 1 | 2 | 2 | |
| | | Evaluation des Mehrwertes für beteiligte OrgEinheiten | | 1-5 | Jahr | 1..00 | 3..00 | | 1 | 1 | 1 | |
| | | Anzahl der am FMS teilnehmenden Dienststellen | | % | Halbjahr | 0..00 | 0..20 | | 1 | 0..60 | 0..59 | |
| | | Anzahl der an FDS teilnehmenden Dienststellen | | % | Halbjahr | 0..00 | 0..20 | | 0..80 | 0..80 | 0..79 | |
| | Den Nutzen der Forschung des ÖBH intern und extern zu kommunizieren | | | | | | | | | | | |
| | | Anzahl der Kommunikationsprodukte | | # | Quartal | 0..00 | 9..00 | | 15 | 8 | 7 | |
| | Den Nutzen der ÖBH-Forschung sowie die ÖBH-Leistungsfähigkeit als Forschungspartner und Forschungsbedarfsträger zu kommunizieren (OZ) | | | | | | | | | | | |
| | | Anzahl der Informationsveransta | | # | Jahr | 0..00 | 0..00 | | 1 | 2 | 2 | |

Abbildung 12 – Kennzahlenbericht

## 6. Abschliessende Betrachtung und Zusammenfassung

Im Zuge des vorgestellten Projektes als Anwendungsbeispiel konnten die Referenzarchitektur und die RoadMap zur Wissensbilanz validiert werden und der theoretische Ansatz praktisch umgesetzt werden. Im Zuge des Projektes traten aber auch klar die neuralgischen Punkte bzw. die kritischen Phasen des Referenzmodells zu Tage. So könnte sich die Abstraktion bzw. die Reduktion von Zielen und in weiterer Folge das Fehlen von eventuell wichtigen Ursache-Wirkungszusammenhängen für die Wissensbilanz als kritisch erweisen. Daher erfolgte die Umsetzung der einzelnen Schritte zur Erstellung einer Wissensbilanz bzw. eine Wissens-Performance-Cockpits teilweise in mehreren Iterationsschritten, in denen immer wieder Plausibilitätsprüfungen und Validierungen insbesondere von Zielen und Kennzahlen durchgeführt wurden. Die Kennzahlen können in jedem Segment des Ursache-Wirkungsmodells quantitativ oder qualitativ sein. Eine genaue Beschreibung des Kontextes der Steuerungsfunktionalität ist aber dezidiert erforderlich, um für die Führungspersonen gleiche Vorraussetzung in der Steuerung zu garantieren. Dies stellt über den gesamten Erstellungsprozess

der Wissensbilanz eine besondere Herausforderung, da hier die Grenzen des Systems sichtbar werden.

Eine weitere Problematik ist die Anbindung von Kennzahlen an Datenquellen. Für das vorgestellte Projekt waren alle relevanten Unternehmensdaten in verschiedenen Ausprägungen vorhanden und konnten in das System integriert werden. Diese Datenanbindung könnte allerdings in anderen Anwendungsbereichen nicht immer in dieser Form sichergestellt werden, man denke hier beispielsweise an klassifizierte Informationen, die aus dem simplen Grund der Unternehmenspolitik nicht in ein solches System eingebunden werden dürfen. Außerdem ist immer auf eine Validierung der den Kennzahlen hinterlegten Werte zu achten, da das Wissens-Performance-System sonst falsche Ergebnisse liefern kann.

Abschliessend konnte mit der praktischen Anwendung des vorgestellten theoretischen Ansatzes nicht nur dessen Tauglichkeit, sondern auch der Nutzen einer Wissensbilanz für eine Organisation unterstrichen werden. Die Management-Ebene erhält damit ein Instrument, das Vorgänge, Ressourcen und Prozesse transparent und nachvollziehbar macht und gleichzeitig die Grundlagen für ein Forschungscontrolling zur Betriebssteuerung und -planung, für die Entwicklung und Umsetzung der Organisationsfähigkeiten, zur Verbesserung der Planungssicherheit sowie der Entwicklung von effizienten und zielgerichteten Strategien in allen abgebildeten Bereichen schafft.

Durch dieses Rahmenwerk, ausgehend von bisherigen Arbeiten wie Studien und WM-Projekten, wurden fundierte Grundlagen geschaffen, um einen prototypischen Demonstrator „Wissensbilanz“ für das ÖBH oder für ausgesuchte Organisationseinheiten zu entwickeln. Damit ist die Möglichkeit zur Schaffung von transparenten Abläufen als Grundlage zur Steuerung in den Bereichen Einsatz, Lehre und Forschung u.a. als Grundlage für Bildungs- und Forschungscontrolling zur Betriebssteuerung und -planung, für die Entwicklung und Umsetzung der Organisationsfähigkeiten und zur Verbesserung der Planungssicherheit, gewährleistet.

Begleitend erfolgt eine Standardisierung der Fach-Terminologien und -Prozesse sowie Anpassung an die in Entstehung befindliche Wissensmanagement-Terminologie des ÖBH. Der Aufbau von Kompetenzen im

Umgang mit modernsten Managementinstrumenten und -methoden für Mitarbeiter des ÖBH sowie für Mitarbeiter in WM-Projekten, stellt eine wesentliche Wertsteigerung für die Organisation dar. Dieses Wissen ist Grundlage für die Weiterentwicklung des Wissensmanagements des ÖBH. Damit verbunden ist eine Steigerung der Reaktionsfähigkeit und Lernfähigkeit und somit eine wesentliche Erhöhung der gesamten Einsatzbereitschaft.

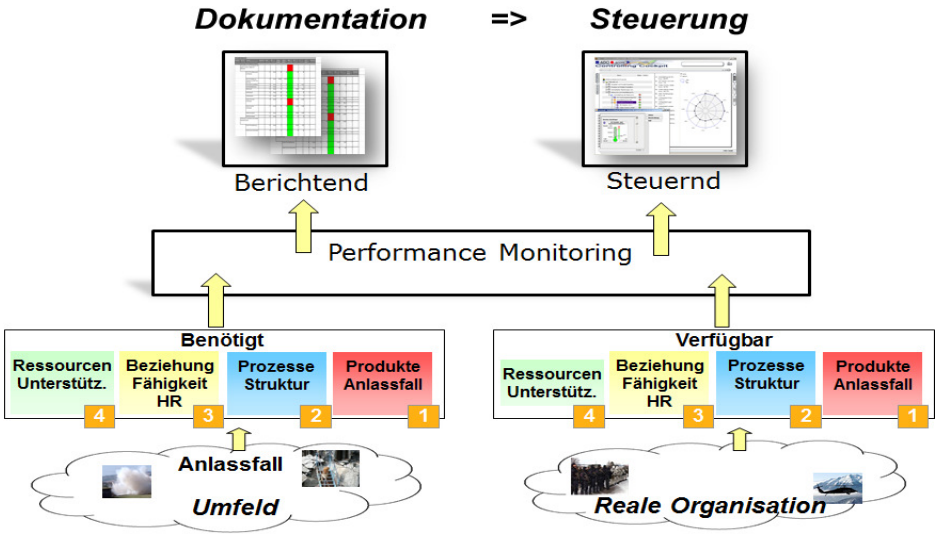



Abbildung 13 - Von der Dokumentation zur Steuerung

Die Dokumentation von Ursache- und Wirkungszusammenhängen von Komponenten einer Einsatzorganisation mittels vorgestellter Methodik kann umgesetzt werden. Die Transparenz aller Ressourcen der Organisation, insbesondere die des intellektuellen Wertes der Mitarbeiter, kann für alle Bereiche der Organisation beispielhaft abgebildet werden.

Die Kommunikation des Unternehmens über eine dynamische Performance-Darstellung könnte ebenso beispielgebend sein wie eine fundierte Organisations- und Personalentwicklung, basierend auf einer integrativen und historisch gewachsenen Bertachtungsweise der Organisation.

Für das Management ergibt sich außerdem die Möglichkeit des frühzeitigen

Erkennens von Wissensbedarf, der durch eine zielgerichtete Mitarbeiterentwicklungsstrategie effizient, rechtzeitig und nachvollziehbar abgedeckt werden kann. Für Kommandanten und Leiter ergeben sich Perspektiven für transparente Entscheidungseinflüsse auf die jeweiligen Führungsbereiche.

**Referenzen**


- BMLVS (2008), Wissensmanagement im ÖBH, Bundesministerium für Landesverteidigung und Sport, Wien, 2008
- BMLVS (2010), Mak, Hofmeister, Göllner, Woitsch, WM-Projekt Forschungsmanagementsystem (FMS) – ÖBH Modell: „Die Forschungsbilanz ÖBH", Wien, 2010
- BMWA (2008), Leitfaden Wissensbilanz – Made in Germany. Bundesministerium für Wirtschaft und Arbeit in Zusammenarbeit mit dem Arbeitskreis Wissensbilanz, URL:
- http://www.akwissensbilanz.org/Infoservice/Infomaterial/WB-Leitfaden_2.0.pdf [13.11.2013]
- Bornemann & Reinhardt (2008), Handbuch Wissensbilanz-Umsetzung und Fallstudien, ESVVerlag, Berlin, S. 13
- Cuviello (2009), Army Knowledge Management - The Interoperability Enabler, LTG, Army Chief Information Officer, US Army, Vortrag, [27.03.2009]
- Hesig (2008), Wissensbilanz – Made in Europe, Wissensmanagement – Das
- Magazin für Führungskräfte, Heft 4/2008
- Hinkelmann, Karagiannis & Telesko (2002), PROMOTE - Methodologie und Werkzeug zum geschäftsprozessorientierten Wissensmanagement. In: Geschäftsprozessorientiertes Wissensmanagement, Springer-Verlag
- Karagiannis (1995) BPMS: Business Process Management Systems: Concepts, Methods and Technologies, SIGOIS Special Issue, SIGOIS Bulletin 10-13, 1995
- Knowledge Research 2002, Verfügbar unter: http://www.knowledgeresearch.com/strategies.htm, [01.11.2002]
- Mak, Göllner, Meurers & Utz (2010), PROMOTE® in the Austrian Armed Forces: The Knowledge Management Processes in the De-

partment of Central Documentation and Information Service/National Defence Academy, 17th EKAW 2010 - Knowledge Engineering and Knowledge Management – Workshop OKM-Open Knowledge Model at the Gulbenkian Foundation, Lissabon, Portugal
- MATURE (2010), MATURE Projekt, "D1.1 Results of the Ethnographic Study and Conceptual Knowledge Maturing Model", URL: http://mature-ip.eu/files/deliverables/D1.1_Ethnographic_Studies_Knowledge_Maturing_Model.pdf, [25.10.2010]
- Nemetz (2006), A Meta-Model for Intellectual Capital Reporting In Reimer,
- Karagiannis, (Hrsg.), Proceedings of the 6th International Conference on Practical
- Aspects of Knowledge Management, Springer, Berlin
- PKM (2009), 1st Workshop on Personal Knowledge Management (PKM),
- Verfügbar unter: http://www.wm-konferenz2009.org/workshops/PKM.php, [12.12.2009]
- PROMOTE (2001), (IST-1999-11658), Deliverable 2.1 Introduction of a knowledge management strategy, setting evaluation criteria, PROMOTE-Consortium, Wien, 2001
- WIEM (2009), WIEM 2009, Messen, Bewerten und Benchmarken des wirtschaftlichen Erfolgs von Wissensmanagement, Verfügbar unter: http://www.wm-konferenz2009.org/workshops/WIEM2009.php, [10.12.2009]
- Woitsch, Mak & Göllner (2010), Grundlagen zum Wissensmanagement im ÖBH – Teil 1: Ein WM-Rahmenwerk aus Sicht praktischer Anwendungen, Wien, 2010
- Woitsch, Mak & Göllner (2010a), Grundlagen zum Wissensmanagement im ÖBH – Teil 2: Wissensbilanz als Steuerungsinstrument im ÖBH: Ein Evaluierungs-Rahmenwerk aus der Sicht praktischer Anwendungen, Wien, 2010
- Woitsch, Mak & Göllner (2010b), Intellectual Capital Management using Knowledge Scorecards: The Austrian Defence Academy Showcase, DEXA 2010-EGOVIS ´10-International Conference on Electronic Government and the Information Systems Perspective

at the University of Deusto, Bilbao, Spanien

**Autoren**

**Ing. Mag. Klaus MAK**
Oberst des höheren militärfachdienstlichen Dienstes
Leiter der Zentraldokumentation (ZentDok) an der Landesverteidigungsakademie
Roßauer Lände 1
1090 Wien
klaus.mak@bmlv.gv.at

**Dipl.-Ing. Christian MEURERS**
Referent Multimedia Dokumentation und Situation Awareness Center an der
Zentraldokumentation/Landesverteidigungsakademie
Roßauer Lände 1
1090 Wien
christian.meurers@bmlv.gv.at

**Dipl.-Ing. Johannes GÖLLNER, MSc**
Leiter Wissensmanagement an der ZentDok/Landesverteidigungsakademie
Roßauer Lände 1
1090 Wien
johannes.goellner@bmlv.gv.at

**Dr. Robert WOITSCH**
BOC GmbH
BOC Asset Management
Operngasse 20b
1040 Wien
robert.woitsch@boc-eu.com

# 9. Sicherheitskonferenz Krems 2011

## 9. Sicherheitskonferenz Krems 2011

*„Auswirkungen der Kriminalität auf sicherheitsrelevante Fragestellungen"*

Donau-Universität Krems, 27.10.2011

Die vom Zentrum für Infrastrukturelle Sicherheit ausgerichtete, deutschsprachige Veranstaltung für Forscherinnen und Forscher aus Wissenschaft und Wirtschaft stand diesmal ganz im Zeichen der Sicherheit im Netz. Der Direktor des Bundeskriminalamtes, Herr General Franz Lang, zeichnete in der Keynote ein anschauliches Bild zur aktuellen Bedrohungslage und verdeutlichte die Dimensionen in konkreten Zahlen zur Kriminalität im Internet.

- 750 Mrd. € Schaden (lt. Europol)
- 150.000 Schadprogramme pro Tag (lt. Europol)
- 150 Mrd. US-$ Umsatzvolumen (lt. FBI) – mehr als durch Drogenhandel

In Österreich sind die Anzeigen auf dem Gebiet des Cyber-Crime in den letzten 10 Jahren um das 6-fache gestiegen. Täglich entstehen neue Deliktsformen im Netz, immer mehr gewinnt die organisierte Kriminalität an Terrain im Netz. Daher stellt die Bewusstseinsbildung in der Öffentlichkeit eine wichtige Komponente zur Prävention und zur Bekämpfung dar. Dies geschieht auch durch eine Vernetzung von Wissenschaft, Forschung, Wirtschaft und Behörden. 150 TeilnehmerInnen aus dem In- und Ausland – informierten sich über die neuesten Forschungsergebnisse auf dem Gebiet von Cyber Security und Cyber Crime.[1]

Donau-Universität Krems
Zentrum für Infrastrukturelle Sicherheit
Dr.-Karl-Dorrek-Straße 30
3500 Krems
http://www.donau-uni.ac.at

Das folgende peer-reviewed Paper wurde im Tagungsband veröffentlicht: Proceedings of 9. Sicherheitskonferenz Krems, Donau-Universitaet Krems, 2011

[1] http://www.bmi.gv.at/cms/BK/presse/files/Nachlese_SIKO_2011.PDF

Die freundliche Genehmigung zur Veröffentlichung in diesem Band wurde durch die Donau-Universität Krems am 04.06.2014 erteilt.

# Open Source Intelligence am Beispiel von KIRAS/MDL

*Gerhard Backfried, Dorothea Aniola, Gerald Quirchmayr, Werner Winiwarter, Klaus Mak, H.C. Pilles, Christian Meurers, Martin Köstinger, Paul Wohlhart, Peter M. Roth*

**Abstract:** Dieses Dokument beschreibt das Multimedia Documentation Lab (MDL), ein System, welches eine große Menge multimedialer Daten, die typischerweise von Open Sources in einer unstrukturierten Form und in verschiedenen Formaten gesammelt werden, in Echtzeit verarbeitet. MDL ist ein Werkzeug für die Lagebild-Erstellung und Risikobewertung. Es erlaubt die Integration von Multimedia-Content in die Analyseprozesse für sicherheitsrelevante Problemstellungen.

## 1. Einleitung

Eine wesentliche Voraussetzung für die Arbeit von Entscheidungsträgern ist es, qualitätsgesicherte Information zur richtigen Zeit am richtigen Ort bereit gestellt zu bekommen. Dies trifft auch auf den Bereich der öffentlichen Sicherheit zu. Nur durch optimierte Informationsbereitstellung und –verarbeitung können Risken und Bedrohungen, etwa durch Organisierte Kriminalität, Terrorismus und im Katastrophenschutz effizient verringert werden. Hatten staatliche Behörden in der Vergangenheit einen signifikanten Informationsvorsprung, gewinnen heute Informationen in öffentlich zugänglichen Systemen für die Unterstützung bei der Entscheidungsfindung immer mehr an Bedeutung. Prominente Beispiele dafür sind das Erdbeben in Haiti oder die Nuklearkatastrophe in Fukushima, wo die Regierung zugibt, sich auf öffentliche Quellen gestützt zu haben und vom Kraftwerksbetreiber nicht entsprechend informiert worden zu sein.

Traditionell werden Medieninhalte wie Text, Animation, Audio und Video entweder isoliert oder als Multimedia-Dokumente betrachtet. Eine Vernetzung von Dokumenten bleibt dabei, wie großteils in der Informationsanalyse üblich, auf Links und Verweise, wie wir sie aus Hypertext-Systemen kennen, beschränkt. Die inhaltliche Vernetzung stellt nach wie vor eher die Ausnahme dar.

Open Source Intelligence, die Suche nach und Analyse von Information in und aus frei verfügbaren Quellen, ist aufgrund des vorhandenen Volumens an Information in der Lage, immer besseren Input zu liefern. Entscheidende Voraussetzung für den Erfolg der Open Source Intelligence ist allerdings die Möglichkeit, die für eine bestimmte Entscheidungssituation relevante Information zeitgerecht zu finden, zu analysieren und dabei unterschiedliche Medientypen integriert betrachten zu können. Darüber hinaus kann sie auch helfen, bestimmte Aspekte besser einzuschätzen, wie etwa die Stimmung der Bevölkerung in einem Katastrophengebiet oder sich abzeichnende Krisen. Zugleich wäre es gerade in Krisensituationen wie Naturkatastrophen extrem wichtig, vor Ort auf die nötigen Informationssammler zurückgreifen zu können, um ein entsprechendes Lagebild erhalten zu können. Obwohl bereits heute ein Großteil dieser Informationen über Social Media Networks geliefert wird, muss leider davon ausgegangen werden, dass sie weitgehend ungenutzt bleiben.

Wie wichtig die Verfügbarkeit und Verlässlichkeit der Informationsquellen und die Qualität der Information selbst sind, zeigt das Beispiel des Abdrehens der USS Ronald Reagan vor Japan. Ohne verläßliche Information über die Ausbreitung des in Fukushima austretenden radioaktiven Materials war es unmöglich, die Sicherheit der Besatzung zu garantieren. Daher war ab einem gewissen Zeitpunkt eine Fortsetzung des Rettungseinsatzes nicht mehr zu verantworten.

Die Aufgabe, in einem stetig ansteigenden Informationsfluss, insbesondere multimedialer Inhalte in zahlreichen Sprachen, relevante Informationen zur Entscheidungsfindung aufzubereiten, wird zu einer interdisziplinären Herausforderung für Organisationen jedweder Art.

In MDL wird die Aufbereitung und Durchsuchbarkeit, sowie die Verteilung und Analyse von mehreren Informationsarten durch einen modulartigen Aufbau des Systems ermöglicht. So können Informationen und Informationsverweise aus Text-, Audio- und Video-Quellen in unterschiedlichen Variationen und Sprachen (wie auch hinsichtlich Qualität und Format) zugänglich gemacht werden. Die Ergebnisse stehen auf einem Multimedia-Server jederzeit zur Verfügung und können analysiert und visualisiert werden. Auch Benachrichtigungen können ausgesandt werden.

Neben der bisherigen Möglichkeit, Textdokumente effizient zu verarbeiten, sollen nun auch Rich-media Inhalte verarbeitet und zur Erstellung eines aktuellen Lagebildes herangezogen werden können. Diese heterogenen Inhalte (Radio, TV, Web-Sites, RSS-Feeds, Blogs, Wikis, Social Media …) müssen in einer Vielzahl von Sprachen, aus unterschiedlichen Quellen und in Echtzeit konstant zur Verfügung stehen. Über Ontologien oder Terminologie-Frameworks sollen Inhalte semantisch verknüpft und somit auffindbar gemacht werden. Letztendlich soll ein Demonstrator entwickelt und zur Verfügung gestellt werden, in dem alle Systemmodule dem Stand der -Technik entsprechen und mit existierenden Infrastrukturen und vorbereiteten Schnittstellen in bereits vorhandene Systeme integrierbar sind.

Im vorliegenden Dokument beschreiben die Autoren das MDL-System stellvertetend für jene Ansätze, die entwickelt werden, um frei verfügbare Information für Analysten und Entscheidungsträger effizient nutzbar zu machen.

## 2. Systembeschreibung

MDL besteht aus mehreren Modulen und Technologien in Komponentenform. Mit diesen Komponenten gemeinsam werden eine Reihe von Toolkits für die Endanwender bereit gestellt, so dass das System in einer sich ändernden Umgebung rasch und autonom erweitert und flexibel angepasst werden kann.

Die Inhalte finden über einen sogenannten Feeder Eingang in das System und werden dabei bereits verschiedenen Prozessen unterzogen. So wird beispielsweise Multimedia-Inhalt in Audio- und Video-*Tracks* gespalten. Für Audio-Daten beinhalten diese Prozessschritte die Segmentierung des Audiosignals, Aufteilung in sprachliche und nicht-sprachliche Segmente, Erkennung von Sprachen sowie textbasierte Verarbeitung der aus der Spracherkennung resultierenden Wortsequenzen.

Text-Inhalte werden normalisiert bevor sie den Prozessen der Erkennung von Named Entities (Named Entity Detection, NED) und der Themenerkennung (Topic Detection, TD) zugeführt werden.

Die aus diesem Prozess resultierenden Ergebnisse der einzelnen Verarbeitungsschienen liegen in einem proprietären XML Format oder in MPEG-7 vor und werden am Ende der Verarbeitungsvorgänge zusammen geführt (Late Fusion). Die XML-Dateien werden zusammen mit einer komprimierten Version der originalen Media Dateien auf den Media Mining Server (MMS) hochgeladen, wo sie durchsuchbar und für die Visualisierung einsetzbar sind.

Die Gesamtarchitektur des MDL-Systems basiert auf einer Server-Client Lösung und erlaubt die Entwicklung von unterschiedlichen Komponenten und Technologien auf unterschiedlichen Plattformen und Rechnern (allerdings sind nicht alle Komponenten multi-platform fähig). Mehrere Feeder, Indexer und Server (die entsprechend MMF, MMI und MMS genannt werden) können zu einem Komplettsystem kombiniert werden. Abbildung 1 bietet einen Überblick der Gesamtarchitektur mit den einzelnen Komponenten des MDL Systems und deren Interaktion.

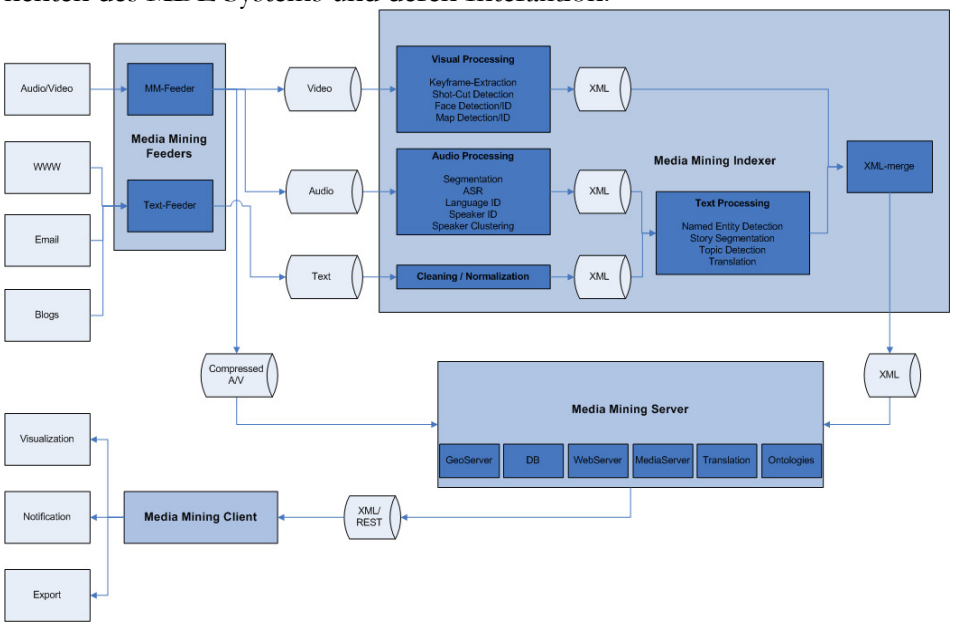



Abbildung 1 Gesamtarchitektur des MDL Systems

## *2.1 Feeder*

*Feeder* stellen die Schnittstellen des MDL-Systems zur externen Umgebung dar. Für Audio oder Audio/Video-Input können diverse Formate von externen Quellen importiert und von Sub-Komponenten verarbeitet werden. Um textuellen Input (etwa Daten von Web-Seiten, Feeds, Emails oder Blogs) zu verarbeiten, kommen unterschiedliche Feeder zur Anwendung, welche die Daten von diesen Quellen extrahieren und sie an die Textverarbeitungskomponenten weiterleiten.

#### 2.1.1. Multimedia Feeder (MMF)

Dieser Feeder basiert auf dem Direct Show Framework von Microsoft und kann eine Vielzahl von Quellen und Formaten verarbeiten. Die Daten werden hierbei auch re-enkodiert, um Windows Media Dateien zu erzeugen. Diese werden auf den Media Mining Server (MMS) hochgeladen, wo sie für spätere Suchvorgänge und Abfragen verwendet werden. Der Audio-Kanal wird an den Media Mining Indexer zur weiteren Verarbeitung weitergeleitet. Der Video-Kanal wird durch eine Reihe visueller Komponenten verarbeitet.

#### 2.1.2. Text Feeder

Text Feeder stellen spezielle Komponenten dar, welche textuelle Informationen aus spezifischen Quellen extrahieren und diese an den Media Mining Indexer (MMI) weiterleiten. Zwei beispielhafte Text Feeder sind der Web-Collector (für die Verarbeitung von Web-Seiten, News-Feeds oder Blogs) und der Email-Collector (für die Verarbeitung von Emails und deren Attachments). Der resultierende Text wird bereinigt, tokenisiert und anschließend an die Text-Verarbeitungskomponenten des MMI weitergeleitet. Text Feeder können an spezielle Eingangsdaten angepasst werden (customized Feeder).

### *2.2. Media Mining Indexer (MMI)*

Der MMI stellt das Herzstück der Verarbeitung von Audio und Text innerhalb des MDL Systems dar. Er besteht aus Technologien, als Komponenten verpackt, welche eine Reihe von Analyseschritten von Audio- und Text-Daten durchführen. Die Verarbeitungsresultate werden hierbei durch Anreicherung von XML-Strukturen kombiniert. Komponenten, um eine

Vielzahl von Sprachen verarbeiten zu können, stehen bereits mittels MMI zur Verfügung. So ist beispielsweise die automatische Sprachverarbeitungskomponente bereits für über ein Dutzend Sprachen einsetzbar. Als Teil des MDL-Projektes wurde ein Modell zur Verarbeitung von Mandarin-Chinesisch entwickelt.

### 2.2.1. Segmentierung

Nach initialer Konvertierung durch den Feeder wird das Audio-Signal klassifiziert und segmentiert. Weitere Normalisierungs- und Konversionsschritte werden im Rahmen dieser Verarbeitung angewandt, wodurch das Audio-Signal in eine Sequenz homogener Abschnitte unterteilt wird. Die entstandenen Segmente stellen die Bausteine für alle weiteren Audio-Verarbeitungsschritte dar. Im Rahmen der Segmentierung kommen Modelle von sprachlichen- wie auch nicht-sprachlichen (z.B. Atemgeräusche, Lachen,...) Lauten zur Anwendung, um den optimalen Segmentierungspunkt zu ermitteln[1]. Die Segmente werden in Bezug auf ihren Sprachinhalt untersucht. Es werden ausschließlich Segmente, welche eine ausreichende Menge an Sprache enthalten, zur weiteren Verarbeitung herangezogen.

### 2.2.2. Sprechererkennung (Speaker-ID, SID)

Die Sprechererkennung wird auf die durch die Segmentierung erzeugten Abschnitte angewandt, wobei ein Set von vordefinierten Sprecher-Modellen eingesetzt wird. Diese Modelle umfassen typischerweise eine Reihe von Personen des öffentlichen Interesses. Sollte die Identität eines Sprechers nicht festgestellt werden können, so versucht das System zumindest das Geschlecht des Sprechers zu identifizieren. Daten desselben Sprechers werden zusammengefasst und mit einer eindeutigen ID gekennzeichnet[2].

---

[1] LIU, D. und KUBALA, F., Fast Speaker Change Detection for Broadcast News Transcription and Indexing, Eurospeech, 1999

[2] LIU, D. und KUBALA, F., Online Speaker Clustering, ICASSP, 2003.

### 2.2.3. Automatische Sprachverarbeitung (Automatic Speech Recognition, ASR)

Die Spracherkennungskomponente wurde für große Vokabulare und sprecher-unabhängige, mehrsprachige Erkennung in Echtzeit entwickelt. Die Erkennung erfolgt hierbei in mehreren Schritten. In jedem Schritt kommen dabei genauere und komplexere Modelle zur Anwendung, die Zwischenresultate liefern und diese jeweils verfeinern und erweitern, um ein finales Transkript zu erzeugen[3] . Schließlich werden Verfahren der Textnormalisierung und sprachabhängige Verarbeitungsschritte[4] angewandt und das eigentliche Resultat des Spracherkenners in einem proprietären XML Format erzeugt. Der Spracherkenner verwendet eine zeit-synchrone, mehrphasige Suche, in welcher Gauss'sche Mixture Models, kontext-abhängige Phonemmodelle, und Wort- sowie Sub-wort basierte N-gram Sprachmodelle eingesetzt werden. Der Erkenner selbst ist sprachunabhängig und kann mit einer Vielfalt an Modellen in verschiedenen Sprachen und Bandbreiten betrieben werden.

### 2.2.4. Sprachenerkennung (Language ID, LID)

Sprachenerkennung wird auf Audio-Dateien angewandt, um die Sprache des Audio-Dokumentes zu identifizieren und ein für die Verarbeitung passendes Sprach-Modell zu wählen. Sie wird für Text-Dateien angewandt, damit adäquate Text-Verarbeitungsschritte gewählt werden können (oder eine entsprechende Verarbeitung im Rahmen des LMT bewirkt werden kann).

### 2.2.5. Text-Technologien

Text -Technologien werden entweder auf das Resultat der Spracherkennung oder auf dem Resultat der Text-Normalisierungsschritte angewandt. Normalisierung inkludiert die Vor-Verarbeitung, das Säubern (cleaning) und die Tokenisierung textueller Daten. Weiters werden sprachspezifische

---

[3] SCHWARTZ, R., NGUYEN, L. und MAKHOUL, J., Multiple-Pass Search Strategies, Automatic Speech and Speaker Recognition, 1996.

[4] HECHT, R., RIEDLER, J. und BACKFRIED, G., Fitting German into N-Gram Language Models, TSD, 2002.

Schritte, so wie die Verarbeitung von Zahlen, Komposita, Abkürzungen oder Akronymen, Text-Segmentierung und Normalisierung der Grapheme im Rahmen dieses Schrittes angewandt.

Die Erkennung von Named Entities (NED), wie etwa Namen von Personen, Organisationen oder geographischen Orten, sowie die Erkennung von Zahlen, wird auf dem Resultat der Spracherkennung oder alternativ auf dem Output der Text-Normalisierungskomponenten durchgeführt[5]. Das NED-System basiert einerseits auf Mustern, andererseits auf statistischen Modellen, welche auf Worten oder Wort-Eigenschaften definiert sind. Die Verarbeitung erfolgt auch hier in mehreren Schritten.

Die Themen-Erkennungskomponente (Topic Detection, TD) klassifiziert in einem ersten Schritt Sektionen des Eingangstextes. Die Modelle, die hierbei zur Anwendung kommen, sind durch eine spezifische Themen-Hierarchie vorgegeben. Sektionen, welche aneinander grenzen und einander ähnlich sind (bzw. identisch sind), werden zusammengelegt und reklassifiziert. Die Modelle, welche hierbei zur Anwendung kommen, basieren auf Support-Vector Machines (SVM mit Linearen Kernels)[6].

*2.3 Toolkits*

Im Moment stehen zwei Toolkits zur Verfügung, die es den Anwendern erlauben, Modelle selbständig ihren Anforderungen entsprechend zu entwickeln oder anzupassen.

LMT (Language Model Toolkit): dieser Toolkit erlaubt den Anwendern die Spracherkennungsmodelle anzupassen oder zu erweitern. So können etwa neue, und dem derzeitigen Geschehen angepasste Wörter in das Vokabular des Spracherkenners aufgenommen werden. Gleichfalls können Aussprachen oder Wortverwendungen an lokale Gegebenheiten angepasst werden.

---

[5] BIKEL, D., MILLER, S., SCHARTZ, R. und WEISCHEDEL, R., Nymble: High-Performance Learning Name-Finder, Conference on Applied Natural Language Processing, 1997.

[6] JOACHIMS, T., Text Categorisation with Support Vector Machines: Learning with many Relevant Features, in ECML, 1998.

SIDTK (Speaker ID Toolkit): dieser Toolkit ermöglicht Anwendern die Sprechererkennungsmodelle zu erweitern oder neue Modelle zu erstellen.

Eine Anpassung und Erweiterung der Named-Entity Modelle durch den Anwender ist ebenfalls möglich.

### *2.4 Visuelle Informationsverarbeitung*

Neben der Verarbeitung von Audio-Daten bietet MDL weiters die Möglichkeit Videodaten zu verarbeiten bzw. aus diesen Informationen zu extrahieren. Insbesondere sind das Detektieren bzw. das Erkennen von Personen (Gesichtern) und (geopolitischen) Karten von Interesse. Als kritisch, insbesondere für die Wahl der Methoden, muss in diesem Zusammenhang die Tatsache gesehen werden, dass Video-Streams oft mit starken Kompressionsartefakten behaftet sind oder mangelnde Auflösung aufweisen. Trotz dieser Einschränkungen müssen in Echtzeit akkurate Ergebnisse erzielt werden. Bevor die eigentlichen Schritte durchgeführt werden können, ist es notwendig kohärente zusammenhängende Videosequenzen zu extrahieren[7]. Sobald diese vorliegen, können alle weiteren Verarbeitungsschritte durchgeführt werden, die im Folgenden genauer beschrieben sind.

#### 2.4.1. Gesichtsdetektion und –erkennung

Um in den Videodaten Gesichter von Personen erkennen zu können, müssen diese zunächst detektiert werden. Dazu wird in jedem Einzelbild des Video-Streams ein effizienter Gesichtsdetektor angewandt (z.B. [8]), der Positionen und Ausmaße aller im Bild vorhandenen Gesichter liefert. Danach werden diese in einem eigenen Erkennungsschritt mit Einträgen aus einer Datenbank bekannter Gesichter abgeglichen, wobei zunächst die Positionen charakteristischer und wiedererkennbarer Gesichtsmerkmale (wie z.B. Augen, Mundwinkel, ...) lokalisiert und durch robuste Beschreibungen (Histogram of Oriented Gradients, Gabor Wavelets) dargestellt werden.

---

[7] SMEATON, A.F., TABAN, R. und OVER, P., The TREC-2001 video track report, In Proc. Text Retrieval Conference, 2001.

[8] VIOLA, P. und JONES, M.J., Robust Real-Time face detection, Int'l Journal of Computer Vision, 57(2):137–154, 2004

Um eine vollständige Suche zu vermeiden, werden gelernte Modelle verwendet (z.B. Support Vector Machines), die eine effizientere Klassifikation ermöglichen. Dazu sind allerdings annotierte Trainingsdaten notwendig, die in der Praxis schwer zu erhalten sind bzw. ist dies mit einem großen manuellen Aufwand verbunden. Um diesen zu reduzieren, kann das System selbständig neue Gesichter von unbekannten Personen aufnehmen[9]. Dazu werden aus mit dem Video assoziierte Informationen (z.B. Teletext) oder mittels OCR (Optical Character Recognition) erkannte Texteinblendungen verwendet, um automatisch die Identität von Personen zu ermitteln.

Da nicht alle Ansichten eines Gesichts für eine präzise Erkennung geeignet sind (z.B. Profilansichten oder auch stark nach vorne oder hinten geneigte Posen) wird eine gefundene Person durch das Video hindurch verfolgt und es werden Einzelbilder generiert, die sie aus unterschiedlichen Blickwinkeln zeigen. Um diese so genannten Face-Tracks zu erhalten, werden individuelle Detektionen, die in einem zeitlichen und räumlichen Zusammenhang stehen, über Bewegungsinformation (Optical Flow) miteinander verknüpft.

### 2.4.2. Kartendetektion und –erkennung

Um geopolitische Karten in Nachrichtensendungen detektieren und in weiterer Folge erkennen zu können, wird ein dreistufiges Verfahren angewandt. Als erster Verarbeitungsschritt werden rechteckige Regionen bestimmt, die möglicherweise eine Karte enthalten. Dazu wird eine klassische Hough Transformation[10] berechnet, um horizontale und vertikale Linienzüge zu extrahieren. Danach werden die so ermittelten Regionen durch lokale visuelle Deskriptoren wie Farbhistogramme (LAB, RGB), -mittelwert, -varianz und Grauwertableitungen beschrieben und mit mit einem effizienten Klassifikator - Extremely Randomized Forest - (ERF)[11] gelernt. In der Testphase werden so Regionen, die mit sehr hoher Wahrscheinlichkeit keine Karten aufweisen, zurückgewiesen. Die verbleibenden

---

[9] WOHLHART, P., KOESTINGER, M., ROTH, P.M., und BISCHOF, H., Multiple Instance Boosting for Face Recognition in Videos , In Proc. DAGM Symposium, 2011 (to be published).

[10] HOUGH, P., Method and means for recognizing complex patterns, In USENIX Security Symposium, 1962.

[11] GEURTS, P., ERNST, D., und WEHENKEL, L., Extremely randomized trees, Machine Learning, 36(1):3–42, 2006

Regionen werden hingegen einer detaillierten Analyse unterzogen.

Diese verbindet hierarchisches Shape Matching mit Texterkennung. Anschaulich wird hierbei verglichen, ob die in einer Region vorkommenden Konturen (z.B. Länderumriss) mit der Kartenbeschriftung (z.B. Ländername) übereinstimmen. Textuelle Hinweise etwa auf Länder oder Städtenamen bieten direkten Rückschluss auf die Lage. Konturen von Subregionen (z.B. Provinz- oder Länderumriss) helfen zu disambiguieren, ob die Region wirklich eine Karte darstellt, oder fälschlicherweise als solche eingeordnet wurde. Weiters ist es so möglich Karten zu erkennen, die keine Beschriftung aufweisen oder Fälle abzudecken, in denen die Texterkennung fehlschlägt. Für die Detektion selbst werden mittels eines Segmentierungsbaumes[12] aussagekräftige Konturen von Subregionen bestimmt. Die dabei entstehenden Regionen werden mit der Global Administrative Areas (GADM)[13] Datenbank abgeglichen.

### *2.5 Media Mining Server (MMS)*

Der Media Mining Server umfasst den eigentlichen Server, welcher zur Speicherung von XML und Multimedia-Dateien verwendet wird, wie auch ein Set an Tools und Schnittstellen, anhand derer der Inhalt der Datenbank abgefragt und aktualisiert werden kann. Sämtliche Interaktion mit dem MMS auf Seiten des Anwenders findet über den Media Mining Client (MMC) statt.

#### 2.5.1. Media Server

Der Server stellt Speicherplatz für XML, Indices, Audio und Video-Dateien zur Verfügung. Er basiert auf dem Oracle 11g Datenbanksystem, welches sämtliche Such- und Analysefunktionalitäten zur Verfügung stellt. Die Semantic Technologies von Oracle stellen hierbei die Basis für alle ontologie-relevanten Funktionalitäten innerhalb von MDL zur Verfügung.

---

[12] GU, C., LIM, J., ARBELAEZ, P., und MALIK, J., Recognition using regions, In Proc. Conf. on Computer Vision and Pattern Recognition, 2009.

[13] http://www.gadm.org/

### 2.5.2. Ontologien

Ein Ontologie-Modell in MDL wird durch eine Reihe von Konzepten, Instanzen und Beziehungen definiert[14]. Sie stellen einen zentralen Knotenpunkt innerhalb des Systems dar und erlauben die Verknüpfung von Informationen, welche aus unterschiedlichen Sub-Systemen stammen[15]. Übersetzungen sind mit Konzepten der Ontologie verknüpft, wodurch eine konzept-basierte Übersetzung möglich ist. Während der Suche können Ontologien eingesetzt werden, um Suchkriterien zu erweitern oder einzuschränken. Das Netzwerk von Konzepten kann zu diesem Zwecke navigiert und eingesetzt werden. Verwandte Konzepte können aufgrund der strukturellen Information aus der Ontologie angezeigt und untersucht werden. Eine geographische Ontologie wurde bereits entwickelt und kann nun als Basis weiterer Entwicklungen verwendet werden. Weitere Ontologien, insbesondere im Gebiet der Naturkatastrophen (Überflutungen) befinden sich in Entwicklung. Im finalen System soll es möglich sein, Ontologien, welche mit externen Werkzeugen entwickelt wurden (etwa mittels Protégé) auf einfache Weise zu importieren[16].

### 2.5.3. Übersetzung

Unterschiedliche Arten von Schnittstellen zu Übersetzungswerkzeugen werden von MMS zur Verfügung gestellt[17]. Parallel-Übersetzungen können bei Upload auf den MMS durch Zuhilfenahme von externen Übersetzungssystemen generiert werden. Weiters werden Wort-für-Wort Übersetzungen sowie eine Schnittstelle für menschliche Übersetzer zur Verfügung gestellt. Übersetzungen werden sowohl bei Suchen wie auch zur Visualisierung herangezogen.

---

[14] ALLEMANG, D. und HENDLER, J., Semantic Web for the Working Ontologist. Morgan Kaufman, 2008.

[15] DAVIES, J., GROBELNIK, M. und MLADENIC, D. (eds), Semantic Knowledge Management. Integrating Ontology Management, Knowledge Discovery, and Human Language Technologies, Springer-Verlag, 2009.

[16] Protégé Web-Site at Stanford University, http://protege.stanford.edu/, 2010.

[17] JURAFSKY, D. und MARTIN, J. H. Speech and Language Processing, Pearson, 2009.

*2.6 Media Mining Client (MMC)*

Der MMC stellt generell die Benutzerschnittstelle für Suche, Visualisierung, Updates und sämtliche Interaktion mit dem MMS dar. Benutzer können Abfragen durchführen, Inhalte herunterladen, Übersetzungen anfordern und Kommentare zu den Inhalten hinzufügen. Abfragen können freitextlich oder mittels logischer Ausdrücke durchgeführt werden, wobei der zugrunde liegende Datenbestand selektiert werden kann. Abfragen können abgespeichert und später für automatische Notifizierungen genutzt werden, wenn Dokumente, welche der abgespeicherten Abfrage entsprechen, auf den Server geladen werden. Suchergebnisse werden analog der vom MMI erzeugten Struktur dargestellt. Zusätzliche Informationen, wie etwa die Namen der erkannten Sprecher, Named Entities oder detektierte Karten werden mit dem Transkript eines Audio-Dokumentes zusammen dargestellt. Sowohl einzelne Sektionen, wie auch das gesamte Dokument können bei Bedarf abgespielt werden.

### 2.6.1. Visualisierung

Visualisierung der Datenbestände, welche den Anwendern erlaubt, diese in verschiedenen Sichtweisen darzustellen, spielt in MDL eine besonders wichtige Rolle. Suchergebnisse und Zusammenfassungen können verschiedenartig visualisiert werden. Dies gestattet Benutzern, Daten und Sachverhalte aus unterschiedlichen Blickwinkeln zu betrachten und iterativ von generellen zu spezifischen Blickpunkten wechseln. Eine Globus-Ansicht erlaubt, Ereignisse mit Örtlichkeiten zu verbinden. Named Entities (NEDs) können durch einen Beziehungsgraphen miteinander in Verbindung gebracht werden oder durch einen Trendgraphen zeitlich betrachtet werden. Durch eine Cluster-Ansicht können Entities und Informationsquellen miteinander in Beziehung gesetzt werden.

Weiterführende Abfragen können aus allen Visualisierungsmechanismen abgesetzt werden. Dies erlaubt z.B. in einem ersten Schritt, Ereignisse geographisch zu betrachten und in weiteren Schritten - ausgehend von der geographischen Information - tiefergehende Analysen zu starten. Ontologien können im Rahmen der Suche verwendet werden, um Abfragen zu modifizieren oder zu leiten. Informationen, welche aus Ontologien abgeleitet werden, können bei der Suche direkt Einfluss finden (etwa durch se-

mantische Erweiterung von Suchbegriffen) sowie für die Resultatsdarstellung angewendet werden.

*2.7 Crisis Room (CR)*

Einen weiteren Client stellt der Crisis Room dar, welcher zur gleichzeitigen Beobachtung zahlreicher TV- oder Radio-Kanäle eingesetzt werden kann. Ein typisches Szenario umfasst dabei die Projizierung mehrerer TV Kanäle mittels Beamer, wobei eine Vielzahl von Layouts für die Darstellung der gewählten TV Kanäle möglich ist. Zusätzlich steht ein Arbeitsplatz zur Verfügung, welcher zur Interaktion mit dem CR dient. Der CR erlaubt die kontinuierliche parallele Beobachtung des Auftretens von spezifischen Schlüsselwörtern und die gezielte Suche nach Stichworten. Das Auftreten eines Schlüsselwortes bewirkt dabei ein visuelles Feedback-Signal. Die Aufmerksamkeit des Benutzers wird auf einen konkreten Kanal gelenkt, wobei dieser nachfolgend auch zur Suche und für Playback verwendet werden kann. CR erlaubt folglich eine zeitnahe Analyse und Fokussierung auf relevante Themen und Ereignisse.

## 3. Status und Ausblick

Eine Vielzahl an Komponenten, wie etwa mehrere Feeder, Komponenten des MMS sowie sämtliche im Rahmen des MMI eingesetzten Komponenten sind bereits verfügbar und in Verwendung. Weitere Komponenten, beispielsweise zur visuellen Verarbeitung oder des MMS, befinden sich zur Zeit in Entwicklung oder sind als Prototypen verfügbar. Ein initiales System wurde beim Endanwender installiert und wird zu Evaluierungszwecken und für die Generierung von Feedback eingesetzt. Weitere Komponenten und Technologien werden schrittweise in die bestehende Installation integriert, um ein möglichst rasches Feedback zu erlauben.

Das MDL-System stellt ein Komplett-System entsprechend dem Standder- Technik im Bereich der Open Source Intelligence dar. Der finale Demonstrator wird sämtliche beschriebene Komponenten beinhalten. Um einen konstanten Informationsfluss zu gewährleisten, werden Feeders zur Beobachtung von TV Kanälen in einem 24x7 Modus eingesetzt werden. Diese werden Eingang in einen MMI finden, welcher seinerseits einen kontinuierlichen Eingangsstrom an Daten für den MMS erzeugt. In weiterer

Folge werden Text-Feeder eingesetzt werden, um konstanten Input an textuellen Daten, etwa RSS-feeds oder Web-Seiten, zu liefern. Alle Verarbeitungsschritte sollen in Echtzeit und mit minimaler Verzögerung durchgeführt werden. Die Resultate aller Verarbeitungsschritte werden auf dem MMS und zum Export in die vorhandene Infrastruktur bereit gestellt. Es ist beabsichtigt, MDL als eine zentrale Komponente des existierenden SAC (Situational Awareness Center) Systems zu etablieren. Auch über den Kontext des gegenständlichen Projektes hinaus wird MDL in einer Reihe von Anwendungsgebieten, wie etwa in der Bekämpfung der Organisierten Kriminalität oder bei der Terrorismusbekämpfung eingesetzt werden können.

## 4. Literatur


[1] LIU, D. und KUBALA, F., Fast Speaker Change Detection for Broadcast News Transcription and Indexing, Eurospeech, 1999.
[2] LIU, D. und KUBALA, F., Online Speaker Clustering, ICASSP, 2003.
[3] SCHWARTZ, R., NGUYEN, L. und MAKHOUL, J., Multiple-Pass Search Strategies, Automatic Speech and Speaker Recognition, 1996.
[4] HECHT, R., RIEDLER, J. und BACKFRIED, G., Fitting German into N-Gram Language Models, TSD, 2002.
[5] BIKEL, D., MILLER, S., SCHARTZ, R. und WEISCHEDEL, R., Nymble: High-Performance Learning Name-Finder, Conference on Applied Natural Language Processing, 1997.
[6] JOACHIMS, T., Text Categorisation with Support Vector Machines: Learning with many Relevant Features, in ECML, 1998.
[7] SMEATON, A.F., TABAN, R. und OVER, P., The TREC-2001 video track report, In Proc. Text Retrieval Conference, 2001.
[8] VIOLA, P. und JONES, M.J., Robust Real-Time face detection, Int'l Journal of Computer Vision, 57(2):137–154, 2004.
[9] WOHLHART, P., KOESTINGER, M., ROTH, P.M., und BISCHOF, H., Multiple Instance Boosting for Face Recognition in Videos , In Proc. DAGM Symposium, 2011 (to be published).
[10] HOUGH, P., Method and means for recognizing complex patterns, In USENIX Security Symposium, 1962.
[11] GEURTS, P., ERNST, D., und WEHENKEL, L., Extremely randomized trees, Machine Learning, 36(1):3–42, 2006.
[12] GU, C., LIM, J., ARBELAEZ, P., und MALIK, J., Recognition using regions, In Proc. Conf. on Computer Vision and Pattern Recognition,

2009.
[13] ALLEMANG, D. und HENDLER, J., Semantic Web for the Working Ontologist. Morgan Kaufman, 2008.
[14] DAVIES, J., GROBELNIK, M. und MLADENIC, D. (eds), Semantic Knowledge Management. Integrating Ontology Management, Knowledge Discovery, and Human Language Technologies, Springer-Verlag, 2009.
[15] Protégé Web-Site at Stanford University, http://protege.stanford.edu/, 2010.
[16] JURAFSKY, D. und MARTIN, J. H. Speech and Language Processing, Pearson, 2009.

**Autoren**

**Gerhard Backfried, Dorothea Aniola**
Sail Labs Technology AG, Wien

**Gerald Quirchmayr, Werner Winiwarter**
Universität Wien, Fakultät für Informatik, Institut für Distributed and Multimedia Systems, Institut für Scientfic Computing, Wien

**Klaus Mak, H.C. Pilles, Christian Meurers**
Landesverteidigungsakademie, ZentDok, Wien

**Martin Köstinger, Paul Wohlhart, Peter M. Roth**
Technische Universität Graz, Institut für maschinelles Sehen und Darstellen, Graz

# 14th FRAP - Finance, Risk and Accounting Management Perspectives Conference

## 14th FRAP - Finance, Risk and Accounting Man-agement Perspectives Conference

*„New Perspectives in Finance Risk and Accounting Management"*

Oriel College of the University of Oxford, 22.09.-24.09.2014

Understanding and bridging disciplinary as well as cultural boundaries in Finance, Risk and Accounting Management research.

This conference aims to overcome the often self-imposed paradigmatic boundaries and reflexive isomorphisms of the individual fields, and invites fresh perspectives. Despite its methodological and disciplinary openness, it does so with a strong focus on academic rigour and robustness. All abstracts and articles will be strictly double-blind peer reviewed, and there will be longer discussion sections during the conference in which authors can discuss their research in-depth with a small group of interested participants from industry and academia.
Every year around 100 participants from more than 20 nations are selected by a rigorous review process and come together to exchange their research ideas, build collaborations and discuss the future of theory and practice in Finance, Risk and Accounting Management!

### ACRN Academic Research Network

The ACRN Academic Research Network was originally founded as a joint venture by three leading European business schools of renowned universities from Austria, Finland and the UK to promote and host conferences and summer-schools in the social and managerial sciences, as well as to advance methodological know-how for doctoral students and young researchers. It is now a distinct entity with a clear impact mission and a highly respected international advisory board overseeing its corporate governance, firmly embedded in the Oxford research landscape.

ACRN Oxford Ltd.
1 Kings Meadow, OX2 0DP
Oxford, Oxfordshire, United Kingdom
http://www.acrn.eu/

The following peer-reviewed paper will be published in the conference proceedings. The date of publication is not fixed at the editorial deadline. The reference to the conference proceedings can be found at http://www.acrn.eu/finance/ after the publication date.

Full proceedings will be published with ISBN in Dec. 2014 and available from Google Bookstore.

# Framework for a Generic Meta Organisational Model

*Johannes Göllner, Thomas Benesch, Stefan Schauer, Karin Schuch, Stefan Schiebeck, Gerald Quirchmayr, Martin Latzenhofer, Andreas Peer*

**Abstract:** A comprehensive risk management is the foundation of all management, core and support processes in an organisation. In particular, a special emphasis is placed on risk management on a strategic and operative level due to the sensitive tasks and challenges in this area. As a first step we apply a Multi-Layer Multiple Vector Model in order to structurally categorise threats. A meta organisation model connects these generic concepts. It identifies four major groups: organisational development, actor model, resources and enablers. By applying this approach we are able to map risk aspects of finance and banking. Furthermore we plan to develop a meta risk model (plan and base for the design of the future information system architecture and IT-Tools) which considered all national, supranational and international bank- and finance risk requirement of current and future development of capabilities and organisational frameworks/requirements in relation to an development of an enterprise risk model which is relevant for banking and insurance companies.

**Keywords:** Risk Management, Multi-Layer Multiple Vector Model, Meta Organization Model, Meta Risk Model, Meta Supply Chain Network

## Introduction

As a foundation of all management, core and support processes within an organisation, a comprehensive and well integrated risk management can be understood as key factor to establish resilience and trust. With respect to information security, the target-group-oriented and competency-driven communication, management and controlling of risks has distinct influence on the acceptance and usability of every security information and management system, see Schiebeck (2005).

Based on an evaluation of different risk management catalogue sources identified by Schiebeck (2013, as cited in ENISA, 2007), the German Fed-

eral Office of Information Security is maintaining one of the most extensive risk management catalogues to establish a standardised, modular view on organisational assets, threats and safeguards, integrated with competence-driven role definitions. Organisations employing the IT-Grundschutz model can achieve an internationally recognised ISO/IEC 27001 certification. Because of this, control-mappings to common standards and frameworks like ISO/IEC 27001/2 (BSI, 2008), COBIT and ITIL (ISACA, 2008) (ITGI, 2006), NIST SP 800-53 and SANS 20 (SANS, 2011) are available.

Schiebeck (2007) promotes target-group-oriented management of assets, threats as well as safeguards and substantially supports the risk management process. Accordingly we are developing a generic meta risk model in order to find a way expressing risks in general by using a formalised modelling language for a future enterprise risk management implementation concept. We follow the approach of Karagiannis, Fill, Höfferer, Nemetz (2008) which leads to a comprehensive and integrative way describing risk management, no matter which field of application (e.g. ICT, environmental risks, finance risks) is on interest. Building upon this taxonomy, risk controlling aspects in the meta risk model can be facilitated by allowing knowledge and resource-based establishment of security targets and indicators for assets, as well as interconnected threats and safeguards required for risk mitigation. In order to support automation and therefore minimise recurring operational efforts for risk assessment, expert knowledge is incorporated and used to model the correlation between key performance indicators and key risk indicators.

The standards and frameworks identified have not sufficiently addressed characteristics necessary for homogenous risk models, nor have they addressed solutions to incorporate advanced controlling or monitoring features. Most standards like ISO/IEC 31000, ISO/IEC 27005, ISO/IEC 28000, etc. do not define a generic model but rather its high-level processes and requirements.

Up to now, the scientific community has primarily focused on the formulation of single-discipline approaches to establish and analyse complex risk models, e.g. covering functional relationships in Wang & Wulf (1997), neural networks in Haykin (2013), Fuzzy Logic in Shang & Hossen (2013) or

Bayesian belief networks in Simonsson, Lagerström, Johnson (2008) and Mo, Beling, Crowther (2009). These models tend to have a limited range of application and often focus on a single type of risk (e.g. financial, operational/technical). When looking at an organisation it is obvious that the organisation is influenced by different risk types, which makes it impossible to properly analyse such a complex risk model using only a single approach. Hence, a meta risk model can be used to define a wide scope of risk, using a generic description and thus providing an entire point of view. Based on this meta model, various approaches from different disciplines, e.g. finance and banking, can be applied to analyse the risk.

As a first step towards a risk analysis on such a generic level, an equally generic categorisation model has to be used to properly identify the threats in this complex risk model.

**Multi-Layer Multiple Vector Model („Doppelvektorenmodell")**

The complexity of systems requires a common terminology and a method for categorisation to structure system components and elements. This allows a standardised and analytical process to compare various elements. The categorisation taxonomy of the multi-layer multiple vector model is shown in the following Figure 1.

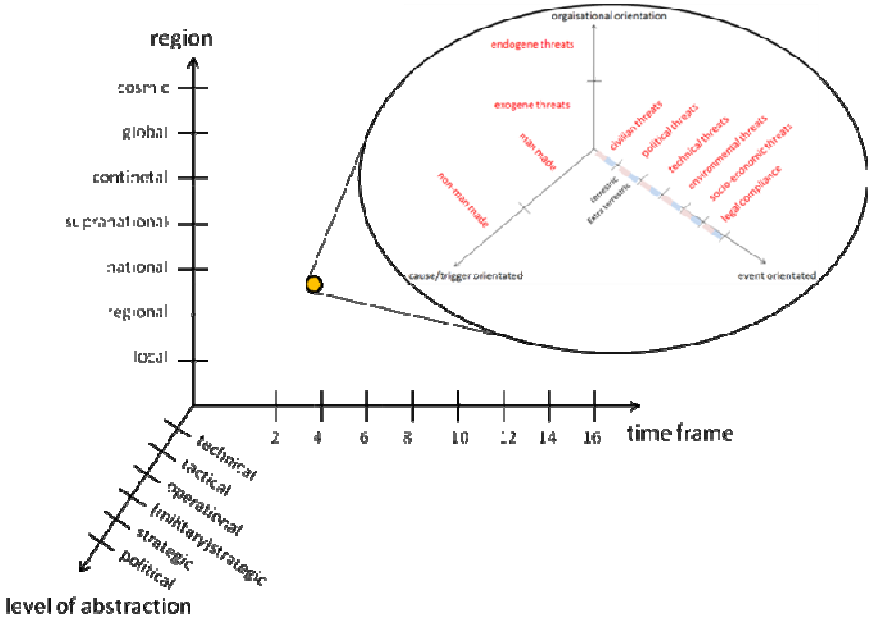



Figure 1: „Doppelvektorenmodell“[1]

The multi-layer multiple vector model is a spatial, multilevel meta classification system to specify every element of an event with the vectorial classification of the defined characteristics and attributes (as an extension of Abell, 1980). The first layer distinguishes between the axes of time and spatial aspects as well as the level of abstraction. Within the second layer (Göllner, 2009), the event is categorised considering its initiator and whether there is an endogenic or exogenic organisational reference. At last, the third axis of the second layer describes the event orientation with regards to the event genesis (i.e. terrestrial or extra-terrestrial). Hence, with this model it is possible to identify common patterns of possible critical situations in specific categories.

## Description of the Organisation Model

Besides the meta classification system given by the “Doppelvektorenmodell”, we have to define a meta model of an organisation. This enables to

[1] developed by Göllner J., Peer A., Mak K., Meurers C., Povoden G. (2011)

describe a generic organisation, detached from its field of application (e.g. finance, banking, logistics), and to define a generic meta risk model upon it. In the following, we present such a generic meta model of an organisation, including internal processes, resources and actors as well as the meta supply chain network for this organisation (see Figure 2).


Figure 2: Figure 2: Meta model of an organisation

The developed model of the organisation based on for instance ISO 31000, European and National Economy Law and specified legal compliance regulation ("Euro-SOX", Basel II and III, Solvency I and II, ORSA, Money Laundering, MaRisk, Sarbanes-Oxley Act, COSO 2013) consisting of various parts, divided in four major groups: organisational development, actor model, resources and enablers for the organisational development. The biggest part is the organisational development, where not only the corporate identity is modelled, but also the requirements on corporate compliance, including the structural and organisational models as well as the business process models. In the latter, all relevant business processes of the organisation are represented in a generic form.

The actors in context with the organisation can be described under three different points of view. Firstly they can belong to various groups of actors, e.g. actors within the organisation, supplier, customers and third parties, which are interested in the organisation. As second point, the actors could

be various types, e.g. a natural person or a legal person, whereas legal persons can be further divided into organisations under private or public law. The third point comes from the knowledge management and describes the different roles an actor can be part of. Each actor in context with the organisation has to be modelled considering all three sites of this point of view.

The third group describes the resources required and utilised by the organisation. This group consists of financial, human, organisational and technological resources.

The fourth group are the enabler of organisational development. Beside the multi-layer multiple vector model there are incidents on several levels which have to be considered. Both the multi-layer multiple vector model and the various incidents describe the input for the risk management techniques applied by the organisation (e.g. the risk management concepts, models, methods and tools).

The meta supply chain network is an important part of this model, since it includes all the infrastructures and suppliers the organisation relies on, e.g. energy, information, communication. It includes all potential customers of the organisation as integral part.

## Conclusion

The compliance is in particular since of its costs by use in the banking sector in a high prioritised position (Cocheo, 2014). This leads automatically to an extended sight of compliance, which will end in a generic meta risk model.
The introduced generic meta organisational model is the first part of a generic meta risk model, which expands and generalises the approach of the enterprise risk model. The target is behind the coordinated management of all risks faced by a firm and the systematic understanding of the interdependencies and correlations among risks, whether it is risk related to corporate governance, auditing, supply chain, distribution systems, IT, or human resources (McShane, Nair, Rustambekov, 2011). The focus lies on the integration of the involved persons and their individual activities into a workflow-supported operative situation report system and decision support

system for a web-based demonstrator platform for modelling and visualising correlations as well as collaboration.

This research is based on the research project „MetaRisk“, which is supported and partly financed by KIRAS (Austrian National Security Research Programme, http://www.kiras.at/).

**References**

- Abell, D. F. (1980). Defining a business - The Starting Point of Strategic Planning. Englewood Cliffs, New Jersey: Pretice-Hall, Inc.
- BSI - Bundesamt für Sicherheit in der Informationstechnik (2008). Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/Vergleich_ISO27001_GS.pdf?__blob=publicationFile.
- Cocheo, S. (2014). Widening your risk view. American Bankers Association Banking Journal, Vol. 106(2), pp-14-17.
- ENISA - European Union Agency for Network and Information Security (2007). Reference Source for threats, vulnerabilities, impacts and controls in IT-Risk-Assessment. Retrieved from http://www.enisa.europa.eu/act/rm/files/deliverables/reference-source-for-threats-vulnerabilities-impacts-and-controls-in-it-risk-assessment-and-risk-management/at_download/fullReport.
- Göllner, J., Meurers, C., Peer, A., Langer, L., & Kammerstetter, M. (2014). Bedeutung des Risikomanagements von Smart Grids. Symposium Energieinnovation 14.2.2014, Graz: Technical University.
- Göllner, J., Meurers, C., Peer, A., & Povoden, G. (2011). Hybridisation of Social Network Analysis in Context with other Methods for a Scenario Based Risk Analysis-Case Study: Critical Infrastructure for Energy Security in Austria. 7th Social Network Conference. London: University of Greenwich.
- Göllner, J. (2009): Definition in the lecture risk management at the Danube University Krems. Krems: Danube University.
- Haykin, S. (2013). Neural Networks. A Comprehensive Foundation, Person Education. Retrieved from

http://www.ib.cnea.gov.ar/~redneu/2013/BOOKS/Haykin.pdf.
- ISACA (2008). Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit. Rolling Meadows, Illinois: IT Governance Institute and Norwich, Norfolk: Office of Government Commerce. Retrieved fromhttp://www.isaca.org/KnowledgeCenter/ Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_ Eng_1108.pdf.
- ITGI (2006). COBIT Mapping. Mapping SEI's CMM for Software With COBIT 4.0. Rolling Meadows, Illinois: IT Governance Institute.
- Karagiannis, D., Fill, H.-G., Höfferer, P., & Nemetz, M. (2008). Metamodeling Some Application Areas in Information Systems. Information Systems and e-Business Technologies, Volume 5. Lecture Notes in Business Information Processing. Berlin, Heidelberg: Springer.
- McShane, M.K., Nair, A., & Rustambekov, E. (2011). Does Enterprise Risk Management increase Firm Value? Journal of Accounting, Auditing and Finance, Vol. 26(4), pp. 641-658.
- Mo, S., Beling, P., & Crowther, K. (2009). Quantitative assessment of cyber security risk using bayesian network-based model. Charlottesville, Virginia: Systems and Information Engineering Design Symposium SIEDS 24.4.2009. Retrieved from http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5166177.
- SANS (2011). Looking at the SANS 20 Critical Security Controls. Mapping the SANS 20 to NIST 800-53 to ISO 27002. System Experts Corporation. Retrieved from http://systemexperts.com/media/pdf/SystemExperts-SANS20-1.pdf.
- Schiebeck, S. (2013). Continuous Information Security Risk Assessment focused on Security Measurements. Research Report: University of Vienna, Austrian Research Promotion Agency (FFG). Vienna: University of Vienna.
- Schiebeck, S. (2007). IT-Risikomanagement. Anforderungen, Vorschriften und Toolevaluierung. Master Thesis: FHOÖ Campus Hagenberg. Hagenberg: University of Applied Sciences Upper Austria.
- Schiebeck, S. (2005). Zielgruppengerechte Vermittlung von IT-Sicherheitsthemen. Bachelor Thesis: FHOÖ Campus Hagenberg.

Hagenberg: University of Applied Sciences Upper Austria.
- Shang, K., Hossen Z. (2013). Applying Fuzzy Logic to Risk Assessment and Decision-Making. Casualty Actuarial Society, Canadian Institute of Actuaries, Ottawa. Retrieved from http://www.soa.org/Files/Research/Projects/research-2013-fuzzy-logic.pdf.
- Simonsson M., Lagerström R., & Johnson P. (2008). A Bayesian Network for IT Governance Performance Prediction. 10th International Conference on Electronic Commerce (ICEC), Innsbruck. Retrieved from http://portal.acm.org/citation.cfm?id=1409542.
- Wang C., Wulf W. (1997). Towards a Framework for Security Measurement, Department of Computer Science, University of Virginia, Charlottesville. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.100.9803&rep=rep1&type=pdf.

**Authors**

**Johannes Göllner, MSc MSc,** is currently head of the section Knowledge Management in the Department of Central Documentation and Information Service at the National Defence Academy of the Federal Ministry of Defence and Sports in Vienna, since 2008. His research areas from 2009 up to now include knowledge management, organizational development, trend- and risk analysis with natural, environmental, technical, civilian, socio-economical influences as well as scenario planning and development, particularly considering economic and finance aspects. He chaired conferences in the area of risk and crisis management and was involved in several EU research projects. He contributed several standardisation initiatives, like the Austrian Standards Institute, International Standards Organisation and European Committee on Standardisation. Furthermore he held lectures on risk-, crisis-, security management, and critical infrastructure at the University of Natural Resources and Applied Life Sciences, Vienna, and Danube University, Krems, Austria, where he was also director for a master programme on risk management from 2009 to 2012.

**Thomas Benesch, Dr.habil PhD PhD,** Head of Research & Development at s-benesch

**Stefan Schauer, PhD,** is a scientist and researcher in the Safety & Security Department of the Austrian Institute of Technology (AIT). He studied Computer Science at the University of Klagenfurt and received his PhD in Theoretical Physics, working on Quantum Cryptography, at the Technical University Vienna. Since 2005 he is working for the AIT in several projects related to the fields of classical security and risk management. Currently, his main focus lies in the field of risk management and risk assessment as well as security architectures for critical infrastructures. In this context he is interested in novel approaches to risk assessment taking the socio-economic interplays of a company and its environment into account.

**Karin Schuch, MSocEcSc,** is a scientific researcher at the MasterMind Consulting Risk & Crisis.

**Stefan Schiebeck, MSc,** is a scientific researcher at the Austrian Institute of Technology and has held national and international talks regarding information security and risk management. His relevant certifications include Ethical Hacker, accredited ISO/IEC 27001 Lead and Internal Auditor as well as ONR Risk Manager.

**Gerald Quirchmayr, Prof PhD PhD,** holds doctors degrees in computer science and law and is Professor at the Department of Distributed and Multimedia Systems (MIS) at the University of Vienna. In 2001/2002 he held a Chair in Computer and Information Systems at the University of South Australia. 2005 - 2010 he headed the Department of Distributed and Multimedia Systems and served as Vice Dean of the Faculty of Computer Science 2008 - 2010. Since 2011 he serves as deputy head of the MIS group. He currently serves as Deputy Director of the Doctoral Studies Programme Natural and Technical Sciences and is appointed as Director starting October 2014.

**Martin Latzenhofer, MSocEcSc**, is a PhD fellow at University of Vienna and is currently working on risk management topics. After his studies of Business Informatics he worked for various companies - e.g. T-Mobile, KPMG - in different roles like Information Security Manager, IT Auditor, IT Service Manager, IT Consultant, IT Trainer and Information Officer. He is accredited CISA, CISM, CRISC, ITIL Service Manager v2, ITIL Expert v3. Besides he has been given courses for Business Informatics stu-

dents for twelve years.

**Andreas Peer, MA MA, i**s a member of the section Knowledge Management of the Department of Central Documentation and Information Service at the National Defence Academy of the Federal Ministry of Defence in Vienna. He is an expert for risk and crisis management and also knowledge and scenario development. In 2004 he absolved the military academy and became a professional officer and the MA in "military leadership". Andreas Peer was 2006 a participant of the Master of Business Administration "Environmental Threats and Disaster Management". From 2007 to 2011 he was commanding officer and responsible for the deployment of an NBC-defence company. Experience got Andreas Peer during various trainings and missions mostly after natural disasters, in Austria and abroad. He has further experience in kind of In-house Consultant of the EU-Research-Project "FOCUS-Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles", 2009-2012 and various national research projects.

# 5.Konferenz Professionelles Wissensmanagement (WM2009)

**WM2009**
*Erfahrungen und Visionen*
Solothurn, 25.03.-27.03.2009

Die zweijährlich stattfindende Konferenz Professionelles Wissensmanagement will einen breiten integrativen Überblick über die organisatorischen, kulturellen, sozialen und technischen Aspekte des Wissensmanagements liefern. Dabei steht im Mittelpunkt der Konferenz, die verschiedenen Forschungsdisziplinen miteinander zu verbinden und die gesammelten Erfahrungen aus den unterschiedlichen Anwendungsbereichen zu teilen.

Die 5. Konferenz stand unter der Schirmherrschaft von Kurt Fluri, Stadtpräsident der Stadt Solothurn, und wurde von den Fachgruppen Wissensmanagement und dem Querschnittsfachausschuss Modellierung der Gesellschaft für Informatik e.V. sowie dem Institut für Wirtschaftsinformatik der Fachhochschule Nordwestschweiz veranstaltet.

Weitere Informationen finden Sie unter
http://www.wm-konferenz2009.org/

Das folgende peer-reviewed Paper wurde in den Proceedings der Konferenz veröffentlicht:
Hinkelmann, Knut und Wache, Holger(Eds.)
WM2009: 5th Conference on Professional Knowledge Management
2009, 600 Seiten
GI-Edition Lecture Notes in Informatics (LNI) - Proceedings, Volume P-145
Bonner Köllen Verlag (2009)
ISBN 978-3-88579-239-0
ISSN 1617-5468

# Intellectual Capital Management using Knowledge Scorecards: A Best Practice Implementation at the Austrian National Defence Academy

*Robert Woitsch, Wilfrid Utz, Klaus Mak, Johannes Göllner*

**Abstract:** The paper at hand discusses the applicability of knowledge scorecards and intellectual capital management for monitoring and steering of knowledge-driven organizations based upon a best practice project at the Austrian Defence Academy (in particular the School for Atomic, Biological and Chemical Defence). Within this project a model-driven approach based upon the PROMOTE® methodology has been implemented, integrating the knowledge balance/scorecards into management instruments and mechanisms available at the Austrian National Defence Academy.

## 1 Introduction

In today's information and knowledge driven society[1] existing knowledge within organizations is the decisive resource applied in the service delivery process. While highly structured processes have been automated applying business process management principles for continuous improvement, weakly structured processes a different approach is necessary. They require for completion human interaction and decision making hence have a substantial potential for increased economic implication and improvement. Raising effectiveness and efficiency in the latter processes, hence making humanized knowledge evaluable are desirable and considered possible by establishing controlling and monitoring mechanisms for intellectual capital management.

In the following knowledge products are defined as those products which set the strategic proposition of a company and are the output of knowledge-related production process. The term knowledge resource is

[1] i2010 - A European Information Society for growth and employment, Online at: http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm

referred to as humanized knowledge within a company, building up the organizational memory of a company.

The creation, maintenance and improvement of such knowledge resources within a company plays an import role; it includes disciplines such as knowledge management and learning approaches (establishing a "learning organization" [CEN04]). Monitoring/controlling aspects of intangible capital is already well established in other domains such as financial controlling and are summarized under the term "Intellectual Capital Management" [St99]. Within the following sections, an approach on controlling and monitoring of intellectual capital is presented. The well established PROMOTE® [WK05] approach, the PROMOTE® methodology as a procedure model as well as the PROMOTE® modelling language have been used as a basis for defining knowledge products, knowledge resources and knowledge processes all used within the intellectual capital management and reporting mechanisms applying a model-driven mechanism in the implementation process. The approach has been applied in the course of a best-practice project within the Austrian National Defence Academy – more particular within the School of Atomic, Biological and Chemical Defence, an organization heavily dependent on the knowledge and expertise of its employees in order to maintain the necessary level of security and sustainability in critical domains available at every point in time.

## 2 Conceptual Background

The implementation of intellectual capital monitoring and reporting uses the instrument of knowledge scorecards [TC07]. The knowledge scorecard is based upon the Balance Scorecard definition of Kaplan and Norton [KN96] defining perspectives, goals, indicators and measures and its interrelations. For the implementation of the knowledge scorecard a model-driven approach has been applied based upon the PROMOTE® roadmap described below. In the case of PROMOTE® graphical models[2] based upon process models are used to describe the organization knowledge thus increasing the human readability and understandability using symbols and relations/hierarchies resulting in a graphical modelling language for

[2] Graphical modelling dates back to IBM's flow diagrams developed in the 40's see [KM05]

knowledge management. For the Balance Scorecard approach, the modelling environment of the ADO*score*® tool[3] for defining an organization's scorecard has been used, using a fitting graphical notation for its definition. In the following, the PROMOTE® procedure model is described defining the general approach for the implementation project followed by a definition of the applicability of the Balance Scorecard implemented in ADO*score*®.

### *2.1 PROMOTE® Application Scenarios and Approach*

As mentioned above the PROMOTE® approach consists of a general procedure model as well as the PROMOTE® modelling language[4].
The procedure model is based upon the BPMS [Ka95], [TKW01] paradigm consisting of 5 phases (goal definition, knowledge management, knowledge operationalisation, knowledge exectution and knowledge evaluation) structuring a model-driven approach. PROMOTE® supports a set of application scenarios like Process-Oriented Knowledge Management, Knowledge Management Process Optimization, Skill Management and Intellectual Capital Reporting. The last scenario is presented in more detail below.

### *2.2 Knowledge Scorecards for Monitoring of Intellectual Capital*

The intellectual capital management scenario as presented in chapter 2.1 uses mechanisms and constructs of controlling frameworks and establishes these frameworks in the domain of knowledge management. Consequently the PROMOTE® approach as outlined above is regarded as the basis for building up knowledge scorecards. The knowledge scorecards use the same principles as defined for Balance Scorecards by Kaplan and Norton but focus on knowledge management aspects. Therefore the structure of the PROMOTE® based knowledge scorecard is defined as follows: (1) Product Perspective: Goals, indicators and measures for the actual product provided by the organization, (2) Processes and Structure Perspective: Goals, indicators and measures in relation to processes executed(core processes,

---

[3] ADO*score*® Product Information Online at:
http://www.boc-group.com/documents/products/adoscore_flyer_de.pdf

[4] AsIsKnown Project – PROMOTE® language definition in Deliverable D13: Architecture and Implementation of the Smart Profiler

quality-relevant processes, management processes, etc, (3) Human Capital, Relations and Competences Perspective: Goals, indicators and measures of human capital and competences, and (4) Resources and Support Perspective: Goals, indicators and measures of budget, infrastructure, material and tools (structural capital). These perspectives have been derived within the best practice project and validated against literature in the domain [Sv97] resulting in a reference architecture for knowledge scorecards on a generic level.

## 3 Best Practice Project: Austrian National Defence Academy

In the following the best practice project for knowledge scorecards based upon the PROMOTE® approach is described in detail giving insights in the project results and steps performed. The section starts describing the problem statement and motivation for the best practice project, presents project results based upon the conceptual description above and concludes with lessons learned from the perspective of the project partners.

### *3.1 Motivation*

New regulations for academic institutions[5] also changed the reporting responsibilities for knowledge assets within the Austrian National Defence Academy, committing them to issue intellectual capital reports. The above mentioned concept of knowledge scorecards assures compliance with the legal reporting obligations.
The Austrian National Defence Academy is the highest military training and research institution of the Austrian Armed Forces and takes over research, training, documentation and publications tasks, producing knowledge products for specific domains and activities.

### *3.2 Project Execution and Results*

The best practice project has been executed according to the following roadmap for implementing the knowledge scorecards based upon the

[5] Universitätsgesetz 2002 Online at: http://archiv.bmbwk.gv.at/universitaeten/recht/gesetze/ug02/Universitaetsgesetz_20027727.xml

PROMOTE® approach. The results derived and accomplished in each phase are described below.

**Definition of the Initial Situation.** For defining the initial knowledge management situation at the School for Atomic, Biological and Chemical Defence the PROMOTE® modelling environment has been used to identify knowledge products, knowledge management processes and in particular the competences and skills necessary for product provision. The knowledge product model at the School of Atomic, Biological and Chemical Defence has been structured according to the application area (Basis, Training and Action Products) of the products. In a next step competences have been mapped by relating the provided knowledge products to the organizational models available concluding with a competence matrix.

**Specification of Goals.** The next step focused on deriving the target user group and expected results for a knowledge scorecard system (internal vs. external communication, updating mechanisms). Existing management instruments have been investigated and integrated in the knowledge scorecard approach accordingly to enable a comprehensive monitoring and management approach.

**Definition/Identification of Cause-And-Effect Relations**. Based upon the goals identified in the previous phase, cause and effect relations between goals have been identified and enhanced by measurable criteria.

**Quantification of Goals**. During the analysis process and discussions various indicators were identified, subject to operational data available in different systems such as HR management tools, financial controlling systems, etc. Additional to those indicators, criteria have been identified where operational data sources are not yet available and need further investigation. For the operational indicators a detailed specification has been derived giving all necessary information for the reporting and monitoring system.

**Operational Data Coupling**. The next phase considers the operationalisation of the knowledge scorecard through the coupling of the designed models with operational data-sources. Operational data sources used as input are typically data warehouse applications, databases in general or spreadsheets that are updated on a regular basis.

**Communication of the Knowledge Scorecard** and **Steering and Management based on Knowledge Scorecard**. As a reporting and performance monitoring tool, the controlling cockpit has been used to visualize the results of the knowledge scorecard to the targeted audience and provide interactive analysis and reporting functions.

## 4 Conclusion

The implementation of the knowledge scorecard at the School of Atomic, Biological and Chemical Defence resulted in a comprehensive instrument for steering the service provision processes within the organization and built up a transparent framework for evaluation of knowledge assets. The implementation is regarded as a best practice application within the Austrian National Defence Academy that proves that evaluation of knowledge assets and continuous monitoring could improve the reactions capabilities and learning structures of Austrian Armed Forces, leading to an increased readiness for duty in the case of military actions.

## 5. Acknowledgement

The authors would like to thank Bgdr Mag. Hermann Loidolt, MSc and o. Univ Prof. Dr. Dimitris Karagiannis for support during the project acquisition and execution phase as well as Bgdr Norbert Fürstenhofer, Waffengattungschef ABC & Kdt der ABCAbwS, for the possibility to execute the project and continuous review and quality feedback

## References

- [CEN04] CEN/ICCS Knowledge Management Workshop, Europäischer Leitfaden zur erfolgreichen Praxis im Wissensmanagemetn, Brüssel, Frühjahr 2004
- [St99] Stewart, T. A. (1999) Intellectual Capital: The New Wealth of Organizations. New York: Doubleday.
- [WK05] Robert Woitsch, Dimitris Karagiannis: Process Oriented Knowledge Management: A Service Based Approach. J. UCS 11(4): 565-588 (2005)

- [KN96] Robert S. Kaplan, David P. Norton The Balanced Scorecard: Translating Strategy Into Action. Harvard Business Press, 1996.
- [KM05] Kühn H., Murzek M., Modelling: From Caftsmanship to Automation, In: Backlund P., Carlsson S., Söderström E. (Eds): Proceedings of the Fourth International Conference on Business Informatics Research (BIR 2005), ISBN 91-631-7521-5, Skövde, Sweden, October 3.4, 2005, pp. 57-66
- [Ka95] Dimitris Karagiannis, BPMS, Business Process Management Systems: Concepts, Methods and Technologies, SI-OIS Special Issues, SIGOIS Bulleting, 10-13, 1995
- [TKW01] Rainer Telesko, Dimitris Karagiannis, Robert Woitsch, Knowledge Management, Concepts and Tools: The PROMOTE project, Forum Wissensmanagement, Systeme – Anwendungen – Technologien, Oldenburg 2001
- [Sv97] Sveiby, K. E. (1997) The New Organizational Wealth: Managing & Measuring Knowledge-Based Assets. San Francisco: Berrett-Koehler Publishers.
- [TC07] Tai, W-S. and Chen C-T.: An Intellectual Capital Performance Evaluation Based on Fuzzy Linguistic, Proceedings of the Third International Conference on International Information Hiding and Multimedia Signal Processing (IIH-MSP 2007) - Volume 02, IEEE

**Authors**

**Robert Woitsch, Wilfrid Utz**
BOC Asset Management GmbH,
Bäckerstraße 5,1010, Vienna, Austria
{robert.woitsch, wilfrid.utz}@boc-eu.com

**Klaus Mak, Johannes Göllner**
Landesverteidigungsakademie, Zentraldokumentation (ZDok),
Stiftgasse 2a,1070, Vienna, Austria
{klaus.mak, mba.ukm}@bmlv.gv.at

# Open Knowledge Models Workshop / EKAW2010

## EKAW 2010 - OKM

*Erfahrungen und Visionen*
Lisbon, Portugal, 11.10.-15.10.2010

The 17th International Conference on Knowledge Engineering and Knowledge Management is concerned with all aspects of eliciting, acquiring, modeling and managing knowledge, and its role in the construction of knowledge-intensive systems and services for the semantic web, knowledge management, e-business, natural language processing, intelligent information integration, etc. The focus of the 17th edition of EKAW will be on Knowledge Management and Engineering by the Masses. Besides a research track, EKAW will feature a tutorial and workshop program, as well as a poster and demo track. The proceedings of the conference will be published by Springer Verlag in the LNCS series. Poster/demo notes and workshop/tutorial notes will be published separately in a companion booklet.

### Open Knowledge Models Workshop

When analysing the transformation of the information society to a knowledge society an industrialisation of knowledge work can be observed. The maturity, the quality, the process-orientation and the alignment of knowledge to personal or organisational requirements are industrialisation aspects covered by knowledge work. This workshop focuses on process-orientation, based on its evolution over service-orientation towards virtualisation and sees the current industrialisation of knowledge work as a challenge that needs to be tackled not only on social and technical level but also on a conceptual level. As an expression of the maturity the knowledge work can be modelled in form of knowledge motivation, routines, situations, structure and vocabularies, elements and tools.

http://ekaw2010.inesc-id.pt/
http://www.openmodels.at/web/EKAW2010-OpenKnowledgeModels

The following peer-reviewed paper was presented at the workshop and published in-house. Therefore no special copyright permission were necessary.

# PROMOTE® in the Austrian Armed Forces: The Knowledge Management Processes in the Department of Central Documentation and Information Service/National Defence Academy

*Klaus Mak, Johannes Göllner, Christian Meurers, Wilfrid Utz*

**Abstract:** The paper discusses the use and benefits of the process-orientated Knowledge Management approach PROMOTE® in the Department of Central Documentation of the National Defence Academy (CentDoc/NDA) at the Austrian Ministry of Defence. With the PROMOTE® approach it was possible to map all knowledge products and processes of the CentDoc to an interactive process map, which are linked to internal experts on the intranet-portal.

**Keywords:** Knowledge Management, PROMOTE®, Process Management, Documentation, Information, Defence, Austria, Armed Forces, Process Orientation

## 1 Introduction / Initial Situation

The CentDoc[1] of the National Defence Academy (NDA) in the Austrian Armed Forces (AAF) is the operational unit for managing open source information for the AAF. Since 1968 relevant documents for the organisation have been analysed, stored in databases and distributed to defined user groups. The main tasks involve the registration, screening, evaluation, content exploitation, terminology extraction, categorising, and creation of abstracts, profiling and indexing of a wide variety of sources. Application of different tools in the field as well as development and evaluation of new methods and knowledge management approaches such as PROMOTE® to optimize processes and gain a maximum of efficiency are in the focus of CentDoc. Hier finden Sie Fachinformationen zu Themengebieten (Fachinformationen), die sich mit Heer, Verteidigung, Sicherheit u.ä. beschäftigen:

[1] CentDoc: Department of Central Documentation and Information Service of the National Defence Academy at the Austrian Ministry of Defence;

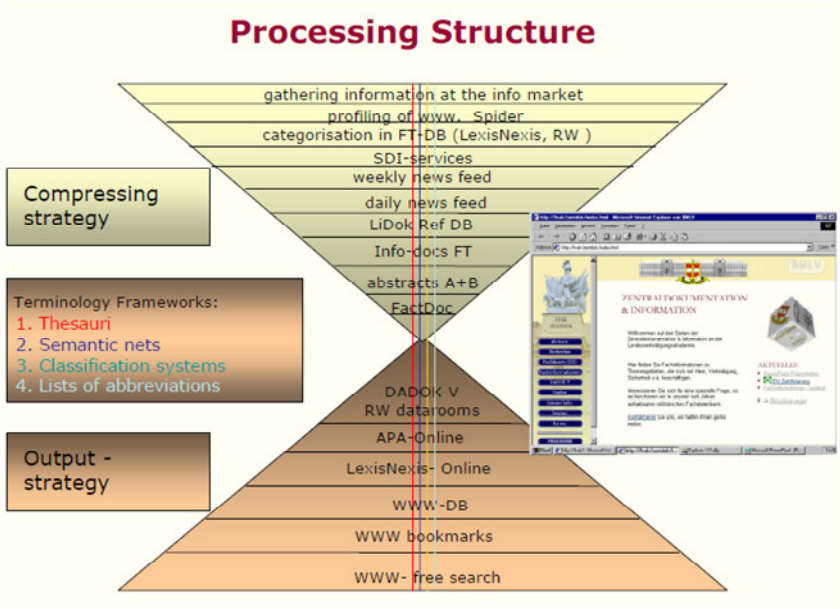



**Fig. 1:** The processing structure shows the compressing strategy, the output strategy,the terminology frameworks and the distribution platform.

Fig. 1 shows the extraction of terminology as an embedded part of the terminology framework. Extraction of terminology is fundamental for categorising and indexing documents with regard to an optimized and efficient access to information. New technologies and applications enable the capability to provide knowledge products (offered product in context of organisation by knowledge management system, distinction between information, consulting and application products[2]) as soon as possible during the running working processes. This is supported by an experts portal, where users access functionalities for online-demands, offered expert services or independent enquiries.

CentDoc is the platform for Knowledge Management in the Austrian Armed Forces. In order to establish a coherent system for knowledge management at the AAF the PROMOTE® approach has been applied to iden-

[2] Woitsch R., Mak K., Göllner J., Grundlagen zum Wissensmanagement im ÖBH Teil 1: Ein WM-Rahmenwerk aus der Sicht praktischer Anwendungen. Landesverteidigungsakademie Wien, (2010)

tify and map relevant processes for knowledge management of AAF using a process-oriented framework. The output is used to recognize synergies between different areas/departments and implement a management framework for controlling and monitoring efficient performance at CentDoc.

Following this introductory section the paper describes briefly the PROMOTE® approach in section 2. Section 3 summarizes the implementation of PROMOTE® at CentDoc and concludes in section 4 by specifying the benefits of the implementation and providing an outlook and further research challenges observed.

## 2 PROMOTE® Approach

PROMOTE® as a Process-Oriented Knowledge Management (POKM) approach defined in[3] has been developed in the course of the EU co-funded project PROMOTE®[4] and further developed in a course of research and industrial projects[5],[6]. Business process management as the basis for POKM can be regarded as commodity today, the challenge lies within combining/aligning process management initiatives with knowledge management in the organisation. The operationalisation of POKM by applying Service Oriented Knowledge Management (SOKM)[7] results in knowledge integration capabilities through orchestration of knowledge services on

[3] Hinkelmann, K.; Karagiannis, D.; Telesko, R.: PROMOTE - Methodologie und Werkzeug zum geschäftsprozessorientierten Wissensmanagement. In: Geschäftsprozessorientiertes Wissensmanagement, Springer-Verlag, (2002)

[4] Karagiannis, D. and Telesko, R.: The EU-Project PROMOTE: A Process-oriented Approach for Knowledge Management, Proceedings of the 3rd International Conference on Practical Aspects of Knowledge Management, Basel, (2000)

[5] Hrgovcic, V., Woitsch, R., Utz, W. and Leutgeb, A.: Adaptive and Smart e-Government Workflows - Experience Report from the Projects FIT and LDCAST, eChallenges e-2008 Stockholm, Sweden, IOS Press, (2008)

[6] .Hrgovcic, V., Utz W., Woitsch R. Knowledge Engineering in Future Internet, in Karagiannis D., Jin Z. (Eds.) Knowledge Science, Engineering and Management, Springer, Vienna, (2009)

[7] Woitsch, R.: PhD Thesis, Process Oriented Knowledge Management: A Service-Based Approach, PhD thesis University of Vienna, (2004)

different levels (possibly through services[8] or mashups[9]).

For the implementation of PROMOTE® at CentDoc/NDA as a process-oriented knowledge management environment[10] the following steps and objectives have been identified:

- Definition of the organisational task by identifying the organisational goals and requirements, analysing and documenting the environment.
- Synchronized analysis of related knowledge products
- Definition of the key elements of the PROMOTE® organisational concept and usage concept. A selection and scoping of appropriate PROMOTE® models is performed.
- Definition the knowledge cycle at CentDoc as high-level process map
- Design of selected knowledge management processes at CentDoc: about 70 main knowledge products (synonymous for organisational products) and additional supporting knowledge products in the areas of core, support, management processes
- Implementation of PROMOTE® as a management tool for CentDoc intranet distribution platform

## 3 Concept of Realisation

The analysis and documentation of the organisational tasks represent the basis for developing the KM concept of the organisation and applying the PROMOTE® knowledge management approach. The first step to implement this approach was therefore the analysis of key elements of the internal organisational concepts and the internal use of these concepts, as well

---

[8] Maier R., Hädrich T., Peinl R., Enterprise Knowledge Infrastructure, Springer Verlag, Berlin (2005)

[9] Schmidt A., Ley T., Lindstaedt S., Workshop o n Knowledge Servcices & Mash-ups, in Hinkelmann K., Wache H., (Eds) WM 2009: 5th Conference on Professional Knowledge Management, March 25-27, 2009, Solothurn, Switzerland, GI-Verlag, Bonn (2009)

[10] Mak, K.: Der Einsatz des prozessorientierten Wissensmanagementwerkzeuges PROMOTE® in der Zentraldokumentation der Landesverteidigungsakademie. Landesverteidigungsakademie Wien, (2005)

as the harmonisation and alignment/mapping with PROMOTE® concepts. All key elements are defined and distinguished from each other. Next, the interfaces between these key elements have to be specified.

Fig. 2 visualizes the key elements of the PROMOTE® concepts. The specification of these elements includes the definitions, the description of the current operational system, and the existing tools and skills, which are required for operating a knowledge management system.

These concepts and their interrelationships represent the fundamental elements of the "Knowledge Management Value Added Chain" and were synchronised with the concepts of CentDoc. Knowledge is the fundamental resource of the "Knowledge Management Value Added Chain". This chain defines the process to the information products and the process to the user groups.

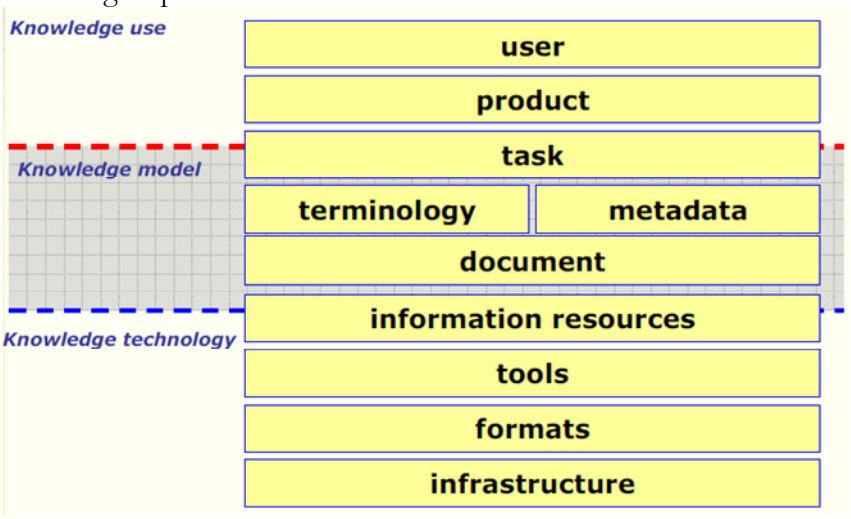



**Fig. 2:** Key elements of the PROMOTE® organisational concept and use concept

In Fig. 3 all relevant sources, the compressing strategy, the information product categories, and the user groups are described. The internal workflow focuses on the compressing strategy, in which the knowledge of experts is made accessible for the user groups in the AAF.

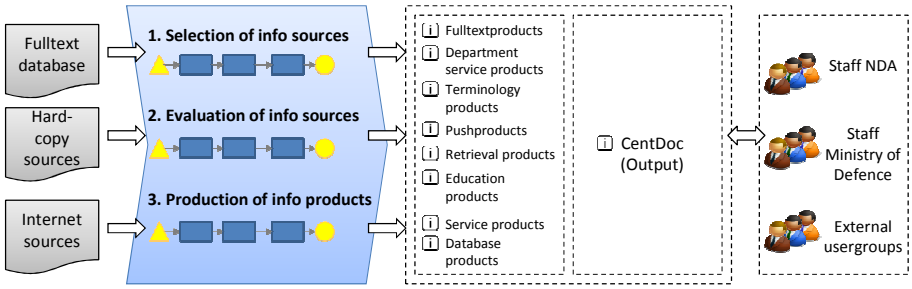



**Fig. 3:** The "Knowledge Management Value Added Chain" of the CentDoc

### *3.1 The Knowledge Cycle – the Main CentDoc Process Map*

The main CentDoc processes have been analyzed and visualized in a knowledge map. The vertical classification differentiates between management tasks, main operational tasks and support tasks and their particular aggregations. Horizontally the different dimensions of the main tasks were mapped: content, time, and organisation. These dimensions are also representing the PROMOTE® process-types. The main CentDoc processes were included in this PROMOTE® model

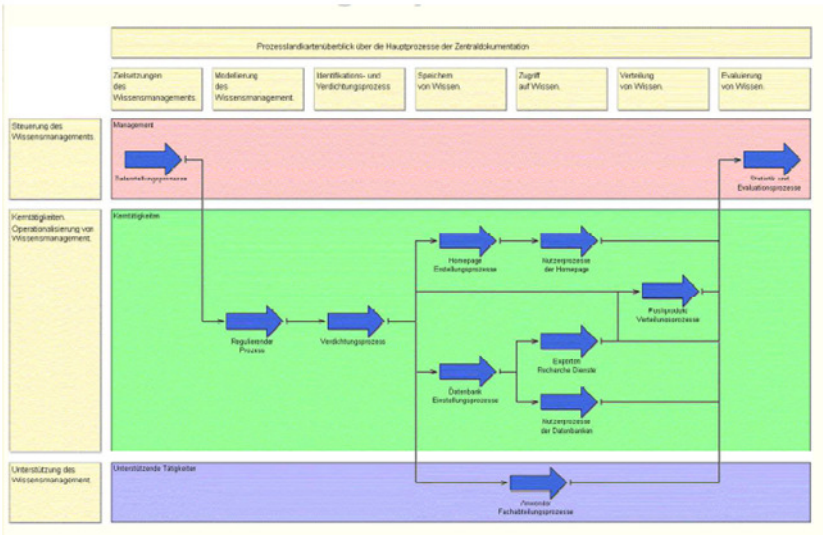


**Fig. 4:** The Knowledge Cycle at CentDoc

This general view of the Knowledge Cycle is followed by another, more

detailed, process map, where the dependencies and relationships between the CentDoc processes and tasks are described more precisely. The compressing strategy process for example results in a process group, which contains 14 identified processes.

### *3.2 PROMOTE® as a Management Platform*

In Fig. 5 the "Management Platform" PROMOTE® describes the position of the CentDoc in the NDA and in the AAF. This model is interactive and all elements like products, processes, sites, knowledge maps, skills, information rooms and tools are linked and can be accessed. This model also describes the interface to the research department and education departments, as well as to opinion leaders and user groups.

1. Representing CentDoc consisting of the expert portal, the offered knowledge products, the knowledge cycle and the organisational environment (processes, organisation, resources, skills)
2. Inputting organisational units of AAF such as research and educational departments as well as external units such as opinion leaders and user groups and interfaces of CentDoc to these units are represented
3. Output consumers and application environment for decision support

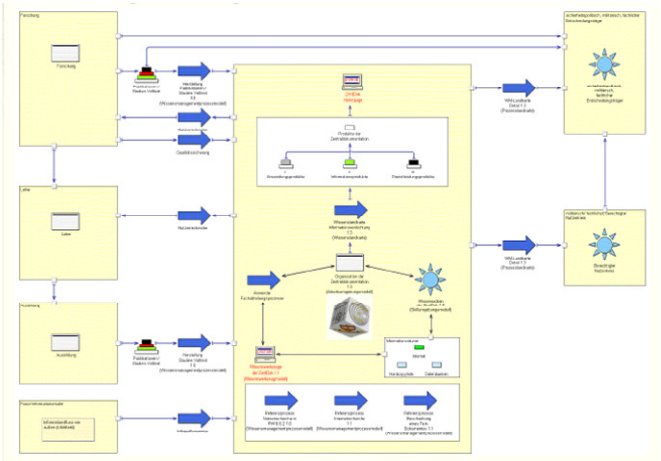


**Fig. 5:** PROMOTE® as a management tool for CentDoc (internal)-Platform

### *3.3 CentDoc Product Map*

The model is representing more than 50 products as part of an interactive product map, distinguished by product classification and production cycle.

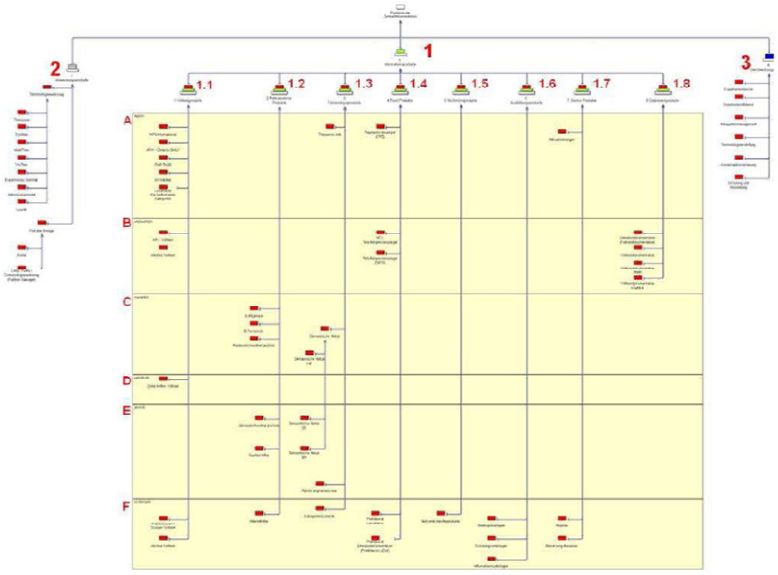



**Fig. 6:** CentDoc Product Map

It includes hardcopy- and online-products, which are results of the compressing and production processes of the CentDoc, as well as application-, service- and education products. The products are linked to the experts portal in the CentDoc Network and directly accessible.

39 types of information products are represented in categories and timelines[10]. The product map offers daily (A), weekly (B), monthly (C), periodically (E), yearly (F) updates, and on demand (G) updated information products. The categories are fulltext-products (1.1), abstracts (1.2), terminology-products (1.3), push-products (1.4), retrieval-products (1.5), education-products (1.6), service-products (1.7) and database-products (1.8).

Application. [2] and service products [3] are linked and directly accessible for the users. Every product has a product id-card, that contains the detailed product information summarized in an aggregated/general product id-card-overview.

| Product ID Card | | | |
|---|---|---|---|
| Product ID | II.2.1 | | |
| Product Name | A-General | | |
| Type of Product | Information product | Category | Department Service Product |
| Format of Product | Hardcopy publication of abstracts of security policy and military content and online publication on CentDoc Website. | | |
| Update | Monthly | | |
| Description | Summaries (Abstracts) of articels of peridocial appearing professional journals produced and published in accordance with a categorized table of content. | | |
| Comment | Fulltext is made available via postal or email system | | |
| Product responsible | Editor in Chief Info-A | | |
| Access control/requirements | Access via distribution of hardcopy publication and via CentDoc Website Link „Abstracts-Allgemein“ for all 3. VE Users possible. | | |
| Link | http://www.lvak.intra.bmlv.at/zentdok/index.html -> ”Abstracts” | | |
| Location | Local Server “LStift2” | | |
| Creation process | 3.3.2.1.3 Production of Abstracts | | |

**Table 1.** shows the product id-card of abstracts (version A, security, military) with the description of product-type, category, content-description and handling-information

## 4 Conclusion and Outlook

Establishing PROMOTE® as an internal “Management and Documentation”-tool has brought several benefits not only for the CentDoc itself, but

for the whole organisation of Austrian Armed Forces. By mapping knowledge-intensive, content-related, administrative and supporting documentation- and information tasks as well as development- and service operations in a highly sophisticated and detailed way, a new kind of transparency and visualisation of the complexity of the organisation can be provided by CentDoc. These advantages of using PROMTOE® are resulting in:

- Adjusted organisational concept and user concept for knowledge management
- Adjusted modelling guidelines for knowledge management processes
- Adjusted knowledge management processes in the CentDoc
- Use of knowledge management–user processes in the whole organisation
- Adjustment and visualisation of the terminology of knowledge management processes
    - The CentDoc processes can be used as an pattern for other organisational units.
    - The clearing function of the CentDoc makes the adjustment of further projects easier.

An observation made is that a focus at AAF lies upon semantic interoperability not only on a terminology level but also on process terminologies and meta-terminology to make the developed model applicable for other organisational units. In the domain of terminologies functionality for analysis, comparison and translation offered as services are needed to instantiate the model accordingly.

**References**


- Mak, K.: Der Einsatz des prozessorientierten Wissensmanagementwerkzeuges PROMOTE® in der Zentraldokumentation der Landesverteidigungsakademie. Landesverteidigungsakademie Wien, (2005)
- Karagiannis, D. and Telesko, R.: The EU-Project PROMOTE: A Process-oriented Approach for Knowledge Management, Proceedings of the 3rd International Conference on Practical Aspects of

Knowledge Management, Basel, (2000)
- Hinkelmann, K.; Karagiannis, D.; Telesko, R.: PROMOTE - Methodologie und Werkzeug zum geschäftsprozessorientierten Wissensmanagement. In: Geschäftsprozessorientiertes Wissensmanagement, Springer-Verlag, (2002)
- Woitsch, R.: PhD Thesis, Process Oriented Knowledge Management: A Service-Based Approach, PhD thesis University of Vienna, (2004)
- Hrgovcic, V., Utz W., Woitsch R. Knowledge Engineering in Future Internet, in Karagiannis D., Jin Z. (Eds.) Knowledge Science, Engineering and Management, Springer, Vienna, (2009)
- Hrgovcic, V., Woitsch, R., Utz, W. and Leutgeb, A.: Adaptive and Smart e-Government Workflows - Experience Report from the Projects FIT and LDCAST, eChallenges e-2008 Stockholm, Sweden, IOS Press, (2008)
- Schmidt A., Ley T., Lindstaedt S., Workshop o n Knowledge Servcices & Mash-ups, in Hinkelmann K., Wache H., (Eds) WM 2009: 5th Conference on Professional Knowledge Management, March 25-27, 2009, Solothurn, Switzerland, GI-Verlag, Bonn (2009)
- Maier R., Hädrich T., Peinl R., Enterprise Knowledge Infrastructure, Springer Verlag, Berlin (2005)
- Woitsch R., Mak K., Göllner J., Grundlagen zum Wissensmanagement im ÖBH Teil 1: Ein WM-Rahmenwerk aus der Sicht praktischer Anwendungen. Landesverteidigungsakademie Wien, (2010)

**Authors**

**Klaus MAK, Johannes GÖLLNER, Christian MEURERS**
Austrian Ministry of Defence, National Defence Academy, Departement of Central Documentation and Information Service, Stiftgasse 2a, 1070 Vienna, Austria
{klaus.mak, johannes.goellner, christian.meurers}@bmlvs.gv.at

**Wilfrid UTZ**
BOC Asset Management GmbH, Bäckerstraße 5, 1010 Vienna, Austria
wilfrid.utz@boc-eu.com

## 7th UK Social Networks Conference 2011

University of Greenwich, 07.07.-09.07.2011

The UK Social Networks Conference offers an interdisciplinary venue for social and behavioural scientists, sociologists, educationalists, political scientists, mathematicians, computer scientists, physicists, practitioners and others to present their work in the area of social networks. The primary objective of the conference is to facilitate interactions between the many different disciplines interested in network analysis. The conference provides a unique opportunity for the dissemination and debate of recent advances in theoretical and experimental network research.

http://www2.gre.ac.uk/about/faculty/business/services/events/events/past-events-2011/uksocialnetworks

The following peer-reviewed paper was presented at the conference, but not published in the proceedings. Therefore no special copyright permissions were necessary.

# Hybridisation of Social Network Analysis in Context with other Methods for a Scenario Based Risk Analysis – Case Study: Critical Infrastructure for Energy Security in Austria.

*Johannes Göllner, Christian Meurers, Andreas Peer, Guenter Povoden*

**Keywords:** critical infrastructure, security, energy, social network analysis, risk assessment, operational capability development, strategy development, scenario.

In the course of the two years project "Scenario Planning" at the National Defence Acadamy of the Austrian Ministry of Defence and Sports a concept has been developed intended for risk assessment and the development of operational and strategic capabilities based on a scenario portfolio. Several military and civilian experts from different branches contributed to this concept which finally turned out to be useful for a variety of applications not limited only to the military.

The concept is based on the hybridisation of various methods including social network analysis for a comprehensive description and analysis of relevant systems which may be regarded as the basis for risk assessment applying certain scenarios[1],[2],[3]. The knowledge generated may be useful for

[1] Goellner, J., Meurers, C., Peer, A., Povoden, G. (2010): Wissensmanagement im ÖBH (Knowledge Management in the Austrian Armed Forces). Systemdefinition, -beschreibung und –begrenzung zur Szenarioentwicklung und Modellierung (Definition, description and boundary of systems). Teil 1: Allgemeine Systemdefinition und Systembeschreibung (Part I: General definition and description of systems). Schriftenreihe der Landesverteidigungsakademie, 12/2010, Reprozentrum Wien 4450/10. ISBN: 978-3-902670-51-9

[2] Goellner, J., Meurers, C., Peer, A., Povoden, G. (2010): Wissensmanagement im ÖBH (Knowledge Management in the Austrian Armed Forces). Systemdefinition, -beschreibung und –begrenzung zur Szenarioentwicklung und Modellierung (Definition, description and boundary of systems). Teil 2: Darstellung von ausgewählten Methoden und möglichen Teilsystemen (Part II: Description of selected methods and possible subsystems). Schriftenreihe der Landesverteidigungsakademie, 13/2010, Reprozentrum Wien 4684/10. ISBN: 978-3-902670-53-3.

the development of strategies and required operational capabilities of an organisation[4].

A pre-requisite for scenarios and a risk assessment is the comprehensive description of the relevant system which is described in various publications, e.g. the models according to Bossel and Vester[5],[6]. The theoretical framework of the presented concept has implemented different sectors of security according to Buzan and Waever[7]:

- Military security
- Political security
- Economic security
- Societal security
- Environmental security

Additionally the regional security concept theory (RSCT) is applied where players and actors at regional, global and local level are identified and how

---

[3] Goellner, J., Meurers, C., Peer, A., Povoden, G .(2010): Einführung in die Soziale Netzwerkanalyse und exemplarische Anwendungen (Introduction of Social Network Analysis and selected applications). Wissensmanagement im ÖBH (Knowledge Management in the Austrian Armed Forces), unpublished, publication confirmed for April 2011: Schriftenreihe der Landesverteidigungsakademie, 5/2010/S, Reprozentrum Wien, ISBN 978-3-902670-56-4.

[4] Mak, K., Goellner, J., Woitsch, R., Utz, W. (2010): Intellectual Capital Management using Knowledge Scorecards: The Austrian National Defence Academy Showcase. DEXA (Database and Expert Systems Applications) and EGOVIS (Electronic Government and the Information Systems Perspective) conference 2010, September 1st 2010, Bilbao, Spain. [https://springerlink3.metapress.com/content/746lr2072723w46x/resource-secured/?target=fulltext.pdf&sid=ycebiv3rrf5ad045sj3xxi55&sh=www.springerlink.com 28.03.2011].

[5] Bossel, H. (2007): Systems and Models. Complexity, Dynamics, Evolution, Sustainability. Books on Demand GmbH, Norderstedt, Germany.

[6] Vester, F. (2008): Die Kunst vernetzt zu denken. Ideen und Werkzeuge für einen neuen Umgang mit Komplexität. Deutscher Taschenbuch Verlag München, 7. Auflage.

[7] Buzan, B. Waever O., Wilde, J. de (1998): Security - A New Framework for Analysis. Lynne Rienner Publications. ISBN-13: 978-1555877842.

they are related to each other[8]. The RSCT is especially relevant for security policy aspects[9] . The interdependency and relations may be for example economic, political or military. The impact of nodes may be also at different levels (global, interregional, regional or local).

The hybridisation of these methods with Social Network Analysis methods and tools delivered a scenario based risk analysis concept. In a case study dealing with the analysis of critical infrastructure this concept is used in order to identify key risk indicators for energy security in Austria contributing to a risk management process. The methodology includes the generation of scenarios which can also be used for the identification of required capabilities of an organisation and may have an impact on its strategy.

The case study is a typical example of an interdisciplinary and also transdisciplinary application of Social Network Analysis and its tools[10], analyzing and visualizing the interdependencies and relations of a transnational and interregional pipeline as an object of strategic relevance with the involved actors, taking into consideration technological, economical, environmental, military and social aspects.

Examples of critical infrastructure[11] connected to the case study may be (in brackets the estimated geographical impact level):

- Supply chain networks (local, regional, interregional)

---

[8] Buzan, B., Waever O. (2008): Regions and Powers. The Structure of International Security. 6th edition, Cambridge University Press, ISBN 978-0-521-81412-6.

[9] Merlingen M., Mireanu M., Stavrevska, E. B. Europäische Sicherheit: Wo stehen wir heute? In: Jahrbuch 2008, Centre for OSCE research (CORE). Das Zentrum für OSZE-Forschung / Centre for OSCE Research (CORE) am Institut für Friedensforschung und Sicherheitspolitik (IFSH) an der Universität Hamburg. [http://www.core-hamburg.de/documents/jahrbuch/08/pdf-gesamt.pdf, 01.03.2011].

[10] Katzmair H., FAS.research (2010): Social Network Analysis - Die Wissenschaft von der Messung, Visualisierung und Simulation sozialer Beziehungen (Social Network Analysis – the science of measuring, visualizing and simulation of social relations), [http://90.146.8.18/de/archiv_files/20041/FE_2004_katzmair_de.pdf, 01.12.2010].

[11] Goellner, J., Kienesberger, G., Peer, A., Schoenbacher, P., Weiler, M., Wurzer, G. (2010): Analyse und Betrachtung von Kritischen Infrastrukturen (Analysis and description of critical infrastructures). Schriftenreihe der Landesverteidigungsakademie, 14/2010/S, Reprozentrum Wien 4889/10. ISBN: 978-3-902670-64-9.

- Life line structures (local, regional)
- Logistic centres and hubs (local, regional, interregional)
- Industrial complexes like refineries and power plants (local, regional or interregional)
- (Potential) gas or oil fields (local, regional, up to global depending on the size)
- Satellites, GPS (global, regional, local)

These infrastructures and objects are closely related to aspects like environment, economy, politics, technology, etc. The actors (organisations, companies, individuals, etc.) may have an impact on objects and infrastructure (erection, destruction, decay, exploitation ...) and other aspects related to environment, technology, industry, etc. and also the other way around, as actors may be receptors as well.

These influences are visualized and the elements (nodes) are ranked according to criticality, centrality or other parameters. For the development of a scenario the identification of critical parameters is essential. These scenarios may include environmental aspects like climate change, earth quakes, political or social changes. As seen in history, industrial sites and other critical infrastructure often were targets in armed conflicts. Strategic bombing of oil refineries and other industrial complexes in WWII is only one example. The impact on the economy and the population was considerable as well as on the environment. The term "TIM (toxic industrial material) release" is widely used today talking about chemical, biological, radiological or even nuclear hazards and threats in modern scenarios embedded in an urban and highly industrialized environment.

Summarizing it is shown that the set of methods described including Social Network Analysis may be used as the methodological framework for a risk assessment and the development of strategies and operational capabilities.

**References:**

- [1] Goellner, J., Meurers, C., Peer, A., Povoden, G. (2010): Wissensmanagement im ÖBH (Knowledge Management in the Austrian Armed Forces). Systemdefinition, -beschreibung und –begrenzung zur Szenarioentwicklung und Modellierung (Definition,

description and boundary of systems). Teil 1: Allgemeine Systemdefinition und Systembeschreibung (Part I: General definition and description of systems). Schriftenreihe der Landesverteidigungsakademie, 12/2010, Reprozentrum Wien 4450/10. ISBN: 978-3-902670-51-9.

- [2] Goellner, J., Meurers, C., Peer, A., Povoden, G. (2010): Wissensmanagement im ÖBH (Knowledge Management in the Austrian Armed Forces). Systemdefinition, -beschreibung und –begrenzung zur Szenarioentwicklung und Modellierung (Definition, description and boundary of systems). Teil 2: Darstellung von ausgewählten Methoden und möglichen Teilsystemen (Part II: Description of selected methods and possible subsystems). Schriftenreihe der Landesverteidigungsakademie, 13/2010, Reprozentrum Wien 4684/10. ISBN: 978-3-902670-53-3.
- [3] Goellner, J., Meurers, C., Peer, A., Povoden, G .(2010): Einführung in die Soziale Netzwerkanalyse und exemplarische Anwendungen (Introduction of Social Network Analysis and selected applications). Wissensmanagement im ÖBH (Knowledge Management in the Austrian Armed Forces), unpublished, publication confirmed for April 2011: Schriftenreihe der Landesverteidigungsakademie, 5/2010/S, Reprozentrum Wien, ISBN 978-3-902670-56-4.
- [4] Mak, K., Goellner, J., Woitsch, R., Utz, W. (2010): Intellectual Capital Management using Knowledge Scorecards: The Austrian National Defence Academy Showcase. DEXA (Database and Expert Systems Applications) and EGOVIS (Electronic Government and the Information Systems Perspective) conference 2010, September 1st 2010, Bilbao, Spain. [https://springerlink3.metapress.com/content/746lr2072723w46x/resource-secured/?target=fulltext.pdf&sid=ycebiv3rrf5ad045sj3xxi55&sh=www.springerlink.com 28.03.2011].
- [5] Bossel, H. (2007): Systems and Models. Complexity, Dynamics, Evolution, Sustainability. Books on Demand GmbH, Norderstedt, Germany.
- [6] Vester, F. (2008): Die Kunst vernetzt zu denken. Ideen und

Werkzeuge für einen neuen Umgang mit Komplexität. Deutscher Taschenbuch Verlag München, 7. Auflage.
- [7] Buzan, B. Waever O., Wilde, J. de (1998): Security - A New Framework for Analysis. Lynne Rienner Publications. ISBN-13: 978-1555877842.
- [8] Buzan, B., Waever O. (2008): Regions and Powers. The Structure of International Security. 6th edition, Cambridge University Press, ISBN 978-0-521-81412-6.
- [9] Merlingen M., Mireanu M., Stavrevska, E. B. Europäische Sicherheit: Wo stehen wir heute? In: Jahrbuch 2008, Centre for OSCE research (CORE). Das Zentrum für OSZE-Forschung / Centre for OSCE Research (CORE) am Institut für Friedensforschung und Sicherheitspolitik (IFSH) an der Universität Hamburg. [http://www.core-hamburg.de/documents/jahrbuch/08/pdf-gesamt.pdf, 01.03.2011].
- [10] Katzmair H., FAS.research (2010): Social Network Analysis - Die Wissenschaft von der Messung, Visualisierung und Simulation sozialer Beziehungen (Social Network Analysis – the science of measuring, visualizing and simulation of social relations), [http://90.146.8.18/de/archiv_files/20041/FE_2004_katzmair_de.pdf, 01.12.2010].
- [11] Goellner, J., Kienesberger, G., Peer, A., Schoenbacher, P., Weiler, M., Wurzer, G. (2010): Analyse und Betrachtung von Kritischen Infrastrukturen (Analysis and description of critical infrastructures). Schriftenreihe der Landesverteidigungsakademie, 14/2010/S, Reprozentrum Wien 4889/10. ISBN: 978-3-902670-64-9.

**Authors**

**Johannes GOELLNER, Christian MEURERS, Andreas PEER, Guenter POVODEN**
Austrian Ministry of Defence and Sports
National Defence Academy, Departement of Central Documentation and Information Service
Stiftgasse 2a, 1070 Vienna, Austria
{johannes.goellner, christian.meurers, andreas.peer,
guenter.povoden}@bmlvs.gv.at

# D A CH 2014

## D A CH Security 2014

TU Graz – Campus Inffeldgasse, 16. und 17. September 2014

Ziel der Veranstaltung ist es, eine interdisziplinäre Übersicht zum aktuellen Stand der IT-Sicherheit in Industrie, Dienstleistung, Verwaltung und Wissenschaft in Deutschland, Österreich und der Schweiz zu geben. Insbesondere sollen Aspekte aus den Bereichen Forschung und Entwicklung, Lehre, Aus- und Weiterbildung vorgestellt, relevante Anwendungen aufgezeigt sowie neue Technologien und daraus resultierende Produktentwicklungen konzeptionell dargestellt werden.

Themen dieser Arbeitskonferenz sind unter anderem:

- Risiko- und Sicherheitsmanagement
- IT-Compliance
- Incident Handling und Business Continuity
- Identitäts- und Rechtemanagement
- Schutz kritischer Infrastrukturen
- Computerkriminalität und Gegenmaßnahmen
- Security Awareness
- Big Data und Analysetools
- Cloud- und Grid-Computing
- eGovernment, eHealth und eCommerce
- Industriespionage u. Geheimdienstaktivitäten
- Verfügbarkeit und Notfallplanung
- Modellierung von Sicherheit
- Netzneutralität, Netzzugang, Netzsperren
- Sicherheit mit /von Open Source
- Privacy, Datenschutz und Rechtsfragen
- Folgen, Akzeptanz, Trends und Perspektiven

http://www.syssec.at/ds14_cfp/?L=ihwlyftisflitr

Das folgende peer-reviewed Paper wurde auf der Konferenz präsentiert. Der Tagungsband war zu Redaktionsschluss dieses Bandes noch nicht verfügbar, daher liegen keine expliziten Copyright-Restriktionen vor.

# Entwicklung einer Test-Umgebung für Risiko-Assessmenttools

*Stefan Schauer, Johannes Göllner, Andreas Peer, Stefan Rass*

**Zusammenfassung:** Das sogenannte Doppelvektormodell umfasst Klassifikationsmethoden, um mögliche Strategien bei einem Angriff auf eine Kommunikationsinfrastruktur einzugrenzen. Im vorliegenden Beitrag beschreiben wir die Anwendung des Doppelvektormodells anhand eines Risiko-Assessments des Kommunikationsnetzwerks eines fiktiven Unternehmens namens „Pharma AG". Diese wurde im Rahmen des Projekts RSB (Risikomanagement für simultane Bedrohungen) als virtuelle Organisation zu Evaluationszwecken und als Demonstrator für neue Verfahren des quantitativen Risikomanagements definiert. Es wurde hierbei ein global agierendes Unternehmen mit etwa 18.000 Mitarbeitern in Zweigstellen auf allen Kontinenten entworfen. Der vorliegende Beitrag beschreibt die Details dieses Testfalls für Risiko-Management und demonstriert hieran die Anwendung des Doppelvektormodells für die Identifikation von Angriffsstrategien. Darüber hinaus bestehen potentiell Anwendungen der fiktiven Unternehmensstruktur der Pharma AG auch über die Projektziele hinaus im Sinne der Entwicklung und Evaluierung neuer Risiko-Assessment Methoden.

## 1 Einleitung

Risiko-Management stellt ein zentrales Werkzeug für die Sicherheit innerhalb von Organisationen dar, das im Wesentlichen auf die Erfahrung und die Kenntnis von Best Practice Methoden aufbaut. Diese bestehen primär aus einer, durch systematische Methoden, Expertenwissen und Erfahrung gestützten, Einschätzung der Risiko-Situation basierend auf Modellen der Geschäftsprozesse und der Infrastruktur innerhalb der Organisation. Damit unterstützen diese Modelle die Identifikation von potentiellen Risiken und die Entwicklung von entsprechenden Schutzmaßnahmen. Ein quantitativer Ansatz für das Risiko-Management steht dabei meist nicht im Vordergrund, da der Aufwand für den Entwurf eines entsprechend hochwertigen Modells dessen Mehrwert übersteigen kann.

Die Entwicklung neuer allgemeiner Verfahren und Methoden zur qualitativen oder quantitativen Risikobewertung gestaltet sich, aufgrund potentiell fehlender Möglichkeiten das Verfahren in realen Infrastrukturen zu testen, oftmals schwierig. In Ermangelung von Infrastrukturen für experimentelle Evaluationen im Bereich Risiko-Management wurde daher innerhalb von RSB eine fiktive Organisation definiert (siehe [RaGP13]), in welcher neue Risiko-Managementverfahren evaluiert und bewertet werden können, um den Reifegrad einer Best-Practice oder Empfehlung untersuchen bzw. belegen zu können. Neben diesem primären Anwendungsfall für die nachfolgend vorgestellte Infrastruktur, welche *explizit nicht* auf Anwendungen innerhalb des RSB-Projektes beschränkt ist, setzen die meisten Risiko-Managementverfahren auch eine umfassende Identifikation von potentiellen Angriffsstrategien voraus. Speziell dieser Vorgang kann durch das sogenannte Doppelvektormodell [GMPP11], [GMP+14], [Göll09] unterstützt werden.

In diesem Artikel wollen wir die, im RSB-Projekt entwickelte, fiktive Organisation beschreiben und auf ihre Anwendung im Rahmen des Risiko-Managements eingehen. Dafür geben wir in Abschnitt 2 eine kurze Übersicht über das RSB-Projekt und die im RSB-Prototyp verwendeten, Methoden. In Abschnitt 3 gehen wir genauer auf die Modellierung und den Aufbau der fiktiven Organisation sowie die Charakteristika des Doppelvektormodells ein. Schließlich beschreibt Abschnitt 4 in Grundzügen den Einsatz der beschriebenen Modelle und Methoden in einem Risiko-Assessment.

## 2 Der RSB-Prototyp

Im Projekt „RSB – Risiko-Management für simultane Bedrohungen“ wird ein solches quantitatives Risiko-Management im Bereich der IT-Security von Unternehmen verfolgt. Dies wird durch eine vereinfachte Modellierung der IKT-Infrastruktur mit Hilfe von Elementen der Graphentheorie sowie durch die Verwendung von Algorithmen und Modellen aus der Spieltheorie erreicht (wie auch schon in [ScRR12] und [ScRS12] beschrieben). Die Kommunikationsinfrastruktur einer fiktiven Testumgebung („Pharma AG“) wird hierbei zum Gegenstand und Anwendungsfall einer quantitativen Risiko-Analyse [RaGP13]. Das Projekt wird durch das KIRAS-Programm der österreichischen Forschungsförderungsgesellschaft (FFG) gefördert (Projekt-N. 836287). Beteiligt sind das Austrian Institute

of Technology (als Projekt-Koordinator), die Alpen-Adria-Universität Klagenfurt, die Firma Bechtle IT Systemhaus, sowie das Bundesministerium für Inneres (BM.I) und das Bundesministerium für Landesverteidigung und Sport (BMLVS, Abteilung für Zentraldokumentation und Information / Landesverteidigungsakademie Wien). Als Betreiber hochsensibler Netzwerke fungieren die beiden Ministerien in diesem Projekt zusätzlich als Bedarfsträger.

Zu den Hauptzielen des Projekts zählt der Aufbau einer sicheren Kommunikation innerhalb der IKT-Infrastrukturen eines Unternehmens, wobei simultan das Risiko für Ausfälle, Abhören und Authentizität optimiert werden soll [RSPG13]. Hierfür wird eine Methodik entwickelt, welche eine – im Sinne multikriterieller Optimierung beste – Risiko-Abschätzung für jedes der drei spezifizierten Sicherheitsziele liefert. Zusätzlich werden die potentiell vorhandenen Wechselwirkungen bei der Optimierung der separaten Risiko-Abschätzungen implizit berücksichtigt (erfordern somit keine explizite Modellierung oder Kenntnis eventuell komplizierter Abhängigkeiten). Vergleichbar mit einem Virtual Private Network (VPN) ist der Zweck des RSB-Systems der Aufbau hochsicherer Kommunikationskanäle, welche sowohl verfügbar, als auch vertraulich und authentisch sind. Im Vergleich zu anderen Systemen aus dem VPN-Bereich ist hierbei *keine* Public-Key Kryptographie notwendig, sondern es wird auf codierungstheoretische Ansätze und Verfahren zurückgegriffen. Somit entfällt weitgehend das sonst übliche Zertifikats- und Schlüsselmanagement für diese Art der Kommunikation, welche durch den Einsatz von Public-Key Kryptographie impliziert wäre.

In diesem Zusammenhang wird das Risiko für eine Kommunikation als die Wahrscheinlichkeit für eine Verletzung der drei Sicherheitsziele (Informationsverlust, Ausfall des Kanals oder Einschleusen von Nachrichten) gemessen. Dadurch fällt diese Methode zur Risiko-Bewertung in den Bereich des quantitativen Risiko-Managements. Wir gehen nachfolgend kurz auf die eingesetzten Techniken ein.

### *2.1 Mehr-Wege-Kommunikation*

Wie bereits in [ScRR12] beschrieben, wird im RSB-Prototyp (wie auch schon im Vorgänger-Projekt SERIMA [ScRS12]) für die sichere Übertra-

gung der Informationen zwischen Sender und Empfänger die Mehr-Wege-Kommunikation (MWK) eingesetzt (das bekannte One-Time Pad (OTP) Verschlüsselungs-Verfahren stellt einen Spezialfall hiervon dar).
Die MWK bedient sich bei der Übertragung von Informationen mehrerer, disjunkter Wege in einem Kommunikationsnetzwerk. Die zu übermittelnde Nachricht wird in einzelne Teile aufgespaltet und auf diesen Wegen vom Sender zum Empfänger übertragen. Dabei gilt die Annahme, dass ein Angreifer höchsten $(n-1)$ Knoten (bzw. $(n-1)$ Wege) im Netzwerk kontrollieren bzw. abhören kann. Um die Sicherheit der MWK zu gewährleisten, wird die Nachricht mit einem One-Time Pad $k$ verschlüsselt (bitweise XOR-Verknüpfung der Nachricht mit $k$), und $k$ wiederum in $(n-1)$ Teilschlüssel „zerlegt", deren bitweises XOR den Schlüssel $k$ reproduziert. Daraufhin wird die Nachricht zusammen mit den $(n-1)$ Teil-Schlüsseln über $n$ disjunkten Wege übertragen. Um eine Nachricht abzuhören müsste ein Angreifer nun sowohl das Chiffrat als auch alle Teil-Schlüssel der Übertragung besitzen. Nachdem der Angreifer aber maximal $(n-1)$ Teile abhören kann, ist es ihm nicht möglich, die Nachricht aus den abgehörten Informationen zu rekonstruieren. Dies ist erst beim Empfänger möglich, da er alle $n$ Teile der Nachricht erhält.

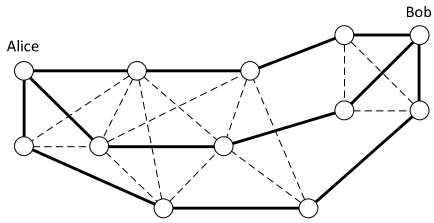



**Abb. 2:** Mehrwegeübertragung auf 3 Pfaden

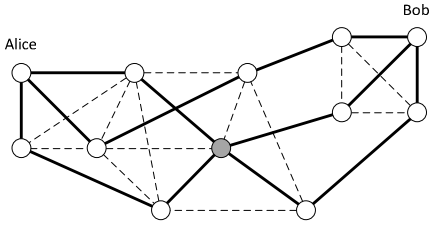



**Abb. 3:** Problem bei kreuzenden Pfaden

Ein Vorteil dieser Kombination aus MWK und OTP besteht darin, dass *kein* Schlüsselaustausch wie etwa durch Public-Key Infrastrukturen erfolgen muss, da sowohl das Chiffrat als auch der Schlüssel vom Sender erzeugt und übertragen werden. Wie oben beschrieben garantiert dabei die MWK,

dass durch die Übertragung des Schlüssels die Sicherheit des Chiffrats nicht kompromittiert wird. Sollte nämlich ein Angreifer alle $(n-1)$ Teil-Schlüssel abfangen und den ursprünglichen Schlüssel rekonstruieren, so kann er dennoch nichts mit dieser Information anfangen, da bei der nächsten Übertragung ein neuer Schlüssel verwendet wird (*one-time* pad). Somit entfallen sonst übliche Mechanismen zur Verteilung und dem Management von Schlüsseln.

Diese Kombination der One-Time-Pad Verschlüsselung mit der Mehr-Wege-Kommunikation stellt im Wesentlichen das einzige, klassische Verfahren zur informationstheoretisch sicheren Übertragung von Informationen dar, wie in [WaDe08] untersucht und gezeigt wurde.

### *2.2 Risiko-Assessment und Spieltheorie*

Es bleibt anzumerken, dass in den meisten, heute verwendeten Netzwerk-Strukturen von Unternehmen es oft nicht möglich ist, die, für die MWK benötigten, *n* disjunkten Pfade von einem Sender zu einem Empfänger zu realisieren. Vielmehr gibt es bestimme Punkte in einem Netzwerk (Switches, Router, etc.) über die eine Vielzahl von Kommunikationspfaden führen und somit einen potentiellen Angriffspunkt bei einer MWK bilden. Ein Angreifer hätte somit die Möglichkeit, Informationen über die übertragene Nachricht zu erhalten, auch wenn er lediglich $(n-1)$ oder auch weniger Pfade abhören kann. Daher besteht die Grundüberlegung der im RSB-Prototyp angewendeten spieltheoretischen Methode darin, die Kommunikationspfade *zufällig* zu wählen. Dies geschieht in einer Weise, dass dem Angreifer eine möglichst geringe Chance bleibt, aus den abgehörten Daten Informationen über die ursprüngliche Nachricht abzuleiten (*Risiko-Streuung*).

Im RSB-Prototyp (sowie auch im Vorgänger-Projekt SERIMA) wird die Netzwerk-Struktur als ungerichteter Graph dargestellt, wobei jede (aktive) Komponente im Netzwerk als Knoten und jeder physikalische Kanal als Kante modelliert wird. Zudem gibt es zwei ausgezeichnete Knoten, Alice und Bob, die als Sender bzw. als Empfänger auftreten. Wie im vorherigen Abschnitt beschrieben wird eine Nachricht $m$ vom Sender Alice in mehre-

re Teile $m_1, m_2, \ldots, m_n$ zerlegt und über die $n$ Pfade $p_1, p_2, \ldots, p_n$ im Netzwerk an den Empfänger Bob gesendet. Dieser erhält nun die $n$ Teil-Nachrichten und kann daraus (und nur daraus) wieder die ursprüngliche Nachricht $m$ rekonstruieren.

Die Strategie des Angreifers ist es nun, eine maximale Anzahl von Knoten unter seine Kontrolle zu bringen, um die darüber übermittelten Teil-Nachrichten $m_i$ abzuhören. Eine entsprechende Strategie des Senders ist es, die Übertragung der Teil-Nachrichten so durchzuführen, dass die Chance des Angreifers, diese Nachrichten abzuhören, so gering wie möglich ist. Diese beiden Strategien lassen die Übertragung als „Nullsummenspiel" modellieren. Ein Nullsummenspiel ist dadurch charakterisiert, dass der Gewinn der einen Partei gleichzeitig den Verlust der anderen Partei darstellt. Im angegebenen Fall ist somit das Abhören einer Nachricht gleichgesetzt mit dem Verlust vertraulicher Information. Formal kann man den Gewinn (aus Sicht des Senders) folgendermaßen festlegen:

$$u(x,y) = \begin{cases} 1, & \text{falls die Übertragung erfolgreich und geheim blieb} \\ 0, & \text{sonst.} \end{cases} \quad (1)$$

Hierbei stellen $x$ und $y$ die jeweiligen Strategien des Senders und des Empfängers dar. Diese lassen sich mathematisch als Wahrscheinlichkeitsverteilungen über den zugehörigen Aktionenräumen $PS_1$ und $PS_2$ des Senders und des Angreifers beschreiben, wobei die Menge $PS_1$ die Menge aller Parameter des Senders (z.B. die gewählten Pfade zur Übertragung der Nachricht) und die Menge $PS_2$ die Menge aller Parameter des Angreifers (z.B. die durch den Angreifer kontrollierten Knoten) darstellt. Für die Erfolgswahrscheinlichkeit

$$v := u(x^*, y^*) \geq u(x^*, y) \text{ für } \textit{beliebiges } y. \quad (2)$$

Im Detail bedeutet dies, dass der Gewinn für den Sender stets größer oder gleich dem Gewinn ist, welcher sich ergibt, wenn der Angreifer sich anders verhält als durch das Nullsummenspiel prognostiziert. Obgleich eine Nullsummenspielannahme dem Angreifer ein sehr bestimmtes (und in Folge

dessen wahrscheinlich nicht reales) Verhalten unterstellt, kann gezeigt werden [Rass09], dass die oben angeführte Ungleichung **Fehler! Verweisquelle konnte nicht gefunden werden.** eine *scharfe* Schranke darstellt, welche auch bei anderem Verhalten des Angreifers erreicht werden kann.

Der Wert $\rho := 1 - v$ stellt somit eine quantitative Risiko-Schätzung für die Wahrscheinlichkeit eines Angriffes auf die Übertragung einer Nachricht im gegebenen Kommunikationsnetzwerk dar (vgl. [AcRa05] für einen verwandten Ansatz). Der RSB-Prototyp ermittelt nicht nur diesen Wert $\rho$, sondern auch die dadurch notwendige Auswahl der Kommunikationspfaden im Netzwerk. Die Gewährleistung, dass die Kommunikation auch über diese Wege durchgeführt wird, wird in weiterer Folge von eigens hierfür entwickelten Protokollen und Network-Provisioning-Komponenten übernommen.

### *2.3 Multikriterielle Spiele*

Die in Abschnitt 2.2 beschriebene Methode ist auf die Risiko-Abschätzung (Abschätzung der Wahrscheinlichkeit eines erfolgreichen Angriffs) für eine sichere Übertragung mittels MWK ausgelegt. Neben Abhörsicherheit berücksichtigt das RSB-System auch *Authentizität* und *Ausfallsicherheit* eines Übertragungskanals. Für diese beiden Sicherheitsziele wurden im RSB-Projekt ebenfalls geeignete Übertragungsverfahren (analog zu MWK) eingesetzt.

Die Authentizität einer Nachricht wird dabei durch eine „Mehr-Wege"-Version einer einfachen MAC-Authentifizierungsmethode (message authentication codes) realisiert. Die Methode stützt sich dabei auf einen „Web-of-Trust"-Ansatz, wie er etwa in PGP verwendet wird (vgl. [Zimm92]), bei dem Vertrauensbildung durch „Leumunde" erreicht wird. Die Idee basiert dabei auf der Verifikation einer handschriftlichen Unterschrift: wird eine Unterschrift auf einem Dokument von hinreichend vielen, unabhängigen Personen verifiziert, wird ihre Authentizität anerkannt. Die Umsetzung im RSB-Prototyp verwendet dazu einen geheimen Authentifizierungs-Schlüssel, die ein Sender sich mit seinen *direkt* (physikalisch oder logisch) *verbundenen* Nachbarn teilt und mit dem ein MAC über einer Nachricht verifiziert werden kann. Genauere Details sind in [RaSc10] nach-

zulesen. Die Modellierung und Sicherheits-Analyse im spieltheoretischen Sinne erfolgt analog wie für MWK.

In gleichem Sinne wie Mehr-Wege-Kommunikation und Mehr-Wege-Authentifizierung kann auch Ausfallsicherheit als Spiel modelliert werden, wobei der Spielausgang in diesem Fall anhand der erfolgreichen oder erfolglosen Zustellung der Nachricht gemessen wird. Auch hier verläuft die Analyse analog zu MWK oder der oben skizzierten Authentifizierung.

Die Erweiterung der in Abschnitt 2.2 angeführten Berechnung zur Risiko-Abschätzung kann jedoch nicht direkt auf mehrere Sicherheitsziele durchgeführt werden. Dies beruht insbesondere auf der Eigenschaft der $\leq$-Relation in Gleichung (2), welche bei der Anwendung auf mehrere Dimensionen (also gleichzeitiger Betrachtung mehrerer Sicherheitsziele) nicht mehr transitiv ist. Deshalb wurde für das RSB-Projekt ein axiomatischer Ansatz gewählt (vgl. auch [Rass13], [RSPG13], sowie Vorgängerarbeiten in [Ghos91], [Voor99] oder [AcRa05]), in dem Risiko-Zusicherungen bei mehreren potentiell wechselseitig abhängigen Sicherheitszielen folgendermaßen charakterisiert werden: Gegeben seien $k$ Sicherheitsziele, welche durch die Gewinn-Funktionen $u_1, \ldots, u_k$ (wie in (1) im vorigen Abschnitt definiert) modelliert werden. Diese messen den jeweiligen Erfolg oder Misserfolg einer Übertragung in Abhängigkeit eines Sicherheitsziels Eine sog. *effiziente Risiko-Zusicherung* $(v_1, v_2, \ldots, v_k)$ im Sinne von $k$ gegebenen Zielen, gemessen durch $u_1, u_2, \ldots, u_k$ bei jeweiligen Verhaltensprofilen $(x, y) \in PS_1 \times PS_2$ ist dann charakterisiert durch folgende Eigenschaften:

**Zusicherung**: Es existiert ein Verhaltensprofil $x^*$ (eine Wahrscheinlichkeitsverteilung über $PS_1$), mit der Eigenschaft, dass $v_i \geq u_i(x^*, y)$ für *beliebiges* $y$ (analog möge somit Ungleichung (2) für jedes Sicherheitsziel einzeln gelten), wobei für jedes Sicherheitsziel ein Angriffsprofil $y_i$ existiert, bei welchem genau der Gewinn $v_i$ erreicht wird (die Schranke soll *scharf* sein).

**Effizienz**: Es gibt kein Verhaltensprofil $x' \neq x^*$ für das in allen Belangen

echt bessere Zusicherungen $v_1' > v_1, v_2' > v_2, \ldots, v_n' > v_n$ existieren (d.h. die Zusicherung ist nicht gleichmäßig verbesserbar).

Ein Vorteil dieser Definition vor Risiko-Zusicherung ist, dass kein explizites Modell für die wechselseitigen Abhängigkeiten zwischen den Sicherheitszielen notwendig ist. Vielmehr werden diese Abhängigkeiten durch die Funktionen $u_1, u_2, \ldots, u_k$ berücksichtigt. Zusätzlich wurde im RSB-Prototyp die Möglichkeit geschaffen, einzelnen Sicherheitszielen unterschiedliche Gewichtungen zuzuweisen, um eine individuelle Anpassung der Bedeutung zu ermöglichen. Zusammen mit dem generischen Unternehmensmodell (wie im nächsten Abschnitt genauer beschrieben) bietet das RSB-Projekt einen Ansatz zum Risiko-Assessment, der auf vielfältige Anforderungen zugeschnitten werden kann.

## 3 Modellierung

Für die Risikoanalyse von Kommunikationsbeziehungen – insbesondere bei quantitativen Ansätzen wie im RSB-Projekt – ist es zweckdienlich, die IKT-Netzwerkstruktur des betrachteten Unternehmens als (ungerichteten) Graph darzustellen, in welchem zwei ausgezeichnete Knoten einen Kommunikationskanal aufbauen (möchten). Hierbei entsprechen die Switches, Router, Server etc. im Netzwerk den Knoten und die Verbindungen den Kanten im Graphen. Um die Verwundbarkeit bzw. Angreifbarkeit eines Knotens zu beschreiben, kann dieser durch eine Reihe von Charakteristika genauer spezifiziert werden. Dazu zählen in etwa die physikalischen Gegebenheiten des Raumes bzw. generell des Standorts der Hardware, deren Hersteller sowie die installierte Firmware-Version, aber auch Informationen aus dem Bereich Human Resources, z.B. über den Administrator der Hardware. Durch die Abbildung der IKT-Netzwerke und der internen Prozesse eines Unternehmens (wie am Beispiel der „Pharma AG“ im folgenden Abschnitt) lassen sich diese Charakteristika an die unternehmensspezifischen Details anpassen und erlauben somit eine realitätsnahe Darstellung einer Organisationsstruktur für Testzwecke.

In weiterer Folge können anhand der Charakteristika eines Knotens unterschiedliche Angriffsstrategien definiert werden. Um dies konsistent umsetzen zu können, bedarf es einer entsprechenden Kategorisierung, welche

zum Beispiel durch das Doppelvektormodell erreicht werden kann (für Details siehe Abschnitt 3.2).

### *3.1 Virtuelles Unternehmen „Pharma AG“*

Zu Demonstrationszwecken und als Anwendungs- und Testfall für die im Rahmen des RSB Projektes entwickelten Methode und Prototyp-Software wurde ein virtuelles, internationales Unternehmen geschaffen [RaGP13]. Dies sollte dabei helfen, die Anforderungen der Bedarfsträger (BMLVS und BM.I) aus dem Projekt schematisch darzustellen, ohne sensible Informationen über die Netzwerke der beiden Ministerien zu verwenden. Es sei hier darauf hingewiesen, dass mögliche Anwendungen dieses Modells keineswegs auf RSB beschränkt sind, da das Modell allgemein gehalten wurde. Die „Pharma AG“ kann somit auch für das Studium und die Illustration anderer Risiko-Managementmethoden herangezogen werden.

Das betrachtete Unternehmen ist ein weltweit agierender Pharma-Konzern mit drei wesentlichen Produktlinien im Medikamentenbereich (bestimmt durch die Verabreichungsform):

- Tabletten
- Kapseln
- Flüssigkeiten

Insgesamt sind mehr als 18.000 Mitarbeiter in 18 Zweigstellen auf 5 Kontinenten beschäftigt. Dabei wurden sämtliche Strukturen inklusive Mitarbeiter und der entsprechenden IT-Ausstattung modelliert. Der nachfolgenden Abbildung ist die Struktur der Konzernleitung bzw. des Hauptquartiers zu entnehmen.

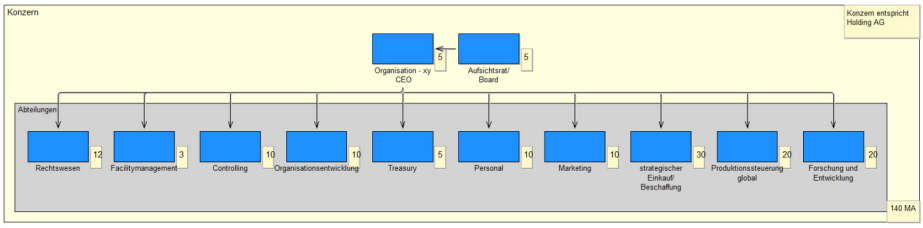



**Abb. 3:** Struktur des HQ [RaGP13]

Für die weitere Analyse wurden neben den konzerninternen Abhängigkeiten die entsprechenden Anbindungen an das Supply Chain Network (wie etwa Energieversorgung, Informations- und Kommunikationstechnologie) der verschiedenen strukturierten Elemente dargestellt. Dadurch ist es in weiterer Folge möglich, Risiko-Betrachtungen durchzuführen.

Im Detail sind für die Risiko-Betrachtung in RSB (aber auch bei alternativen Ansätzen) die Informations- und Kommunikationssysteme von Bedeutung. Hierbei wurde sowohl ein Intranet (firmeninterne Netzwerke), ein Extranet (firmeneigene, gemietete oder selbst betriebene Netzwerke für die Verbindung der Niederlassungen) als auch das Internet (in Form von Providern zugekaufter Kommunikationsdienstleistungen) modelliert.

Die verwendete IT-Infrastruktur ist dabei an Referenz-Architekturen bzw. an Empfehlungen namhafter Hersteller (etwa Cisco) angelehnt, um ein möglichst realitätsnahes Modell zu erhalten (siehe Abb. 4). Im Detail wird zum Zwecke der Ausfallssicherheit eine durchgängig 2-fach redundante Anbindung aller Arbeitsplätze an das Netzwerk angenommen. Im Kern befinden sich zwei Core-Switches (CS), welche sich via Virtual Switching System logisch von außen wie ein einziger Switch verhalten. Jeder Verteilerswitch (VS) ist durch physikalisch getrennte Glasfaserleitungen an jeden der beiden Core-Switche angebunden. Außenstellen werden durch intern betriebene oder extern zugekaufte (gemietete) Glasfaserkabel in einer Ring-Topologie entweder direkt an den beiden Core-Switches oder an zwei Verteiler-Switches angebunden. Der Zugang ins Internet führt über zwei Border-Gateways, welche auch als Firewall agieren.

Dieses Modell ist dabei für jede Niederlassung umgesetzt und entsprechend ihrer Größe und Anzahl der Mitarbeiter angepasst. Als Basis wird eine Versorgung von 1.500 Mitarbeitern angenommen, was somit eine Netzwerkgröße von etwa 60 Switches ergibt (WLAN-Verbindungen wurden hierbei nicht berücksichtigt). Somit ermöglicht das Modell der „Pharma AG“ einen ausführlichen Test von Risiko-Bewertungsmethoden, insbesondere der RSB-Methode.

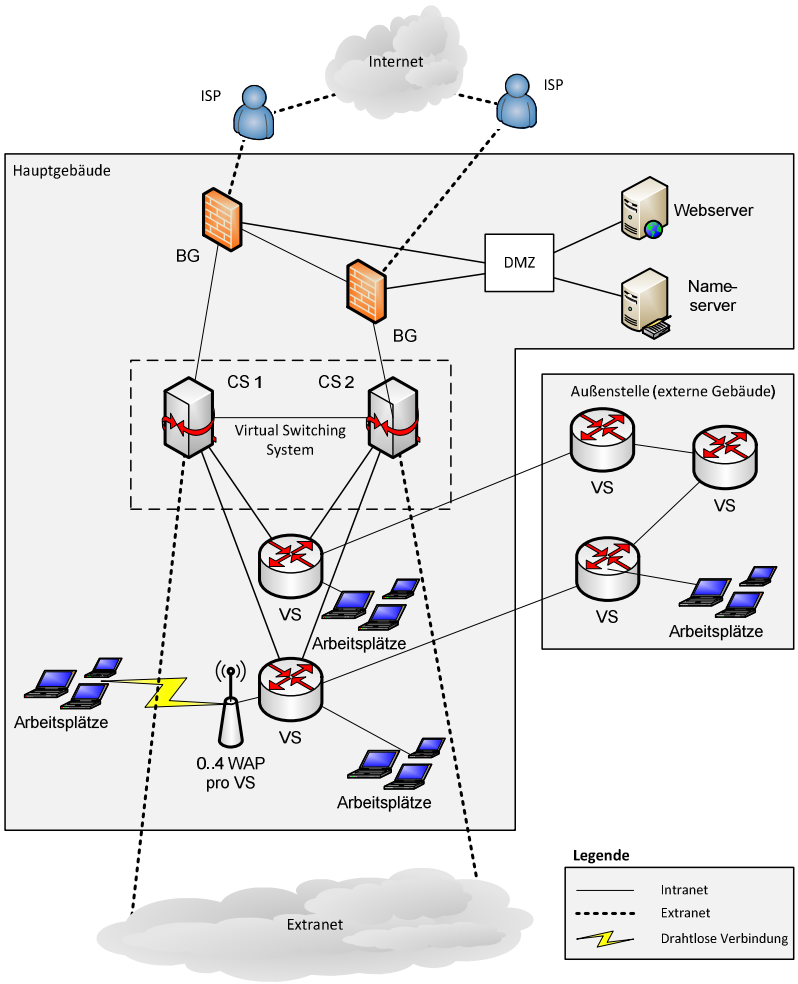



**Abb. 4:** Netzwerk-Struktur eines Standorts [RaGP13]

### *3.2 Doppelvektormodell*

Die Komplexität von Systemen und die Etablierung einer gemeinsamen Terminologie machen Kategorisierungsmodelle erforderlich, um Systemkomponenten und -elemente klassifizieren zu können. Dieser Ansatz garantiert einen normierten und analytischen Prozess, um Ergebnisse und verschiedene Elemente und Komponenten miteinander vergleichen zu

können. Dazu wurde das sogenannte Doppelvektorenmodell auf Basis einer ersten Kategorisierungsebene (Metakategorisierungsebene) im Rahmen des BMLVS-internen Forschungsprojektes „Szenarioplanung und Wissensmanagement im ÖBH“ im Zeitraum 2010 – 2013 durch Johannes Göllner, Klaus Mak, Christian Meurers, Andreas Peer und Günther Povoden entwickelt [Göll09], [GMPP11], [GMP+14].

Das Doppelvektorenmodell stellt ein dreidimensionales, mehrstufiges Meta-Klassifikationssystem dar, in dem jedes Element über die vektorale Zuordnung von definierten Eigenschaften und Attributen dargestellt und beschrieben werden kann. Die erste Ebene unterscheidet die Ordinaten nach zeitlichen und räumlichen Aspekten und bietet zusätzlich einen organisations- bzw. ebenenspezifischen Abstraktionslevel an (politisch, strategisch, (militär-) strategisch, operativ, taktisch, (gefechts-) technisch).

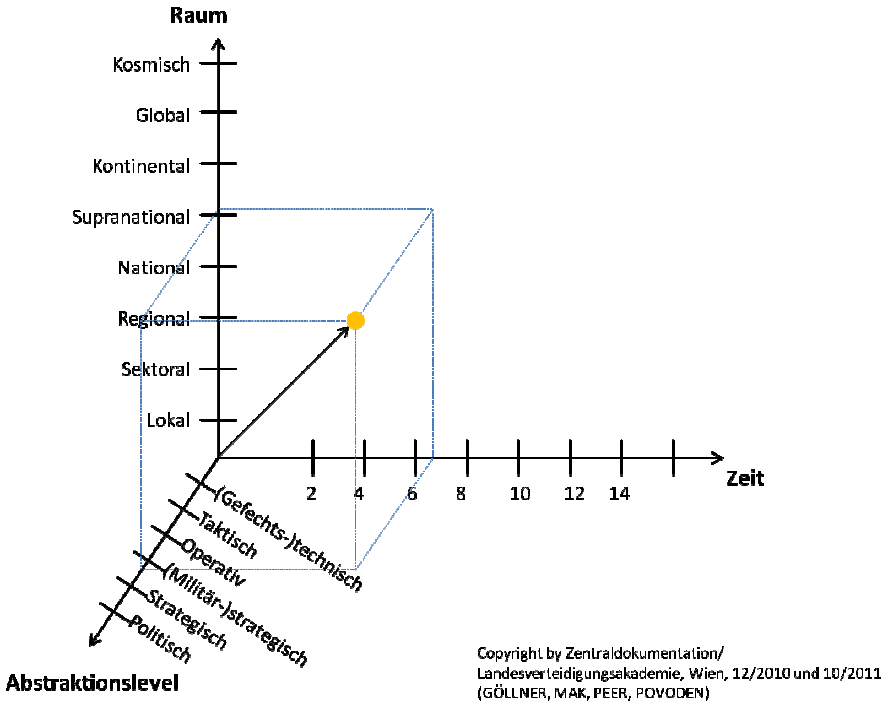



**Abb. 5:** Doppelvektormodell – Vektor 1

In der zweiten Ebenen basiert die Kategorisierung auf der Unterscheidung

eines Ereignisses hinsichtlich des Verursachers und der Einwirkung organisationsimmanenter Gefahren. Zusätzlich wird das Ereignis im Rahmen der Ereignisprinzip-Achse auch unter Berücksichtigung des Ursprunges (terrestrisch, extraterrestrisch) weiter kategorisiert.

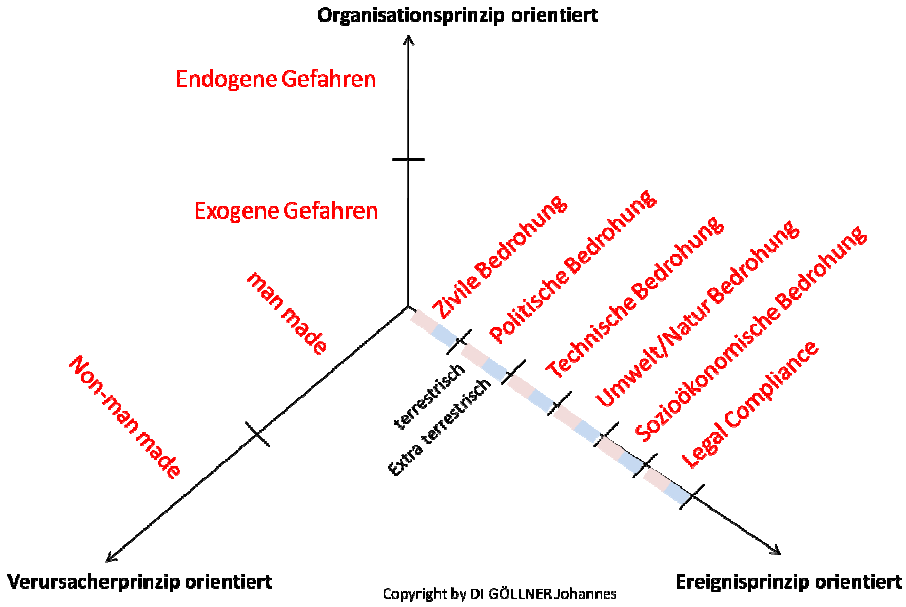



**Abb. 6:** Doppelvektormodell – Vektor 2

Durch das Doppelvektormodell lässt sich prinzipiell jedes Ereignis entsprechend kategorisieren und dokumentieren. In Verbindung mit diversen Akteuren und Wissensrollen lassen sich daraus entsprechend Zusammenhänge und Wechselwirkungen erkennen und ableiten. Ein zusätzlicher Mehrwert ergeht auch aus der Möglichkeit, Muster von Ereignissen in den diversen Kategorien zu identifizieren. Dies dient nicht nur Analysten, sondern kann auch für die Beurteilung von zusätzlich erforderlichem Informationsbedarf zweckmäßig sein.

Auf diese Weise lassen sich unter Anwendung des Doppelvektorenmodelles und der Pharma AG einerseits rasch die wesentlichen (ebenen- bzw. themenspezifischen) Netzwerkknoten identifizieren und zusätzlich die entsprechenden generellen und spezifischen Attribuierungen festlegen. Für eine Anwendung auf ein „reales“ Unternehmen gilt es, entsprechendes,

unternehmensinternes Know How in die Bewertung mit einzubeziehen. Dadurch lassen sich relativ einfach und rasch die spezifischen Parameter, Einflussfaktoren und Attribuierungen eines realen Unternehmens identifizieren.

## 4 Durchführung eines Risiko-Assessments

Die modellierte Pharma AG dient im Rahmen des Projektes RSB als Grundlage zur Entwicklung des Prototyps. Sie kann aber auch als Test-Umgebung für ein Risiko-Assessment im Allgemeinen herangezogen werden. Das Modell der Pharma AG bietet die Möglichkeit, auf Basis einer zwar fiktiven, jedoch realitätsnahen Organisationsstruktur die Einflussfaktoren für die Sicherheit der IKT-Infrastruktur in einem Unternehmen zu analysieren. Entsprechend können im RSB-Prototyp die Knoten des analysierten Netzwerks mit zusätzlichen Informationen annotiert werden, um eine realitätsnahe Beschreibung des Netzwerks zu ermöglichen [RSPG13]. Im Rahmen der derzeitigen Aktivitäten im RSB-Projekt wurden u.a. folgende Einflussfaktoren für diese Knoten des Netzwerks betrachtet:

- Technisch: BIOS-Version, Firmware-Version, Betriebssystem (Version, Servicepack, etc.), Applikations-Software, etc.
- Personal: Administratives Personal, User, Rollen-Modell, etc.
- Lokation: Standort, physikalischer Zugangsschutz (Zutrittskontrollen, Überwachung, etc.), (rollen-basierte) Zugriffskontrollen, etc.

Diese Einflussfaktoren stellen eine Basis für die Sicherheitsanalysen durch den RSB-Prototyp dar. So kann etwa durch diese Faktoren die Angreifbarkeit von bestimmten Knoten bei einer speziellen Angriffsstrategie genauer spezifiziert werden. Nachdem die Pharma AG ein generisches Unternehmen darstellt und der RSB-Prototyp ein weitgehend offenes System ist, können diese Faktoren je nach Bedarf erweitert und angepasst werden, um die konkreten Anforderungen eines realen Unternehmens adäquat widerspiegeln zu können. Dafür ist eine systemische Erfassung der diversen Knoten des Netzwerks im Rahmen eines Risiko-Assessments erforderlich, um die, für ein Unternehmen relevanten Faktoren identifizieren zu können. Die dadurch identifizierten Faktoren können dann zu den bereits beste-

henden hinzugefügt und in die Risiko-Abschätzung des RSB-Prototyps mit einbezogen werden. Auf diese Weise kann in weiterer Folge ein umfassender Katalog an potentiellen Einflussfaktoren erstellt werden. Aufgrund der Verwendung verwandter Systeme und Strukturen innerhalb einer Branche (oder auch branchenübergreifend) ist ein solcher Katalog nicht nur für ein spezielles Unternehmen nützlich, sondern kann auch bei anderen Unternehmen Anwendung finden.

Auf Basis des Doppelvektormodells erfolgt die Erstellung eines Bewertungsmodells, um die identifizierten Einflussfaktoren entsprechend gewichten und bewerten zu können. Dabei wird das Bewertungsmodell so konzipiert, dass es branchen- und unternehmensunabhängig eingesetzt werden kann, was einen wesentlichen Vorteil der Methode gegenüber alternativen Ansätzen darstellt. Der Einsatz des Doppelvektormodells als Kategorisierungsmethode unterstützt dieses Bestreben, da das Modell von seinem Ursprung her bereits auf einem generischen Ansatz basiert und damit kein Anwendungsgebiet a priori ausschließt.

Im Rahmen eines Risiko-Assessments werden nun alle Einträge des Faktorenkatalogs entsprechend den Vorgaben des Bewertungsmodells bewertet und damit die relevanten Faktoren und deren entsprechende Attribute herausgefiltert. In Abhängigkeit der konkreten Anforderungen eines Unternehmens (Zielsetzung, Schwerpunkte, etc.) erfolgt die spezifische Gewichtung der einzelnen Achsen des Doppelvektormodells in Abhängigkeit des gesamten vorliegenden Systems. Daraus resultieren in weiterer Folge sowohl die Bewertungen der einzelnen Knoten, als auch die wesentlichen Faktoren und Attribute für die Analyse, welche dann mit dem RSB-System durchgeführt werden kann.

Gerade diese spezifische Identifizierung von relevanten Einflussfaktoren und Attributen stellt einen markanten Mehrwert der Kombination des Modells der Pharma AG und des Doppelvektormodells dar, da für unterschiedliche Unternehmen die jeweiligen relevanten Aspekte berücksichtigt und als Grundlage für weitere Analyse herangezogen werden können. Durch die Verflechtung des RSB-Prototyps mit dem Modell der Pharma AG kann dieser für eine solche Analyse verwendet werden, wobei sichergestellt ist, dass der Prototyp unabhängig der Unternehmensgröße, des Unternehmensziele oder der Branche zielgerichtet eingesetzt werden kann.

## 5 Zusammenfassung und Ausblick

Das Organisationsmodell des fiktiven Unternehmens „Pharma AG“, welches aus dem RSB-Projekt entstanden ist, kann nicht nur als einzelner Anwendungsfall in dem Projekt gesehen werden, sondern auch als eine generische Test-Umgebung für Risiko-Assessments im Allgemeinen. Durch die detaillierte Abbildung der wichtigsten Aspekte eines global agierenden Unternehmens wird die Basis für ein entsprechend detailliertes Risiko-Assessment geschaffen. Dabei stellt der Bezug zur Pharmaindustrie, der bei der Erstellung des Modells gewählt wurde, keinerlei Einschränkung dar: die Organisationsstruktur kann (eventuell mit kleinen Anpassungen) auf andere Branchen übertragen werden. Gleichsam ist aber durch die Verwendung des generischen Modells der Pharma AG die Methodik bzw. der Prototyp, welcher aus dem RSB-Projekt resultiert, so ausgelegt, dass ein branchenübergreifender Einsatz der in RSB entwickelten Methode selbst ebenso möglich ist.

Aus dem Modell der Pharma AG entsteht die Möglichkeit, einen Faktorenkatalog abzuleiten, in dem sich die konkreten Rahmenbedingungen und Anforderungen eines realen Unternehmens wiederfinden. Ein derart erstellter Faktorenkatalog lässt sich durch die gewonnen Informationen aus einem Risiko-Assessment kontinuierlich erweitern und stellt somit die Basis für weitere Analysen dar. Dafür müssen lediglich die im Modell bestehenden Strukturen hinsichtlich der Abläufe in einem realen Unternehmen zielgerichtet adaptiert und an die organisationalen bzw. baulichen Rahmenbedingungen angepasst werden. Mit Hilfe des Faktorenkatalogs der Pharma AG kann aber bereits ein Großteil der Abläufe in einem realen Unternehmen abgedeckt werden. Durch den Einsatz des Doppelvektormodells lassen sich danach die relevanten Faktoren aus dem bestehenden Katalog herausfiltern und entsprechend der Vorgaben des Unternehmens bewerten. Basierend auf dem generischen Charakter der Pharma AG sowie des Doppelvektormodells lassen sich in weiterer Folge Muster für andere Unternehmen ableiten.

## Literatur


- [AcRa05] F. Acosta Ortega, C. Rafels Pallarola: “Security Strategies and Equilibria in Multiobjective Matrix Games”. Working

Papers in Economics 128, Universitat de Barcelona. Espai de Recerca en Economia (2005).

- [Ghos91] D. Ghose: "A necessary and sufficient condition for Pareto-optimal security strategies in multicriteria matrix games". Journal of Optimization Theory and Applications, 68, 3 (1991), 463–481.
- [GMPP11] J. Göllner, C. Meurers, A. Peer, G. Povoden: "Hybridisation of Social Network Analysis in Context with other Methods for a Scenario Based Risk Analysis-Case Study: Critical Infrastructure for Energy Security in Austria". In: 7th Social Network Conference, University of Greenwich, London, (2011)
- [GMP+14] J. Göllner, C. Meurers, A. Peer, L. Langer, M. Kammerstetter: „Bedeutung des Risikomanagements von Smart Grids". Symposium Energieinnovation 2014, Graz, (2014)
- [Göll09] J. Göllner, „Definition iRd LV Risikomanagement", Vorlesungspräsentation an der Donau Universität Krems iRd ULG Risk Management, (2009)
- [RaGP13] S. Rass, J. Göllner, A. Peer: RSB Deliverable. "Beschreibung einer fiktiven Unternehmensstruktur". Deliverable iRd RSB Projekts, (2013)
- [RaSc10] S. Rass, P. Schartner: "Multipath Authentication without shared Secrets and with Applications in Quantum Networks". In: Proceedings of the International Conferenceon Security and Management (SAM), CSREA Press (2010), Bd. 1, 111-115.
- [Rass09] S. Rass: "On Information-Theoretic Security: Contemporary Problems and Solutions", Dissertation, Alpen-AdriaUniversität Klagenfurt, 2009.
- [Rass13] S. Rass: "On Game-Theoretic Network Security Provisioning". Springer Journal of Network and Systems Management, 21, 1 (2013), 47-64.
- [RSPG13] S. Rass, S. Schauer, A. Peer, J. Göllner: „Sicherheit auf Basis Multikriterieller Spieltheorie". DACH Security 2013, Nürnberg; 17.09.2013 - 18.09.2013; in: P. Schartner, J. Trommler: „DACH Security 2013", S. 289 - 301, (2013)
- [ScRR12] S. Schauer, S. Rass, B. Rainer: „IT-Security Risiko Management mit Elementen der Spieltheorie". In: P. Schartner, J. Taeger (Hrsg.), *DACH Security 2012*, syssec (2012), 106-117.

- [ScRS12] S. Schauer, B. Rainer, R. Schmid: „Ein spieltheoretischer Ansatz für das IT-Security-Risikomanagement“. Datenschutz und Datensicherheit DuD, 7, S. 492 – 496, (2012).
- [WaDe08] Y. Wang, Y. Desmedt: “Perfectly Secure Message Transmission Revisited”, in IEEE Transactions on Information Theory, 2008, vol. 54, S. 2582-2595.
- [Zimm92] P. Zimmermann: “PGP Pretty Good Privacy / Web of Trust”, 1992, http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

**Autoren**

**Stefan Schauer**
AIT Austrian Institute of Technology GmbH
stefan.schauer@ait.ac.at

**Johannes Göllner, Andreas Peer**
Referat Wissensmanagement der Abteilung Zentraldokumentation und Information der Landesverteidigungsakademie Wien des Bundesministeriums für Landesverteidigung und Sport (BMLVS)
{johannes.goellner | andreas.peer }@bmlvs.gv.at

**Stefan Rass**
Alpen-Adria Universität Klagenfurt, Forschungsgruppe Systemsicherheit am Institut für Angewandte Informatik
Klagenfurt, Österreich
stefan.rass@aau.at

## European Intelligence and Security Informatics Conference (EISIC) 2013

*The Premier European Conference on Counterterrorism and Criminology*
Uppsala, Sweden, 12th-14th August 2013

Intelligence and Security Informatics (ISI) research is an interdisciplinary research field involving academic researchers in information technologies, computer science, public policy, bioinformatics, medical informatics, and social and behavior studies as well as local, state, and federal law enforcement and intelligence experts, and information technology industry consultants and practitioners to support counterterrorism and homeland security missions of anticipation, interdiction, prevention, preparedness and response to terrorist acts. The annual IEEE International ISI Conference series (http://www.isiconference.org) was started in 2003.

http://www.eisic.eu/eisic2013/

The following peer-reviewed paper was published in the conference proceedings: Brynielsson, Joel, Johansson, Fredrik, 2013 European Intelligence and Security Informatics Conference, EISIC 2013, Proceedings, IEEE computer society

# Integration of Media Sources for Situation Analysis in the Different Phases of Disaster Management

*Gerhard Backfried, Johannes Göllner, Gerald Quirchmayr, Karin Rainer, Gert Kienast, Georg Thallinger, Christian Schmidt, Andreas Peer*

**Abstract:** In this paper we describe work in progress on a cross-media content analysis approach and framework, which is currently being developed within the QuOIMA project. We describe the role of media, and how possible links between social and traditional media and terminology and communication patterns are envisioned to be connected to the different phases of a disaster model. The paper continues with a discussion of potential benefits for decision makers and planners and concludes with an outlook on further planned activities and developments.

**Keywords:** disaster management, risk management, multimedia processing, network analysis, speech processing, situational awareness, open source information

## I Introduction

Traditional media have a long history in covering disasters and crises. As several examples of recent natural disasters have shown, social media can provide additional useful and effective information which in turn can lead to significantly improved situational awareness for decision makers and planners[1],[2]. Social media combine with traditional media in various ways – sparking off initial coverage, providing different and unfiltered angles or amplifying information – and produce a wide spectrum of coverage of an event. In the process, the boundaries between social media and traditional media and the different types of sources have become increasingly blurred

[1] Kwang-Hoong, L. / Mei-Li, L. The Fukushima Nuclear Crisis Reemphasized the Need for Improved Risk Communication and Better Use of Social Media. Health Physics 103 (3): 307-310.

[2] Tyshchuk, Y. et al. Social Media & Warning Response Impacts in Extreme Events: Results from a Naturally Occuring Experiment. 2012 45th International Conference on System Science (HICSS): 818.

as news providers use social media as alternative channels. As helpful as all this information may potentially be to disaster relief organizations, it usually comes in multiple formats, multiple languages, immense amounts, across multiple media and is generally unstructured and inhomogeneous. Stakeholders have to survive in this dynamic world with a 24-hour news-cycle and manage information and communications. Events will be reported about – whether they participate or not – putting pressure on them to compete and fill the information void[3].

To help meet this challenge, the QuOIMA project[4] has embarked on developing representative scenarios and models to demonstrate how extensions of existing technologies can be applied to improve the situational awareness and knowledge of decision makers. The approach described in this paper is technologically based on the SAIL LABS Media Mining System (MM-System), an open source information (OSINF) platform, and strategically based on a five-phase disaster management model developed at the National Defence Academy of the Austrian MoD. Together they form the framework within which the QuOIMA project tries to improve situational awareness in the area of natural disasters.

## II The Role of Media in Disaster Management

Traditional media, such as TV, radio and web-sources have long been employed to provide information about crises and disasters. Even today, depending on the infrastructure and social factors, these media may still form an important and highly additive source of information. With the advent of social media, the way people communicate, search for and receive information has undergone a radical transformation. Not only have social media changed the way people communicate in their day-to-day lives, but also - and increasingly so - during emergencies and crises. Effectively it can already be assumed, that in many cases a part of the population will indeed

---

[3] Holmes, W., Crisis Communication and Social Media: Advantages, Disadvantages and Best Practices, Univ. of Tennessee, CCISymposium, 2011, Knowville, USA

[4] QuOIMA, Quellenoffene, Integrierte Multimedia Analyse, http://www.kiras.at/gefoerderte-projekte/detail/projekt/quoima-quelloffene-integrierte-multimedia-analyse/ on 04/30/2013

turn to social media during crises[5]. Particularly micro-blogging systems like Twitter, with an open communication structure, play an important role in this respect and form a new way to disseminate and receive crisis information[6,7] . Engaging with and using emerging social media to interact and intervene may place the crisis response community in a better position to respond to disasters on a timely, broad and citizen-involving basis. Social media lend themselves to two-way communication, thus allowing data to be gathered as well as distributed using these channels. This type of communication is valued not only because it allows first responders to send important disaster-related information to the persons who need it most, but also because it allows them to include critical updates from individuals who experience the incident or crisis first hand. The public has thus turned into an important participant in the crisis management community – everyone has turned into a potential watchdog[3]. People share their observations, opinions and emotions and communicate through social media thus acting as a crowd-sourced means to gather and disseminate data. The active dissemination of information, communication with affected persons or mere observers, corrective measures such as clarifying rumors or correcting misinformation form just a few of the possible patterns for outbound communication from the perspective of crisis response organizations[8].

For decades, communities and the public have been relying on specific groups to assist in times of disaster. But the present day communications environment with its new and increased expectations has changed the game, not just for first responders, but also for the general public[9]. (Near) Real-time communication/information, personal involvement, reliable, critically-challenged and -questioned sources, as well as multi-media con-

---

5 Johansson, F., Brynielsson, J., Narganes Quijano, M., Estimating Citizen Alertness in Crises using Social Media Monitoring and Analysis, EISIC 2012, Odense, Denmark

6 Nilsson, J. et al, Making use of New Media for Pan-European Crisis Communication, ISCRAM 2012, Vancouver, Canada

7 Bruns, A., Burgess, J., Crawford, K. and Shaw, F., #qldfloods and @QPSMedia: Crisis Communication on Twitter in the 2011 South East Queensland Floods, 2012, Brisbane: ARC Centre of Excellence for Creative Industries and Innovation

8 Mendoza, M., Poblete, B., and Castillo, C., Twitter Under Crisis: Can we trust what we RT?, SOMA 2010, Washington D.C., USA

9 American Red Cross, The Case for Integrating Crisis Response with Social Media, White Paper, 2010

tent are common requirements and assets of currently shared information. The technology is constantly evolving which will result in people having even higher expectations of first responders and vice-versa. Affected persons may indeed *expect* authorities to respond quickly to information provided via social media[3]. There remains no doubt that the impact of social media on crisis communication is already significant and will only continue to grow in significance in the years to come.

## III Existing Work and Case Studies

Recent events illustrate the active use of new technologies in crisis-situations. During the South East Queensland floods of 2011, social media played a central role in crisis communication. In particular the Queensland Police Service used Twitter to communicate effectively with affected people[10] . The use of social media has been studied in the course of various natural disasters, such as the earthquakes in New Zealand[11], Haiti[10], Chile[8], and the US[12], grassfires in the US[13], or hurricanes Ike and Gustav 2008[14], typhoons in the Philippines and floods in Brazil[15].

Reference[6] provides an overview of social media in the context of crisis information. They find that media – traditional as well as social – form an important source for sending out and retrieving information about different aspects of a crisis or disaster. In particular they examine various approaches and channels which can be used for dissemination of crisis-

[10] Dugdale, J., Van de Walle, B., Koeppinghoff, C., Social Media and SMS in the Haiti Earthquake, SWDM 2012 Workshop, Lyon, France

[11] Bruns, A., Burgess, J., Crawford, K. and Shaw, F., #qldfloods and @QPSMedia: Crisis Communication on Twitter in the 2011 South East Queensland Floods, 2012, Brisbane: ARC Centre of Excellence for Creative Industries and Innovation

[12] Earle, P., et al. OMG Earthquake! Can Twitter Improve Earthquake Response?, Electronic Seismologist 2010

[13] Starbird, K., Palen, L., Pass It On?: Retweeting in Mass Emergency, ISCRAM 2010, Seattle, USA

[14] Lee Hughes, A., Palen, L., Twitter Adoption and Use in Mass Convergence and Emergency Events, ISCRAM 2009, Gothenburg, Sweden

[15] Nagar, S., Aaditeshwar, S., Joshi, A., Characterization of Social Media Response to Natural Disasters, SWDM 2012 Workshop, Lyon, France

relevant information. [16,8] and [14] elaborate on the structure and types of communication which emerge on Twitter, [3] does so particularly for the crisis-case. [17] provides an overview of social media in the disaster context using a set of case spotlights covering specific events. [7] provides an in-depth and comprehensive overview of how social media played a role during the 2011 Queensland floods. [18] focuses on the connection between Twitter and TV from the point of view of how to combine social network interaction with programming. [19] provides a brief overview of existing and potential future uses of social media in disasters. Relatively little attention seems to have been paid to the actual use of language in the context of social media and natural disasters: [8] and [20] deal with this topic to some extent.

Reflecting events such as natural disasters and acknowledging the importance that social media play in them, various research projects aim at improving the effectiveness of communication and alerting during crises. For example, in the FP7 project Alert4All[21], the screening of new media (SNM) tool [6] serves to enhance situational awareness among crisis management personnel with regard to public opinions and emotions found in on-line web content from tweets, blogs, and other social media. In the FP7 project MASSCRISCOM[22] social media is likewise taken into account as an emerging means of mass communication in crisis situations. MASSCRISCOM focuses on the changing demands of the communication systems. However, the strengths and possibilities as well as the risks and weaknesses of use are only addressed superficially.

---

[16] Kwak, H, Lee, C., Park H., Moon S, What is Twitter, a Social Network or a News Media, WWW 2010, Raleigh, USA

[17] Faustino, J.D., Liu, B., Jin, Y., Social Media During Disasters: A Review of the Knowledge Base and Gaps, Final Report to Human Factors/Behavioral Sciences Division, U.S. Department of Homeland Security, College Park, USA, 2012

[18] Harrington, S., Highfield, T. Bruns, A., More Than a Backchannel: Twitter and Television, 2012 COST Action ISO906 Transforming Audiences, Transforming Societies

[19] Lindsay, B., Social Media and Disasters: Current Uses, Future Options, and Policy Considerations, Congressional Research Service, 2011

[20] Bryden, J., Funk, S., Jansen, V., Word usage mirrors community structure in the online social network Twitter, EPJ Data Science 2013

[21] Alert4all, http://www.alert4all.eu on 04/30/2013

[22] MASSCRISCOM, http://www.masscriscom.eu on 04/30/2013

In the Austrian Security Research Program KIRAS, the meta-study SMD4Austria[23] is centered on an overall evaluation of social media use in police work including risk- and crisis communication. Another KIRAS project, MDL[24] which concentrated on the use of multi-media data for situational awareness, provides some of the infrastructure and setup that the QuOIMA project builds upon.

Besides the various research-projects, actual on site use of social media for crisis and disaster management is already practiced e.g. in Australia by the Queensland Police via the @QPSMedia Twitter account[7]. Its use during the 2011 floods forms one of the most important success stories of social media in crisis communication to date.

## IV. THE QUOIMA PROJECT

The QuOIMA project aims at fusing diverse and complementary sources of information – in particular social media and traditional media - and at allowing decision makers to *make sense* of a large, multi-lingual and inhomogeneous body of mixed data. Users are enabled to access data from different modalities just minutes after they have been published and perform various types of visual analytics activities by connecting and inter-linking information from different sources and types of media. The early detection of structures and patterns of communication are expected to allow users to react earlier, swifter and more adequately in situations of crisis or disaster. The *fusion-approach* contrasts the QuOIMA project with most research on the use of social media in the scope of disaster management, which mainly focuses on individual social channels such as Twitter. In addition, to a large extent the work carried out to date is typically performed on English data only, whereas the QuOIMA project emphasizes a multi-lingual approach.

Studying changes in language and terminology as well as of patterns of

[23] SMD4Austria, Social Media Dienste für Sicherheit und Prävention in Österreich, http://www.kiras.at/gefoerderte-projekte/detail/projekt/smd4austria-social-media-dienste-fuer-sicherheit-und-praevention-in-oesterreich/ on 04/30/2013

[24] Backfried, G., Aniola, D., Quirchmayr, G., Winiwarter W., Mak, K., Pilles, HC., Meurers, Ch., Köstinger, M., Wohlhart, P., Roth, P., Open Source Intelligence am Beispiel von KIRAS/MDL Multimedia Documentation Lab, 9.Sicherheitskonferenz, Krems, Austria, 2011

communication stretching across social media and traditional media (e.g. tweets linking to web-pages, quotes in tweets, quotes originating from TV being re-used by social media) as well as integrating results from visual analysis form areas of investigation. The detection and classification of such patterns may lead to the subsequent assignment of affected groups of citizens to particular phases of a disaster - not all affected persons might be in the same stage, e.g. flooding may be at its height for some part of the population whereas for others it may actually already have passed – which may allow for improved and finer-grained situational awareness regarding the overall scenario.

Communication and language patterns will be put into context within a newly proposed model of disasters which has been developed at the National Defence Academy of the Austrian MoD by Johannes Göllner and Andreas Peer[25]. The five phases of the model are depicted in Figure 1.

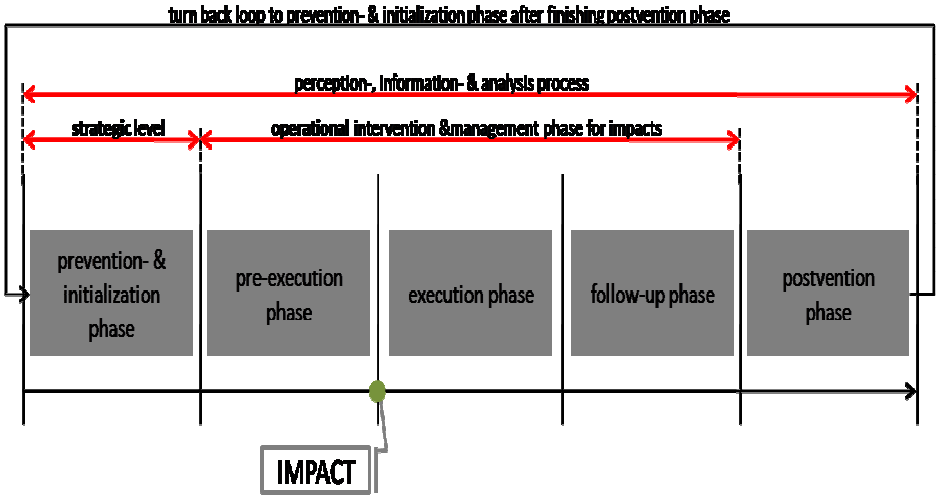



**Figure 1 Five-phase disaster model**

The perception, information, and analysis processes of the model in combination with identified patterns of communication are used to investigate,

[25] KIRAS-Antrag Kooperative F&E-Projekte: Modellbildungs- und simulationsgestützte Entscheidungsunterstützung in der Last-Mile-Katastrophenbewältigung (LMK-MUSE), 28.02.2013, S. 18.

design and develop a generic model of risk- and crisis communication. In particular communication patterns and their connection and relation to the respective phases will be investigated.

As the QuOIMA project focuses on the harvesting and collection aspects of information from the point of view of a first responder or crisis manager, emphasis is placed on the gathering and analysis of (incoming) information, rather than the management of active (outgoing) communication.

Figure 2 depicts a few of the numerous possible cross-media communication patterns expected to occur, to be detected and to be associated to individual phases of a disaster. Particular terminology and usage patterns might be attributed to each of the links in the graph according to the particular phase of a disaster.

The association of particular terminology as well as of communication patterns with phases of a disaster is expected to allow first responders to assess more effectively what stage a given part of the population is in and to communicate more effectively and in a more targeted and timely manner. It enables first responders to obtain a common and complete operational picture with a significantly higher resolution regarding the needs and status of individual groups.

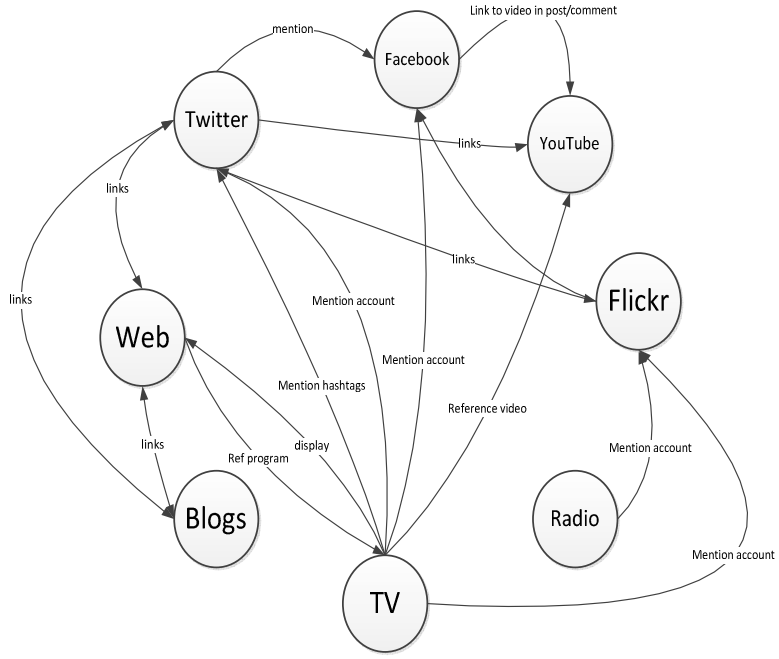



**Figure 2 Cross-media communication patterns**

Technically, the SAIL LABS MM-System forms the framework within which developments in QuOIMA take place. The MM-System is a modular system aiming to cover all activities within the OSINF process. It enables professionals to quickly extract meaningful information and perform analyses from unstructured data in a variety of formats across multiple languages and sources. The MM-System consists of a set of technologies packaged into components and models, combined into a single system for end-to-end deployment[26]. The addition of social media input mechanisms (interfaces) and processing components form some of the recent developments within the MM-System. Further components include the processing of TV, radio and web-content in a variety of languages. Visual analysis, such as the detection of text via on-screen OCR or the classification of scenes as well as interfaces to automatic translation engines form further components in the MM-System.

[26] Backfried, G., Schmidt, C., Pfeiffer, M., Quirchmayr, G., Glanzer, M., Rainer, K., Open Source Intelligence in Disaster Management, EISIC 2012, Odense, Denmark

Together, these technologies form the basis for development within the QuOIMA project. Mechanisms, such as the ones being developed for cross-media fusion of content, are envisioned to be incrementally added to the MM-System with minimal effort, thus allowing for quick transfer of research results to products.

The input mechanisms of the MM-System are also used to collect suitable corpora of data – different types of media, all covering the same natural disasters – an ongoing activity within the project. These corpora are used for model development as well as evaluation purposes.

## V Benefits for Decision Makers and Planners

As stated in [19], monitoring information flows – in our case flows which span multiple media and languages – could help establish and increase situational awareness. Obtaining real-time information as an event unfolds can help officials determine where people are; assess victims' needs, and alert citizens and first responders to changing conditions and new threats.

An analysis of communication content and -patterns might not only lead to improved targeted information to decision makers, but also lead to the identification of structures indicating a specific situation or crisis-phase, such as a the follow-up phase already having started.
From a practical point of view, it is a strategic advantage for decision makers sending in first responders to know how a situation is developing, especially how people affected by a disaster are reacting to the circumstances. Being able to identify certain forms of stress, disappointment, chaos and maybe even a developing tendency to resort to violence against first responders is essential information for team configuration and mission preparation. Being able to detect resilience and self-organized recovery efforts may reduce the requirement for specialized resources.

## VI Privacy

Regarding user-provided content and social media, QuOIMA's goal is clearly to use publicly available (open) sources only and explicitly not to focus on individuals or their means and networks of communication, nor to determine anyone's actual identity. Rather, the scrutiny of privacy and

data protection form essential aspects of the project. For research use apart from emergency situations in which lives or *higher values* are at stake, only consensually provided, open and public information is taken into account, retrieved, compiled, selected and used for the proof of the QuOIMA-concept. It is of importance for the legal compliance[27] of the project that no sensitive personal data are processed.

## VII Outlook and Next Steps

Data collection has been going on since the project's start (11/2012), already yielding several instances of natural disaster coverage across sources (e.g. the recent floods in Central Europe). Models for cross-media clustering of documents (audio, visual and textual) and the detection of links between media are being investigated and developed and will undergo initial stages of evaluation. Should the evaluations be as successful as envisaged, we plan to address further types of first responders, such as the Austrian Red Cross, and to integrate modules into situational awareness centers on a prototypical base.

## VIII References


- Kwang-Hoong, L. / Mei-Li, L. The Fukushima Nuclear Crisis Reemphasized the Need for Improved Risk Communication and Better Use of Social Media. *Health Physics* 103 (3): 307-310.
- Tyshchuk, Y. et al. Social Media & Warning Response Impacts in Extreme Events: Results from a Naturally Occuring Experiment. 2012 45th International Conference on System Science (HICSS): 818.
- Holmes, W., Crisis Communication and Social Media: Advantages, Disadvantages and Best Practices, Univ. of Tennessee, CCISymposium, 2011, Knowville, USA
- QuOIMA, Quellenoffene, Integrierte Multimedia Analyse, http://www.kiras.at/gefoerderte-projekte/detail/projekt/quoima-


[27] Grubmüller, V., et al Analyses Summary Report. Deliverable to the EC within the FP7-ICT-project UniteEurope Social Media Analytics and Decision Support Tools Enabling Sustainable Integration Policies and Measures. 2012 (http://www.uniteeurope.org on 04/30/2013)

quelloffene-integrierte-multimedia-analyse/ on 04/30/2013
- Johansson, F., Brynielsson, J., Narganes Quijano, M., Estimating Citizen Alertness in Crises using Social Media Monitoring and Analysis, EISIC 2012, Odense, Denmark
- Nilsson, J. et al, Making use of New Media for Pan-European Crisis Communication, ISCRAM 2012, Vancouver, Canada
- Bruns, A., Burgess, J., Crawford, K. and Shaw, F., #qldfloods and @QPSMedia: Crisis Communication on Twitter in the 2011 South East Queensland Floods, 2012, Brisbane: ARC Centre of Excellence for Creative Industries and Innovation
- Mendoza, M., Poblete, B., and Castillo, C., Twitter Under Crisis: Can we trust what we RT?, SOMA 2010, Washington D.C., USA
- American Red Cross, The Case for Integrating Crisis Response with Social Media, White Paper, 2010
- Bruns, A., Burgess, J., Crawford, K. and Shaw, F., #qldfloods and @QPSMedia: Crisis Communication on Twitter in the 2011 South East Queensland Floods, 2012, Brisbane: ARC Centre of Excellence for Creative Industries and Innovation
- Dugdale, J., Van de Walle, B., Koeppinghoff, C., Social Media and SMS in the Haiti Earthquake, SWDM 2012 Workshop, Lyon, France
- Earle, P., et al. OMG Earthquake! Can Twitter Improve Earthquake Response?, Electronic Seismologist 2010
- Starbird, K., Palen, L., Pass It On?: Retweeting in Mass Emergency, ISCRAM 2010, Seattle, USA
- Lee Hughes, A., Palen, L., Twitter Adoption and Use in Mass Convergence and Emergency Events, ISCRAM 2009, Gothenburg, Sweden
- Nagar, S., Aaditeshwar, S., Joshi, A., Characterization of Social Media Response to Natural Disasters, SWDM 2012 Workshop, Lyon, France
- Kwak, H, Lee, C., Park H., Moon S, What is Twitter, a Social Network or a News Media, WWW 2010, Raleigh, USA
- Faustino, J.D., Liu, B., Jin, Y., Social Media During Disasters: A Review of the Knowledge Base and Gaps, Final Report to Human Factors/Behavioral Sciences Division, U.S. Department of Homeland Security, College Park, USA, 2012

- Harrington, S., Highfield, T. Bruns, A., More Than a Backchannel: Twitter and Television, 2012 COST Action ISO906 Transforming Audiences, Transforming Societies
- Lindsay, B., Social Media and Disasters: Current Uses, Future Options, and Policy Considerations, Congressional Research Service, 2011
- Bryden, J., Funk, S., Jansen, V., Word usage mirrors community structure in the online social network Twitter, EPJ Data Science 2013
- Alert4all, http://www.alert4all.eu on 04/30/2013
- MASSCRISCOM, http://www.masscriscom.eu on 04/30/2013
- SMD4Austria, Social Media Dienste für Sicherheit und Prävention in Österreich, http://www.kiras.at/gefoerderte-projekte/detail/projekt/smd4austria-social-media-dienste-fuer-sicherheit-und-praevention-in-oesterreich/ on 04/30/2013
- Backfried, G., Aniola, D., Quirchmayr, G., Winiwarter W., Mak, K., Pilles, HC., Meurers, Ch., Köstinger, M., Wohlhart, P., Roth, P., Open Source Intelligence am Beispiel von KIRAS/MDL Multimedia Documentation Lab, 9.Sicherheitskonferenz, Krems, Austria, 2011
- KIRAS-Antrag Kooperative F&E-Projekte: Modellbildungs- und simulationsgestützte Entscheidungsunterstützung in der Last-Mile-Katastrophenbewältigung (LMK-MUSE), 28.02.2013, S. 18.
- Backfried, G., Schmidt, C., Pfeiffer, M., Quirchmayr, G., Glanzer, M., Rainer, K., Open Source Intelligence in Disaster Management, EISIC 2012, Odense, Denmark
- Grubmüller, V., et al Analyses Summary Report. Deliverable to the EC within the FP7-ICT-project UniteEurope Social Media Analytics and Decision Support Tools Enabling Sustainable Integration Policies and Measures. 2012 (http://www.uniteeurope.org on 04/30/2013)

## IX. Acknowledgements

The authors would like to express their gratitude to Mark Pfeiffer for many helpful discussions. QuOIMA is supported by the Austrian National Security Research Development Programme KIRAS.

**Authors**

**Gerhard Backfried, Christian Schmidt**
SAIL LABS Technology AG, Vienna, Austria
{gerhard.backfried, christian.schmidt}@sail-labs.com

**Johannes Göllner, Andreas Peer**
National Defence Academy, Dept. of Central Documentation, Austrian MoD, Vienna, Austria
{johannes.goellner, andreas.peer}@bmlvs.gv.at

**Gerald Quirchmayr**
University of Vienna, Multimedia Information Systems Research Group, Vienna, Austria
gerald.quirchmayr@univie.ac.at

**Karin Rainer**
INSET Research&Advisory, Vienna, Austria
karin.rainer@inset-advisory.com

**Gert Kienast, Georg Thallinger**
Joanneum Research, Inst. for Information and Communication Technologies, Graz, Austria‡
{gert.kienast, georg.thallinger}@joanneum.at

## TIEMS Berlin Conference

*Public alerting and social media during crisis and disasters*
Fraunhofer FOKUS, Berlin, 30th Octobre – 1st November 2013

Recognizing that the conference on "Public alerting and social media during crises and Disasters' held in Fraunhofer FOKUS, Berlin, Germany from 30th October until 1st November was attended by Emergency Management professional and practitioners from 20 countries and was a successful in providing opportunities to discuss important topics such as:

- Use of public sirens warning systems
- Modeling of public dissemination of alerts
- Lessons learn
- Monitoring and analyzing social media channels
- Social media as a sensor
- App's for disaster

Appreciating digital access is not equal around the world. There is a technology divide between the developed and developing world in terms of availability 'smart' phones and Information Technology (IT). Furthermore different generations have different sensitivities to 'new' and 'old' media channels. Also appreciating social media has a role to play in Emergency Management, so it is essential Emergency Managers and Crisis Communication Managers establish a protocol for utilizing the medium.

http://tiems.info/images/TIEMS%202013%20Berlin%20Declaration%20V2.pdf

The following peer-reviewed paper was presented at the conference and – referencing TIEMS copyright policy – does not underlie any copyright restrictions regarding this conference.

# Social Media Information and Analysis for Crisis and Disaster Management

*Hermann Huber, Georg Neubauer, Andrea Novak, Joachim Klerx, Bettina Jager, Klaus Mak, Christian Meurers*

**Keywords:** Social Media, Data Mining, Information Extraction, Crisis and Disaster Management

**Abstract:** Mining Social Media content provides a lot of opportunities for various application domains. This paper investigates opportunities and challenges of mining social media data specifically for crisis and disaster management (CDM). Social Media content can be characterized as vast, noisy, distributed, unstructured and dynamic (Gundecha & Liu, 2012). In order to make use of the enormous amount of potentially useful content, efficient and scalable data extraction and analysis tools may be required. Hence, we introduce some promising basic techniques originating from the data mining research area that can be applied to process social media content in order to eventually generate useful and previously unknown insights for the CDM domain. Those insights may be used to create more accurate prediction models, support crisis managers in the decision making process, reveal influential peers in communication networks or improve the accuracy and the overall process of public alerting. We refer to this process as Social Media Mining (SMM). Utilizing user-generated content in crisis situations induces some additional, rather non-functional issues like privacy, accuracy or reliability concerns. We propose some system design considerations in order to circumvent these issues by design. Furthermore, we describe some common CDM challenges that may be addressed with the use of SMM and emphasize the necessity of combining Social Media and Data Mining techniques by illustrating a practical showcase. Finally, we provide a discussion and assess potentials and risks.

## Introduction

According to a 2011 IDC survey[1] the amount of existing data is estimated to approximately 1.8 zettabytes which is 1.8 trillion gigabytes. Furthermore, the mass of data is doubling every two years. In the same period of time the amount of IT staff is estimated to grow by factor 1.5. In order to make use of this huge mass of data, advanced analysis tools are needed to derive knowledge that is implicitly hidden in that data. During the last decade the popularity of social media as well as the number of participating users increased steadily, e.g. 73 % of wired US teens used social networks in 2010 reflecting an increase by 18 % since 2006. Even though user statistics are still far from being representative regarding the entire society, the tremendous amount of available data encourages the idea of computer supported analysis for CDM purposes. Such data can be used to reveal indications of previously unknown societal parameters like opinions, trends or human behaviour in certain contexts that eventually generate new knowledge relevant for domains such as crisis and disaster management.

The challenge is to collect raw data and transfer it to usable knowledge. Literature provides numerous definitions of the term *knowledge*. (Ackoff, 1989) describes the relation between data and knowledge in the so called Pyramid- or Data-Information-Knowledge-Wisdom-Model (DIKW, see Figure 1). The data layer is the most basic one. According to his definition, data is just non-interpreted symbols. Data observed in a certain context generates information (i.e. the digits "17" is raw data, 17°C is information). Adding context to information pushes it to the next level in the model which is knowledge. The boundary between information and knowledge is not well defined in literature. (Koohang, et al., 2008) describe knowledge as meaningful and useful information (i.e. in winter 17°C is quite much in Austria). The last layer describes wisdom which, according to (Ackoff, 1989), can be perceived as evaluated understanding. Paradoxically, wisdom, the most complex and diffuse DIKW concept is known to mankind since hundreds or thousands of years. At the same time, the rather easy to understand concept of data is young, at least in a linguistic sense. Today it seems

[1] IDC Survey 2011, "Digital Universe Study: Extracting Value from Chaos", http://germany.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf, accessed 11.06.2013

to be impossible for ICT systems to handle the concept of wisdom. However, extracting information from data is a commonly applied, well understood task in various domains. With respect to Ackoff's model, we define the term data in the context of Social Media as highly structured content (e.g. database tables, markup languages, etc.) that can be used as input for algorithms without any further pre-processing. Though, the majority of Social Media content is human readable which is unstructured by nature. Plain text for instance carries a lot of information that is easily extractable by humans. Machines need to pre-process and analyse the symbols in order to extract valuable information like person names or emotions.

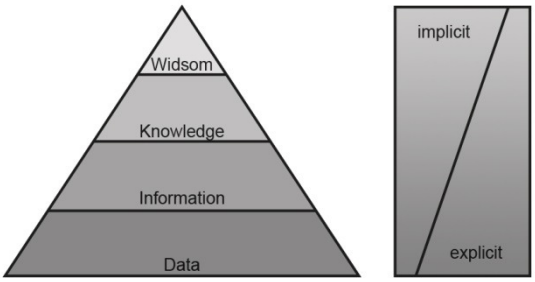



**Figure 1:** Relation between Data, Information, Knowledge and Wisdom (Ackoff, 1989). The representation of the respective concepts is explicit in lower layers and implicit in upper layers. The data mining research area focuses on revealing implicit knowledge from raw input data.

**Data mining** techniques can be used to perform transitions between several DIKW layers. Various research areas are already making use of such transitions. Astronomy for instance uses data mining techniques in order to analyse images taken by telescopes. Discovering supernovae on their early stages is a crucial success factor exploring Dark Energy. Today, astronomers detect about 100 supernovae a year. Once the Large Synoptic Survey Telescope (LSST) will be on duty in 2029 researchers expect to reveal 1000 supernovae per night which in terms of image data is about 30TB (Borne, 2009). Investigating this huge amount of data requires advanced analysis techniques and can hardly be done manually. The data mining research area aims to provide elaborate techniques to reveal knowledge that is implicitly hidden in explicit data.

According to (G.K.Gupta, 2009), Data Mining may be defined as

> "… a collection of techniques for efficient automated discovery of previously unknown, valid, novel useful and understandable patterns in large databases. The patterns must be actionable so that they may be used in an enterprise's decision making process."

This definition comprises all major aspects of the data mining process. First of all it is important to notice that data mining is a collection of techniques, algorithms and software tools rather than a single technology or product. (Liu, 2007) describes data mining as a multidisciplinary field that involves machine learning, statistics, databases, artificial intelligence, information retrieval and visualization. So implementation and configuration of some chosen techniques may differ according to the given use case. Another aspect is to discover previously unknown, valid and novel patterns in large databases. What that means is that ideally, data mining reveals new insights that didn't exist previously rather than to prove or disprove a given hypotheses. The term valid refers to the fact that all newly discovered patterns have to be reproducible and must not be the result of random fluctuation in given data. This is where the amount of data comes into play. Increasing the amount of analysable data will lead to a better significance regarding the validity of a detected pattern.

A very basic data mining technique is the concept of *association rule mining*. Association rules are often applied in shopping chart analysis scenarios to detect which items are purchased together frequently in order to place them next to each other in the shelf or release suitable marketing campaigns. A typical association rule may be of the type: "If the customer is male, between 20-30 years and if his average phone call length is less than 1:30min then he'd most probably terminate his contract within the next fortnight." An important fact is that the rule doesn't contain any justification nor does it prove any causal relation. More investigations might be necessary to determine the reason of causal relations, in this case the sudden contract cancelations (i.e. competitor offerings, missing features, bad service, etc.). *Supervised Learning*, also referred to as *classification*, is probably the most prominent data mining technique. It aims to create a so called classifier that assigns new data items to previously defined classes. Incoming mails may be grouped in classes like "Business", "Family", "Confiden-

tial" and "Spam". Whenever a new mail arrives at the user's inbox the classifier studies its characteristics and assigns the mail to the most likely class. In order to do so, the classifier needs to learn the characteristics of each single class in advance (i.e. keywords, senders address, message length, time of arrival, attachments, etc.). This can be achieved with a representative set of training data mails that are already assigned to the correct class manually. *Unsupervised Learning* does not require the availability of a pre-classified training data set. This technique is also referred to as *clustering*, as it aims to group similar data items together in so called clusters. Data items within the same cluster share similar characteristics and provide a high degree of cohesion. In contrast, clusters are different to each other and are loosely coupled. With some text analysis algorithms in combination, the clustering technique is able to process given text documents (e.g. papers, web sites, tweets, etc.) and group them in clusters that share the same topic (e.g. radiology, sports, earthquakes, etc.). It is important to understand that clustering techniques are not designed for deriving a suitable cluster name. The resulting groups have to be interpreted by a domain expert who makes further decisions about the similarities found.

**Social media** potentially holds a lot of implicit information and is therefore a suitable subject to data mining analysis. Generally, Social Media comprises various digital media technologies to enable user interaction and the creation of multimedia content for sharing within a community or individuals. By interacting socially, one-to-many communication is turned into the communication type "many-to-many" which is more familiar to human nature (Shirky, 2009). Researchers benefit from extracting useful information from raw data retrieved from social media by discovering and exploring the information flow as a type of fieldwork experience. Structuring and classifying the unsystematic data is one of the key challenges in gaining relevant information for knowledge extraction.

The Haitian earthquake in 2010 was mentioned as the first use case of coordinating and engaging support for first responders via digital media, such as short message services and social media platforms. As summarized by (Fraustino, et al., 2012), social media played a key role in information dissemination in the Haitian earthquake 2010. Different types fulfilled various public needs. Twitter for example, was used to stay in contact with others (2.3 million tweets) and to coordinate disaster relief efforts by providing

special skills voluntarily (e.g. technology skills). As an example, the appearance of the U.S. volunteers' initiative led by Tufts University developed the platform Ushahidi-Haiti, a crisis map based on incident reports of residents and volunteers. Crowdsourcing allows a qualified crowd to participate in different tasks such as provision or validation of information, but also editing in case of request (Gao, et al., 2011). Hurricane Sandy (2012) stimulated the appearance of social media in the disaster context. While Twitter served as a source of information and misinformation at the same, the hurricane achieved the second place on Facebook's hot topic and latest storm-pictures were provided to the public via Instagram. It is known that each social media type has its own purpose; while blogs are often used for emotional release and support, Twitter is used as a source for breaking news. Sometimes, content sharing platforms like YouTube have a negative connotation due to the opportunity to view and share shocking disaster videos (Fraustino, et al., 2012).

**Processing social media content** for CDM applications generates interesting opportunities but at the same time induces some additional issues that have to be taken into account. One of the major non-functional challenges is to use data without violating any privacy or legal constraints. Another important aspect is to detect invalid or unreliable content providers (i.e. persons, platforms, channels, etc.). This paper describes how to address these issues in terms of system design and assesses the applicability of several Social Media platforms regarding SMM purposes.

## Thesis

An effective approach to circumvent the non-functional issues is to provide applications (i.e. social platforms, websites, mobile apps, etc.) dedicated to specific CDM use cases and accordingly inform users about its purpose as well as to clarify what is going to happen to their data. This approach is very close to the concept of crowd-sourcing. A lot of initiatives exist to foster the idea of utilizing user-generated content. The most prominent ones are Ushahidi[2] and Sahana[3]. These initiatives provide free and open-source software collections that facilitate geo-spatial information col-

[2] http://www.ushahidi.com , last accessed on 2013/08/12
[3] http://sahanafoundation.org, last accessed on 2013/08/12

lection and visualization in crisis situations. The crowd-sourcing approach heavily depends on a high number of participants which are encouraged to self-adjust invalid information. (Neubauer et al, 2013) extended the user-generated content idea by explicitly asking specific users or groups of users to contribute some relevant but yet missing input to reduce fuzziness and gain additional reliability which is especially important for the CDM domain. However, determining reliable verifiers in the crowd as well as the development of trust management systems is still an open research question (Gao, et al., 2011). Advanced analysis of both anonymized user data and their provided content is a promising first step to establish automatic and highly scalable trust systems (Havlik, et al., 2013). Similar approaches have been applied to detect influential social media creators during disasters. (Mills, et al., 2009) analysed twitter feeds dedicated to the San Diego wildfires in 2007 and identified three feeds as most influential (one local broad casting news station and two local residents). One data point of influence, in this case a tweet containing a link resource, induced 10.000 clicks conducted by followers. Therefore, identification of reliable and influential nodes in Social Media applications is also fundamental regarding public alerting during on-going crisis or disasters.

So basically there are two dimensions that have to be taken into account considering social media mining for crisis management (see Figure 2). The first dimension indicates whether the used material is structured or not. The second dimension describes whether individuals are identifiable or not. (Gundecha & Liu, 2012) argue that information provenance in social media is an important but yet unsolved research issue to differentiate rumours from truth.

So, in order to determine validity or reliability of certain users or data sources it is essential to be able to perform unique identification. We propose to use unique IDs or anonymized codes. Additionally, many social platforms (e.g. twitter) use nicknames for user identification which is absolutely sufficient for mining purposes. The important aspect is to be able to assign collected data to uniquely identifiable sources rather than knowing individual's personal information (i.e. name, date of birth, etc.). Implementing proper identification facilitates further assessment steps like verification conducted by users or data mining algorithms. Depending on the use case, even more dimensions may play an important role in mining social media

data for CDM (i.e. actuality, geo-spatial resolution, etc.).

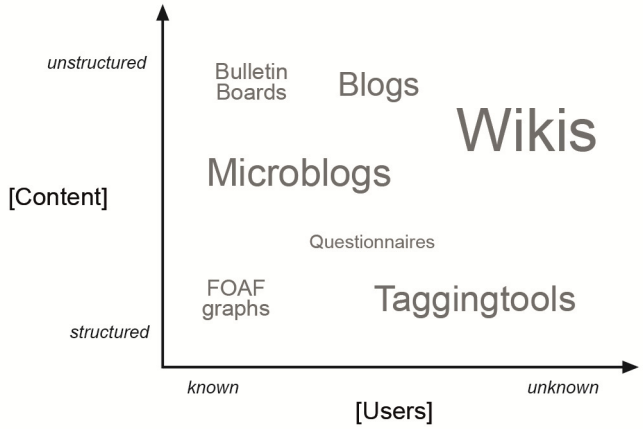



**Figure 2:** We determined two basic dimensions that one has to consider when planning a SMM application in the CDM domain. Certain applications may require identifying every participating user, others might not. Dealing with unstructured content may entail additional pre-processing steps.

The choice regarding the Social Media platform may not only depend on its provided content and the involved users is may also depend on the crisis situation. SMM may gain significant advantages in every single situation:

**Pre-crisis situations**: SMM may be used to detect crisis in their early stages even before public mass media starts reporting about it. Adding a specific focus on dedicated events like earthquakes, flooding, etc., may additionally improve reliability and accuracy. *Example*: use twitters public API and process tweets with by using the classification approach.

**In-crisis situations**: SMM may be used to analyse the current situation in terms of available resources or humanitarian needs. Social media content also comprises geo-related data which adds extra value for crisis coordination. *Example*: use Flickr API and search for photos, dedicated to a specific crisis event and apply clustering to their geo-position in order to reveal hot spots.

**Post-crisis situations**: Having collected a reasonable amount of data during on-going crisis, SMM may be used to analyse crisis activities in order to derive new models. These models help to better understand relations and

can be applied in training scenarios or support pre-crisis analysis to provide more accurate predictions. *Example*: analyse data for common vocabulary to create crisis related thesaurus.

Since different Social Media platforms provide different kind of content we investigated several platforms and assessed their applicability regarding the CDM domain. On the basis of our findings, we propose a best practice data mining process for Social Media in crisis and disasters.

**Application**

A typical characteristic of Social Media is that users generate their own content. Some of the most used Social Media services, like Facebook, Twitter, Linkedin, Youtube and Flickr have between 0,5 and 1 Billion user. Even if only a very small proportion of the users are engaged in content creation, like on Youtube, they create a very large amount of content, which is a challenge for the data mining processes. From a data mining point of view, these services have two important basic data structures.

1. Almost all social media services are developed as network forming communities. Often the personal identity or the profile (not necessarily an approved identity) is treated as network node. Network links are formed by personal relationships, common interest or other network forming information. This implies that social network analysis (SNA) can be used as one of the main data mining methods to identify hubs and authorities. According to SNA hubs are specific nodes with a lot of outbound links. Authorities are nodes with a lot of inbound links. In this classification the directed links are understood as a vote for trust. In mass communication it is always an important task to identify communities of trust and communication multiplier in this community. This can be used in CDM to improve the efficiency and reliability of communication processes.
2. Almost all social media sites let users produce content, either as text, short text, picture, video, profile or full HTML content. This content can be used to understand the thematic structure of ongoing communication processes and discover new trends and new discussion topics. In CDM this can be used for issue management,

public communication and request for crowd support.

Social media sites usually combine network data and content data, some of them with a stronger focus on network data (e.g. Facebook, Google +, LinkedIn) and other with a stronger focus on content data (e.g. Youtube, Twitter, Flickr and other). Table 1 shows the most popular social media sites, classified by network orientation or content orientation (bold is more important) and similarity of the data structure (separated by double lines).

| Service | User[4] | Data aquisition | Network Data | Content Data |
|---|---|---|---|---|
| Face-book | 1.5 bn | REST API, JSON and XML datasets about profiles, most of the data only visible in privat communities | **Network of friend-ship communities and relation ships** | Privat multimedia data, for friendship communities |
| Google + | 343 m | REST API, JSON and XML datasets about profiles, most of the data only visible in privat communities | **Network of friend-ship communities and relation ships** | Privat multimedia data, for friendship communities |
| Youtub e | 1 bn | HTTP, only meta data, and video streaming supported | Similarity of videos | **Videos and com-ments, only stream-ing** |
| Twitter | 500 m | REST API for full communica-tion as twitter client and stream-ing API for high volume re-quests. | Network of followers | **Microblog text, links, hash tags** |

4 http://expandedramblings.com/index.php/resource-how-many-people-use-the-top-social-media/, last accessed 2013/08/12

| | | | | |
|---|---|---|---|---|
| Tumblr | 216 m | HTTP requests and JSONP response | Network of followers | **Microblog text, links, hash tags** |
| Linkedin | 238 m | REST API with html response to all data available to authenticated user | **Network of professionals** | Information about interests, expertise, and reputation |
| Flickr | 87 m | REST API with JSON or XML response | Network data about contacts and groups | **Photos and comments** |
| Pinterest | 70 m | No API, SDK only for upload of content | Sharing community | **Virtual pinboard to share content from web** |
| Wordpress | 66 m | PHP Software for blogging, only partly centralised | Network by links to other homepages (not centralised) | **Webcontent, organised by posts** |

**Table 1:** Amount of available data sets, data acquisition, data structure and service specific content. Double lines group platforms with a similar data structure. (Source: AIT)

Data analysis for CDM should use both types of data structures and all sorts of different services to generate a more complete situational awareness. However, most of the data in social networks are restricted to limit access to friends. Therefore, a Social Media strategy in CDM should include a strategy to build up a supporter community.

As depicted in the table above, some Social Media services offer similar information. In Facebook and Google+, e.g. private multimedia data and links to multimedia data are available. However, access is usually restricted to friendship communities. For all members, only attributes like ID, Name, User Name, Country or Gender are available. With authentication additional technical data for developers, like browser type, unique IDs and session information can be retrieved. For more useful data, user permission is necessary. With this, a complete access to profile is possible. In case of a

crisis, in principle, pictures, videos, links, wall posts can support situational awareness. However, to get these data sets, it is necessary to convince the user to give their permission. Search is only allowed in public objects, which makes it very difficult to get discussions, with relevant information for a crisis.

LinkedIn is similar to Facebook and Google+, but put more emphasis on professional information about competences, interests and experience in a business context. The search function is more useful for CDM than at Facebook and Google+. It is possible to search for people, groups, companies and access company profiles. LinkedIn enables members to establish and grow their networks with invitations and messages by using the API. This makes it possible to develop a CDM application for a supporter community.

Microblogging services like Twitter and Tumblr, blogging services like Wordpress, discussion forums and multimedia repositories provide valuable datasets for content analysis. Due to the limited length of the microblogging messages the main information of the post is often behind encrypted links to multimedia content stored in picture or video repositories, as well as content from other homepages. However, the full analytical power is reached with a combination from SNA results, results from content analysis, applied in a network-centric issue management for mass communication in CDM.

**Social Media Monitoring Services** usually concentrate on frequency statistics or semantic analysis. This has been proven by an internal AIT market research in 2011 which investigated about 90 monitoring services. There was no service or software available for what we call it, network-centric issue management (with issue identification, issue prioritisation and stakeholder identification according to a specific issue.) The AIT market research, as well as the presentation of top tools in traditional social media monitoring makes clear, that these tools are based on business needs.[5] Specifically in CDM the whole word vector for topic classification is superior

[5] "50 Top Tools for Social Media Monitoring, Analytics, and Management", http://socialmediatoday.com/pamdyer/1458746/50-top-tools-social-media-monitoring-analytics-and-management-2013, last accessed 2013/08/12

to classical frequency analysis. However, this is only one aspect in appropriate text mining for CDM.

The left column of Table 2 lists features, which are state of art in topic mining within existing social media monitoring solutions. The right column lists features which do not exists yet but would be beneficial in crisis communication.

| State of the Art feature in Social Media | Beyond state of the Art features for CDM |
|---|---|
| Search for keywords | Search concepts |
| Filter (time, relevance, geography, resources) | Emerging topic detection with expectation |
| Relevance assessment | Emerging topic detection without expectation |
| Frequency analysis at item-level | Weak signal detection |
| Frequency analysis on subject level | Exception reporting using word vectors |
| Frequency analysis of trends | Issue management process control |
| Author profiles | Buzz tracking (tracking of discussion) |
| Author interactions in social media | Influencer networks |
| Tag cloud | Automated cluster detection |

**Table 2:** Beyond state of the art features for topic mining in CDM (Source: AIT)

With these new features, Social Media monitoring can address in particular the information overflow of crisis managers. For authorities it is very important to be informed about all the topics, discussed in social networks and to have a prioritization of these topics, so that they do not miss important information and that they are aware of escalation triggers. Therefore, the main focus on development is to concentrate on the most important information for the crisis manager and to provide this information in a clear and reliable manner.

**Emotion mining** is a quite new topic and somehow it is a kind of buzz word. It is very difficult to identify real emotions in written text. It is possible to identify emotions in sound files and from body signals. However even for humans it is not easy to identify emotions from email and SMS. Thus emoticons and abbreviations are used in social media to express emotions. This was one of the first methods for emotion mining in messages. Later, specific words were used in text mining, to identify emotion in messages. In the AIT market research, we found that existing social media monitoring companies often use dual sentiment classification. This means, that classifiers only differentiate between right or wrong, positive emotion or negative emotion.

Table 3 gives an overview, of what emotion mining is about in actual media monitoring software solutions and what emotion mining can be in CDM specific monitoring software.

| State of the Art features | Beyond state of the Art features for CDM |
|---|---|
| Tonality with key words, manual tagging | multi emotion classification |
| Association graph | identify emotions useful for CDM communication |
| Sentiment with SVM | emotional clusters |
| Search with Search Clouds | sentiment in each emotional cluster |
| Tonality with SVM | geo-referencing of emotional cluster |
| Sentiment with key words | tracking of sentiments over time |

**Table 3:** Beyond state of the art features of Social Media monitoring solutions facilitating emotion mining for CDM (Source: AIT)

**A best practice data mining process for CDM** will start with a process to identify relevant channels of communication, for a specific use case. It can be expected, that there are sources for network data and content data in the results. Second, social network analysis will produce a structure of the relevant community. Geo-referenced are very beneficially. However, most of the social networks have unreliable information regarding location in the entity profile. We expect that this will improve in the future. Third, based on the network of relevant users, content data acquisition can start

and should continue over the period of crisis. Topic mining and emotion mining is used to extract the relevant content. Finally, a network-centric issue management can be set up for effective mass communication in CDM. The network-centric issue management uses the same processes as classical issue management (see Figure 4), but relies on results from SNA to make communication more effective.


**Figure 3:** Network- centric issue management in CDM (Source: AIT)

The approach to combine both data mining and Social Media content generates a lot of very beneficial use cases for the CDM domain. Anyway, processing social media content requires a high amount of social responsibility as well as legal and respectful administration of user's privacy. SMM applications may exclusively utilize data that is explicitly available for the general public. This excludes data being available by accident (e.g. misconfiguration, opt-out trap, etc.). However, the CDM domain may gain a lot of interesting insights in various scenarios in order to understand people's needs and their behaviour and foster proper communication between all stakeholders.

## Use Case Scenario: Flooding

Flooding scenarios can usually be anticipated for a certain time period ahead by weather forecasts and repeated monitoring of river gauges, so that the forces (such as disaster relief units, fire fighters, or emergency response

organisations) can be put on alert on time. Unfortunately, disaster management is still always a race against time, including a set of developments, which – due to the nature of crisis, cannot be foreseen for all possible cases. Residents affected by disastrous events are likely to share their experiences and exchange their thoughts via Social Media platforms. Gaining data from this exchange of information certainly contributes to receive a better picture about the most up to date developments from the various, existing acute flooding scenario. On the other hand channels are established, enabling direct communication between the residents of the affected regions and the forces. This helps to better predict and react to the developments of flooding scenarios in place. Not only the typical attributes and characteristics of the relevant flooding scenarios can be explored, also the evolving patterns of the crisis and the disaster development can be recognized by the forces in an enhanced manner. We developed a model that distinguishes between three phases in flooding scenarios, each resulting in different tasks and challenges for the integrated crisis and disaster management and describes possible reactions of the operating emergency response organisations.

During the **pre-phase**, weak signals and first impacts of possible flooding events can be detected. Flood monitoring measures and local explorations are the basis for decisions of the operation staff which triggers warnings and flood alerts. Besides that, first instructions are suggested to coordinate the local residents. Social Media information helps to detect and analyse additional signals and developments earlier, and can be used to predict and identify possible flood incidents ahead. The **integrated operation control phase** starts with flood intervention by different emergency response and military organisations such as the Austrian Red Cross, fire fighters, or the Austrian Army and other emergency response or non-governmental organisations, being operative in different fields of intervention (i.e. Medical Care, Psychological Care, Supply & Logistics or Technical Infrastructure). A high level of coordination and therefore a sophisticated information management is necessary to establish a „shared awareness“ to be able to optimize and synchronize every action over all fields of intervention. After the flooding, after-action– and incident-reviews are held in a **post-phase**, while recovery measures are triggered by the results and gained experience out of the operation. SMM applications may be used to assist the Lessons Learned process which helps to optimize the detection and handling of

flooding events in the future and closes the feed-forward-loop to the next pre-phase.

## Discussion

The use of data from social media in the domain of crisis management offers on one hand multiple chances, but is also associated with many challenges on the other. Opportunities encompass the availability of real time data on crisis evolution to help crisis managers to sharpen their decisions, new or additional approaches to co-ordinate emergency forces in the field or psychological assistance of affected people (Rainer, et al., 2013). Challenges encompass legal aspects such as data protection, liability and privacy issues and in some cases copy right aspects. Moreover, ethical aspects like misuse of data by a despotic regime have to be taken into account, too. Finally, cultural aspects caused by the degree of availability of and the willingness to use the internet by specific populations need to be considered (Rainer, et al., 2013). Data provided from social media can be used in different ways by crisis managers. One approach is to use them in order to obtain information from social media in order to enrich the picture on the development of a crisis obtained from traditional sources of information. The other approach is to use social media to establish communication paths between the multiple actors in crisis, e.g. crisis managers, emergency forces, affected population, volunteers providing help or representatives of mass media. The communication processes can be uni- or bidirectional and can be open or can be controlled by the crisis manager. In any case there is need to extract relevant information out from the huge amount of data by applying methodologies such as those described in the introduction chapter. The process required to generate relevant knowledge from data obtained by social media is described by (Neubauer, et al., 2013) in more detail. A common requirement on all methodologies such as association rule mining is to identify relevant data in order to extract crisis relevant information, because the unstructured, not corrected data does not contain all demanded and necessarily correct information. Another relevant aspect is the credibility of the obtained data. Before the generation of knowledge to support crisis managers, the reliability of the extracted information has to be validated by approaches such as peer reviews or credibility checks. Major questions are liability and privacy aspects, that may vary from state to state being involved in on specific crisis. In case of wrong decision causing

damages or even human losses, the question arises who is liable. Nevertheless, if all those aspects are considered, social media offer brilliant perspectives for crisis management.

**References**


- Ackoff, R. L., 1989. From data to wisdom. Journal Of Applied Systems Analysis, Volume 16, pp. 3-9.
- Borne, K. D., 2009. Scientific Data Mining in Astronomy. Next Generation of Data Mining, pp. 91-114.
- Fraustino, J. D., Liu, B. & Jin, Y., 2012. Social Media Use during Disasters: A Review of the Knowledge Base and Gaps. Final Report to Human Factors/Behavioral Sciences Division, U.S. Department of Homeland Security
- G.K.Gupta, 2009. Data Mining with Case Studies. New Delhi: PHI Learning Private Limited
- Gao, H., Barbier, G. & Goolsby, R., 2011. Harnessing the Crowdsourcing Power of Social Media for Disaster Relief. Intelligent Systems, 26(3), pp. 10-14.
- Gundecha, P. & Liu, H., 2012. Mining Social Media: A Brief Introduction. TutORials in Operations Research, INFORMS, Volume 9, pp. 1-17.
- Havlik, D., Egly M., Huber H., Kutschera P., Falgenhauer M., Cizek M., 2013. Robust and trusted crowd-sourcing and crowdtasking in the Future Internet, in: Hřebíček, J., Schimak, G., M. Kubasek M., Rizzoli A. (eds.) Environmental Software Systems. Fostering Sharing Information. IFIP Advances in Information and Communication Technology, Springer, Heidelberg (2013)
- Koohang, A., Harman, K. & Britz, J., 2008. Knowledge Management: Theoretical Foundations. Santa Rosa, California: Informing Science Press
- Liu, B., 2007. Web Data Mining. Berlin Heidelberg New York: Springer
- Mills, A., Rui, C., JunKyu, L. & H., R., 2009. Web 2.0 Emergency Applications: How useful can Twitter be for Emergency Response. Journal of Information Privacy & Security, 5(3)
- Neubauer G., Nowak A., Jager B., Havlik D., Foitik G., Kloyber C.,

Flachberger C., 2013. Crowdtasking for crisis and disaster management - opportunities and challanges, Interdisciplinary Information and Management Talks
- Rainer, K. Grubmüller V., Pejic I., Götsch K., Leitner P., 2013. Social Media Applications in Crisis Interaction. systems. connecting matter, life, culture and technology 1(1), pp. 110-127.
- Shirky, C., 2009. Here Comes Everybody: The Power of Organizing Without Organizations. s.l.:Penguin Books.

**Authors**

**Hermann Huber** studied Information & Knowledge Management at the University of Technology in Vienna. He was employed as assistant for business intelligence and did research on data mining in the cultural heritage domain. Today, he is employee of AIT and is involved in several research projects related to CDM.

**Georg Neubauer** is thematic coordinator for "ICT solutions for crisis and disaster management" at AIT. He was lecturer at the University of Technology in Graz from 2002-2010. Since 2004 he gives lectures at the University of Technology in Vienna. Mr. Neubauer worked as a consultant for several international organisations like the EU, WTO or BMVIT.

**Andrea Nowak** joined AIT in 1992 and is Head of Business Unit "Informationmanagement & eHealth". She studied Mathematics at the University of Vienna and was employee of Siemens for several years. Mrs. Nowak successfully managed R&D projects in cooperation with the Austrian Army and is member of diverse international research boards.

**Joachim Klerx** is predominantly active in the research field of innovation systems with a strong focus on innovative groups in society since 14 years. He is an expert in the research fields of data mining, artificial intelligence and multi-agent systems and was part of numerous research projects in the European Union.

**Bettina Jager** studies political science at the University of Vienna and is part of the Crisis and Disaster Management Team at AIT since 2010. Mrs.

Jager focuses on politics and administration, good governance, technological impact assessment related to CDM.

**Klaus Mak** is Head of Central Documentation at the National Defence Agency of the Austrian Armed Forces. He is lector on several educational institutes for information and knowledge management. Mr. Mak is responsible for conceptual planning and R&D projects with strong focus on knowledge management at the Austrian Armed Forces.

**Christian Meurers** studied Informatics at the University of Technology in Vienna and is responsible for the Situation Awareness Center at the National Defence Agency. His main research areas are cyber & information war and technology & society.

## 6th International Conference on Advances in Information Technology

*The Social and Mobile Computing*
Bangkok, Thailand, December 12-13, 2013

The intention to organize IAIT is to establish the place where researchers and industrial practitioners can share their work and achievement in information technology, both theoretical and application. We make IAIT to serve as venue to foster collaboration among industrialists and academia from different parts of the world. A lot has been achieved since the launch of the first IAIT in 2005; however, many challenges remain to be found in the years to come.

In addition to the appropriate program offered by IAIT, the conference provides an excellent environment to meet your peers in IT profession, build relationships, and exchange lessons learned. During the conference, we believe participants will present and discuss the latest topics in Information Technology, ranging from technical knowledge and experiment to future strategic directions.

http://www.iait-conf.org/IAIT2013/

The following peer-reviewed paper was published in the conference proceedings:
Papasratorn, Borworn, Charoenkitkarn, Nipon, Vanijja, Vajirasak, Chongsuphajaisiddhi, Vithida (Eds.), Advances in Information Technology, Communications in Computer and Information Science, 2013, Springer International Publishing, ISBN 978-3-319-03782-0, p.13-22

# Cross-Media Analysis for Communication during Natural Disasters

*Gerhard Backfried, Johannes Göllner, Gerald Quirchmayr, Karin Rainer, Gert Kienast, Georg Thallinger, Christian Schmidt, Mark Pfeiffer, Christian Meurers, Andreas Peer*

**Abstract:** In this paper we describe the role of media in the context of natural disasters. Traditional media have a long history in covering disasters and will continue to be a major provider of information in the future. In recent years, however there has been a significant change: information about natural disasters has increasingly been disseminated on a large scale on social media platforms. These media are typically faster but may be less reliable. They provide additional and complementary angles on events and, combined with traditional media, provide a wider spectrum of coverage. We argue that cross-media information combined with multi-lingual data provides huge opportunities for first-responders and decision makers to gain improved situational awareness allowing for improved disaster relief, support, mitigation and resilience measures.

**Keywords:** disaster communication, multimedia processing, social media, situational awareness

## 1 Introduction

Traditional media have a long history in covering disasters and crises. They are a major provider of information in times of disasters and will without a doubt remain so in the future. As recent natural (and man-made) disasters have shown, social media have become a new vehicle to provide additional useful insights into events as they unfold. They combine with traditional media in various ways sparking off initial coverage, amplifying information or providing different and unfiltered angles. Together they produce a wide spectrum of coverage of an event and lead to significantly improved situa-

tional awareness for decision makers and planners[1,2]. The boundaries between social media and traditional media have become increasingly blurred as news providers use social media as alternative and additive channels. For example, 8 out of the 10 most active Twitter users reporting on an earthquake in Chile in 2010[3] were found to be directly related to mass-media. Likewise, TV stations receive input about storm damage which is then broadcast immediately on TV[4]. In other cases, such as the Queensland floods[5] social media even became a main source for mainstream media. As helpful as all this combined information may potentially be to disaster relief organizations, it usually comes in multiple formats, multiple languages, immense amounts, across multiple media, is generally unstructured and inhomogeneous and also attributed with different levels of reliability and trust. Whereas in this paper we focus on incoming information, clearly many aspects regarding the integration of social media and traditional media equally apply to outgoing information, communication between first-responders and the affected population as well as among themselves.

## 2 Media in Disaster Communication

For large portions of the population traditional media, such as TV, radio and web-sources remain a major source of information even today. Depending on the infrastructure and social factors, they may still even form the primary source of information. Under certain conditions, official and traditional channels may not be readily accessible or only be able (or willing) to provide partial information. Nevertheless, these media form an integral part of the spectrum of sources used to obtain situational awareness in

---

1 Kwang-Hoong, L. / Mei-Li, L. The Fukushima Nuclear Crisis Reemphasized the Need for Improved Risk Communication and Better Use of Social Media. Health Physics 103 (3): 307-310

2 Tyshchuk, Y. et al. Social Media & Warning Response Impacts in Extreme Events: Results from a Naturally Occuring Experiment. 2012 45th International Conference on System Science (HICSS): 818

3 Mendoza, M., Poblete, B., and Castillo, C., Twitter Under Crisis: Can we trust what we RT?, SOMA 2010, Washington D.C., USA

4 Holmes, W., Crisis Communication and Social Media: Advantages, Disadvantages and Best Practices, Univ. of Tennessee, CCISymposium, 2011, Knowville, USA

5 Bruns, A., Burgess, J., Crawford, K. and Shaw, F., #qldfloods and @QPSMedia: Crisis Communication on Twitter in the 2011 South East Queensland Floods, 2012, Brisbane: ARC Centre of Excellence for Creative Industries and Innovation

times of crises and disaster and will continue to do so in the future.

With the advent of social media, the way people communicate, search for and receive information has undergone a radical transformation. Not only have social media changed the way people communicate in their day-to-day lives, but also - and increasingly so - during emergencies and crises. Effectively it can already be assumed, that in many cases a part of the population will indeed turn to social media during crises[6] .[7] Particularly micro-blogging systems like Twitter play an increasingly important role in this respect and form a new way to disseminate and receive information[5,8]. Social media lend themselves to two-way communication, allowing data to be gathered as well as distributed. This type of communication is valuable to first responders because it allows them to not only receive information, observations, opinions and emotions from individuals who experience the incident or crisis first hand, but also allows them to send out important disaster-related information, critical updates, clarifications or corrections to each other and to the persons who need it most. Activities of affected persons are not limited to mere communication and observation but also involve active participation at the disaster site to perform specific tasks relevant for immediate support, relief activities, preventive on-site tasks or additional fact-finding. In terms of situational awareness, data from social media have to be combined, reconciled and contrasted with information from traditional sources to arrive at a more complete picture of an event.

For decades, communities have been relying on specific groups to assist in times of disaster. But the present day communications environment with its new and increased expectations has changed the game, not just for first responders, but also for the general public[9]. (Near) Real-time communication/information, personal involvement, reliable, critically-challenged and -

---

[6] Johansson, F., Brynielsson, J., Narganes Quijano, M., Estimating Citizen Alertness in Crises using Social Media Monitoring and Analysis, EISIC 2012, Odense, Denmark

[7] It should be noted, though, that in a broad spectrum of societies, large social groups are still far from being able to participate in this form of communication due to limited economic/technical access, education or gender.

[8] Nilsson, J. et al, Making use of New Media for Pan-European Crisis Communication, ISCRAM 2012, Vancouver, Canada

[9] American Red Cross, The Case for Integrating Crisis Response with Social Media, White Paper, 2010

questioned sources, as well as multi-media content are common requirements and assets of currently shared information. The technology is constantly evolving which results in people having even higher expectations of first responders but also vice-versa. Affected persons may indeed expect authorities to respond quickly to information provided via social media[4]. There remains no doubt that the impact of social media on crisis communication is already significant and will only continue to grow in significance in the years to come.

Even though social media may sometimes not be regarded as the actual drivers of news[10], they can certainly be viewed as amplifiers and often play a time-critical role in the development and communication of events. In certain settings, they may actually be the first medium on which an event is reported about and form the spark for coverage on other, more traditional media channels. On other occasions, professional journalists may still be the first ones to report. In a study comparing trending hash-tags on Twitter and headlines on CNN it was found that in approximately 50% of the cases CNN was ahead of Twitter[11]. Regarding professional sources, a large portion of the activity on social media may simply be re-emitting content which is available via other channels (such as feeds from the same source). Both, professionals as well as numerous individuals (citizens) may provide further insight on and add different angles to events already covered by traditional media. Including them and following the information provided by links within them allows for increased coverage and better and extended contrast across sources and media. Social media may add valuable dimensions like detailed micro-perspectives and (near) real time images of dynamically changing situations to a complex, already multi-lingual, multi-source, multi-media environment. In addition, they might provide unfiltered information, in contrast to official or commercial sources, whose coverage may be biased in different ways. Social media, particularly the links mentioned in them, can be regarded as a gateway and amplifier to yet more relevant news-sites covering similar or identical topics. An increased amount of links may point to certain types and stages of events and serves

[10] Lee Hughes, A., Palen, L., Twitter Adoption and Use in Mass Convergence and Emergency Events, ISCRAM 2009, Gothenburg, Sweden

[11] Kwak, H, Lee, C., Park H., Moon S, What is Twitter, a Social Network or a News Media, WWW 2010, Raleigh, USA

as an indicator of the amount of external information included in communication[12]. Particularly in this context, social media may act as information brokers and broadcasters[4,10]. Regarding the quality, veracity and trustworthiness of the retrieved data, the frequency by itself is usually no reliable indicator. However, re-tweeting behavior can serve as an indicator of whether or not a tweet's content can be trusted[13] . Linking tweets to traditional media can likewise be envisioned to serve this purpose.

## 3 Existing Work, Case-Studies and Technology

The first decade of the 2000s witnessed the birth of a number of social media platforms. These have been adopted on a wide scale and are being used by increasingly large portions of the population for personal and professional purposes. They have changed the digital landscape immensely and in a lasting way and produced new online social- and communication behaviors. Clearly, there are regional and cultural differences in the popularity and accessibility of individual platforms and the way users embrace them. However, some large networks - above all Facebook - have managed to dominate increasingly large regions of the globe and continue to extend their reach, establishing the de facto standard across many countries.

Social media platforms may roughly be classified into the following categories:

- Social Networks (e.g. Facebook, LinkedIn, Google+, Odnoklassniki,…)
- Micro-Blogging (e.g. Twitter, Weibo,…)
- Photo-Sharing (e.g Flickr, Instagram,…)
- Video-Sharing (e.g. YouTube)
- Bookmarking (e.g. Delicious, StumbleUpon,..)
- Social News (e.g. Digg, Reddit,…)
- Discussion Forums
- Incident-related platforms (e.g. Ushahidi, Crisis-Tracker,…)

---

[12] Bruns, A., Stieglitz, S., Towards More Systematic Twitter Analysis: Metrics for Tweeting Activities, Journal of Social Research Methodology, 2013

[13] Starbird, K., Palen, L., Pass It On?: Retweeting in Mass Emergency, ISCRAM 2010, Seattle, USA

These platforms target different user-groups, environments and objectives and offer different sets of features and functionalities. Many of them involve the process of sharing textual and/or multi-media data and the possibility to establish links and communication threads between them and/or the involved persons and entities. Some of them, like Ushahidi involve crowd-sourcing or activist-mapping. The nature of these platforms ranges from purely commercial ventures to open-source projects.
Since their respective time of introduction, social media have also been used to collect and disseminate information about natural disasters. Not all platforms and services lend themselves to a natural and direct use within disaster communication. Platforms like Twitter or Facebook, allowing to disseminate snippets of information in realtime to a selected or general public and allowing users to comment and enrich information have found wide adoption during crises and disasters. Photo-sharing services, being fed by an increasing amount of mobile devices have been used as targets for linking of information across media. Web sites and RSS-feeds are used for similar purposes in addition to providing a separate source in their own right. Linking between the different media, e.g. including links to video in tweets or mentioning Facebook accounts on TV has become a common way of communicating and referencing information.

Since 2004, several disasters have been investigated in the context of social media and crises. Figure 1 depicts some of the platforms and their respective years of launch along with a set of natural disasters which have been investigated using social media as information sources.

Examples of investigated disasters are the South East Queensland floods of 2011 where social media played a central role in crisis communication. During this disaster, the Queensland Police Service used Twitter (@QPSMedia) to communicate with affected people[5]. Social media have likewise played important roles during and following the earthquakes in New Zealand[14] , Haiti[15], Chile[3], and the US[13], grassfires[13] , hurricanes Katri-

[14] Bruns, A., Burgess, J., Local and Global Responses to Disaster: #eqnz and the Christchurch Earthquake, 2012 Disaster and Emergency Management Conference, Brisbane, Australia

[15] Dugdale, J., Van de Walle, B., Koeppinghoff, C., Social Media and SMS in the Haiti Earthquake, SWDM 2012 Workshop, Lyon, France

na[16] Ike, Gustav[10] and Sandy[16],[17], typhoons in the Philippines and floods in Brazil[18]. Their role in the floods in central Europe in May and June 2013 is being investigated in the QuOIMA project[19].

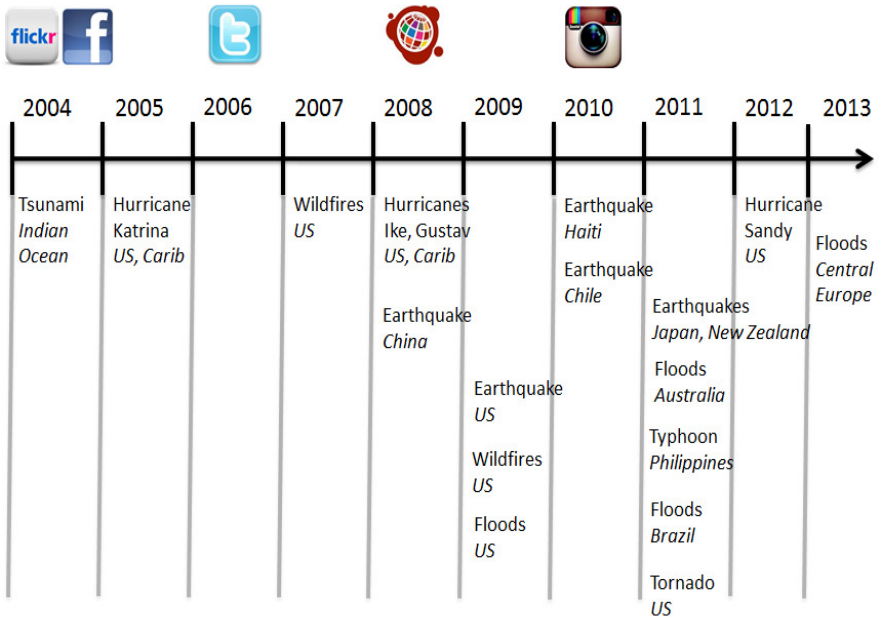



**Fig. 1.** Social media platforms and research on their use in natural disasters

Other disasters during the same period of time, such as the winter storm in the US in 2010 known as *Snowmageddon*, the wildfires in Russia in the same year, several floods, landslides, earthquakes or droughts in Africa, South-East Asia or Central America were almost certainly also covered by social

[16] Faustino, J.D., Liu, B., Jin, Y., Social Media During Disasters: A Review of the Knowledge Base and Gaps, Final Report to Human Factors/Behavioral Sciences Division, U.S. Department of Homeland Security, College Park, USA, 2012

[17] DHS Report, Lessons Learned: Social Media and Hurricane Sandy, available at https://communities.firstresponder.gov/DHS_VSMWG_Lessons_Learned_Social_Media_and_Hurricane_Sandy_Formatted_June_2013_FINAL.pdf, 08/30.2013

[18] Nagar, S., Aaditeshwar, S., Joshi, A., Characterization of Social Media Response to Natural Disasters, SWDM 2012 Workshop, Lyon, France

[19] Backfried, G., Göllner, J.,Quirchmayr, G. et al. Integration of Media Sources for Situation Analysis in the Different Phases of Disaster Management, EISIC 2013, Uppsala, Sweden

media platforms. However, no research on their particular role and the extent to which they were used in these events seems to have been carried out thus far.

Reference [8] provides an overview of social media in the context of crisis information. They find that media – traditional as well as social – form an important source for sending out and retrieving information about different aspects of a crisis or disaster. In particular they examine various approaches and channels which can be used for dissemination of crisis-relevant information. [3], [10] and [11] elaborate on the structure and types of communication which emerge on Twitter, [4] does so particularly for the crisis-case. [16] provides an overview of social media in the disaster context using a set of case spotlights covering specific events. [5] provides an in-depth and comprehensive overview of how social media played a role during the 2011 Queensland floods. [20] focuses on the connection between Twitter and TV from the point of view of how to combine social network interaction with programming. [11] provides a brief overview of existing and potential future uses of social media in disasters. Relatively little attention seems to have been paid to the actual use of language in the context of social media and natural disasters: [3] and [16] deal with this topic to some extent.

Numerous research projects aim at improving the effectiveness of communication and alerting during crises. For example, in the EU FP7 Alert4All [20], the screening of new media (SNM) tool [8] serves to enhance situational awareness using opinions and emotions found in on-line web content and social media. MASSCRISCOM[21] takes social media into account as an emerging means of mass communication during crisis situations. At QCRI in Qatar, the AIDR project[22] aims at developing semi-automated mechanisms, combined with crowd-sourcing, to form the foundations of a Twitter-based dashboard for analytical purposes during crises. In the Austrian Security Research Program KIRAS, the project QuOIMA[19]) aims at combining cross-media, multi-lingual analysis with visual analytics methods.

---

[20] Harrington, S., Highfield, T. Bruns, A., More Than a Backchannel: Twitter and Television, 2012 COST Action ISO906 Transforming Audiences, Transforming Societies

[21] MASSCRISCOM, http://www.masscriscom.eu on 08/30/2013

[22] AIDR, http://www.qcri.qa on 8/30/2013

It is notable that most research in connecting social media with natural disasters seems to have been carried out in - or at least been focusing on - a single language (English), a single medium (text) and a single source (Twitter) only. In addition, roughly half of the investigated disasters concerned the US.

This may be attributed to a number of factors:

- the affected population may have used Twitter for communication
- internationally visible target organizations of such systems operate primarily in English speaking countries
- researchers are limited in the languages they focus on, sometimes ruling out portions of a collected data set
- research programs may prefer to fund particular setups
- natural language processing (NLP) tools may exist only for a limited set of languages, in particular for English
- automatic speech recognition may not be available for particular domains (and wider range of languages)
- visual processing technology may not be available for a particular domain
- data sets may have been collected by entities in the English speaking world
- data sets are available for a single medium only (no parallel corpora across different media)
- data may simply be accessible more easily for certain platforms than for others, particularly for Twitter (privacy and legal concerns naturally play a strong role)

## 4 Media Requirements of First Responders

Since social media were not created from the start with first responders in mind, but rather for the general public to simply connect and share their thoughts and emotions with friends and family, certain limitations exist for first responders in the context of disaster communication. New ways to systematically incorporate and integrate social media and the related technology into disaster communication and combine them with traditional

media form current areas of research and development. Technologies, which are not purely based on textual input, such as speech recognition or visual processing form natural extensions of current systems, augmenting, extending and complementing existing sources which currently remain largely untapped. Clustering methods for data across media – e.g. multiple video clips of almost identical content - are required for navigating large amounts of data and presenting them in an efficient and manageable way. The speed and granularity of reporting across the different kinds of media need to be balanced against the requirement of obtaining reliable information. A combination of social media (fast but not less reliable), traditional media (slow but more reliable) and background material provided by official and governmental organizations (slow but more reliable) has to be balanced and structured flexibly to allow for different setups and foci during the different stages of a disaster. Information provided in several languages may have to be consolidated along the way, especially in international and cross-border settings of crises.

Fusing these diverse, mixed and complementary sources of information and allowing decision makers – and the public - to make sense of a large and inhomogeneous body of data is of utmost importance to first responders and their coordinating organizations. Access to data from different modalities just minutes after they have been published should allow users to perform various types of visualization and analysis activities by connecting and inter-linking information from different sources and media. The early detection of structures and patterns of communication as well as of perceived incidents are required to allow authorities to react earlier, swifter and more adequately in situations of crisis or disaster. It enables them to position vital assets adequately in order to minimize impact, speed up recovery and rebuilding efforts and even anticipate critical events before escalation.

Figure 2 depicts a generic 5-phases model developed at the National Defence Academy of the Austrian MoD[23]. First responders can benefit in all phases by the combined processing of data across media and languages and their underlying patterns of communication in a unified, fused manner.

[23] KIRAS-Antrag: Modellbildungs- und simulationsgestützte Entscheidungsunterstützung in der Last-Mile-Katastrophenbewältigung (LMK-MUSE), 28.02.2013, S. 18

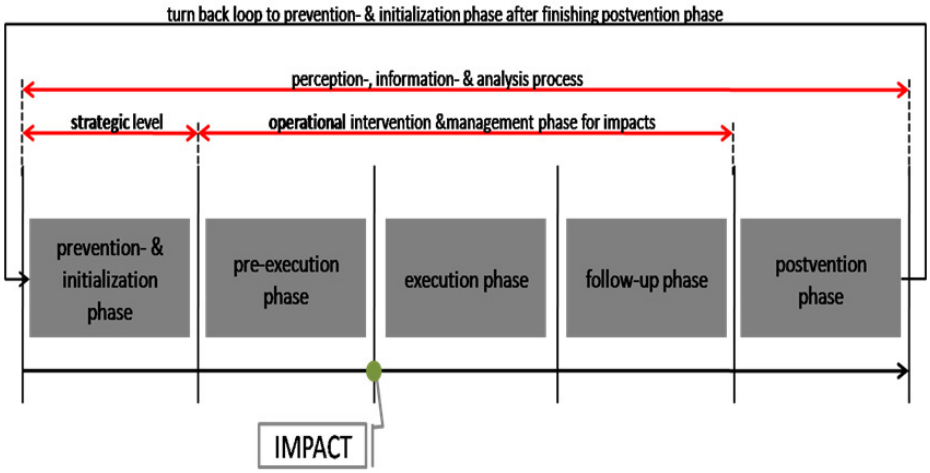



**Fig. 2**. 5-phases disaster model

According to the above model first responders face different challenges and requirements in crisis and disaster communication depending on the management / leadership level (strategic, operational etc.) as well as the phases themselves. On the strategic level first responders should have the ability to use the results of media fusion for analytical tasks to identify communication patterns and to link them to particular disaster phases. Emerging risks could be identified more quickly and reliably and the behavior of the affected population interpreted, monitored and influenced more effectively. On the operational level first responders require a large amount of information to understand the local requirements and tasks and to gain insights about emerging risks and possible threats to the population. The combination of media sources could help to improve shared situational awareness beyond organizational limitations which may exist between the different first responder organizations.

Additionally first responders require complex (semi-) automated analysis and visualization tools and techniques to complement and support their decision making processes. The technologies involved have to be multilingual and have to provide cross- and multi-media analysis facilities to ensure access to a large variety of diverse media and information sources. Accessibility and persistence of information has to be guaranteed for later justification of actions or decisions taken or not taken. Visual analysis is required to tap into the growing number of photographic and video-

content collected and uploaded to social media sites. These documents do not exist in a vacuum but rather form a complex network with textual and audio-data available across different media. The combinations of these modalities can serve as the base for a holistic approach of disaster communication and management. A combined system may also serve as a platform for first responders to share awareness, coordinate the operation, capitalize on synergy effects and synchronize their forces in a theater of operation. It cannot be stressed enough, that all methods and technologies should not be designed to replace people but to help decision makers to handle the increasing flood of information and fulfill their tasks in a more efficient way. Technological advances have to be accompanied by the establishment of best practices that enhance the goals of communication in crisis and disaster situations[4].

## 5 Expected Benefits and Approach

As stated in [24], monitoring information flows – spanning multiple media and languages – will establish and increase situational awareness for decision makers and planners. Obtaining real-time information, as a complex event unfolds, can help officials determine where people are; arrange mitigation measures, assess concerned persons' needs, and alert citizens and first responders to changing conditions and new threats and allow them to target their relief-measures more precisely and timely.

Analysis of communication content and -patterns might lead to the identification of structures indicating a specific situation or crisis-phase, such as the follow-up phase already having started. This in turn could result in improved and more targeted communication towards to affected population. Few or no models seem to exist thus far, capturing such communication patterns and deducing operation relevant parameters. Figure 3 depicts a schematic overview of which different types and sources of information and their interrelationship could be identified and combined into a unified analysis model for disaster communication.

[24] Lindsay, B., Social Media and Disasters: Current Uses, Future Options, and Policy Considerations, Congressional Research Service, 2011

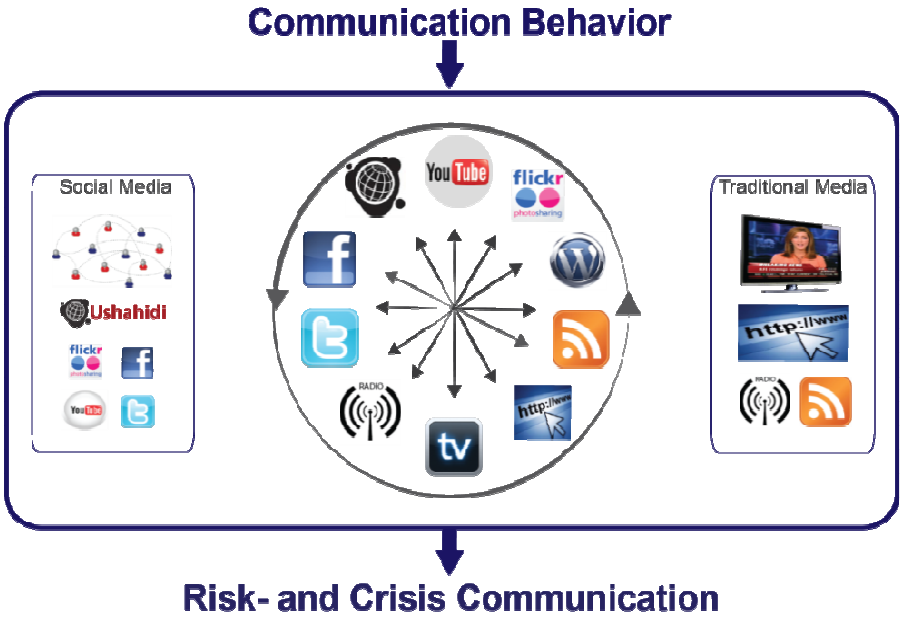



**Fig. 3.** Cross-media communication model

References from one medium linking to information in other media could be collected, followed and put into perspective for analysis. This is envisioned to take place in a unified framework, thus allowing to capitalize on the combination- and fusion capabilities of the system. Textual, audio as well as visual information and cues could be combined to arrive at a more complete picture. Multi-lingual information might add different angles and aspects not visible within a single medium or source. Media clips recorded around a number of key locations during a disasters are typically uploaded multiple times to different platforms leading to (near-) duplicate information. Being able to detect and interconnect such items, link them to other media and group them more adequately for navigation might reduce the workload of first responders significantly. Verification and completion of information or the detection of inconsistencies and rumors might be possible by combining the different sources and media. However, in all of these processes human intervention is expected to occur and eventually also be required to some extent. This is in line with an architecture aiming to support rather than to replace human operators. From a practical point of view, it is a strategic advantage for decision makers sending in first responders to know how a situation is developing. This forms an essential

input for team configuration and mission preparation.

The authors are actively engaged and cooperating with first responders in creating such a unified model fulfilling the above identified requirements to the largest extent possible. These requirements as well as the models and technologies involved are being refined as new disasters strike and insights are gained. With the help and support of first-responders, assumptions are verified against real-life environments and checked with regard to their real-world applicability and integration into best practices.

**References**


- Kwang-Hoong, L. / Mei-Li, L. The Fukushima Nuclear Crisis Reemphasized the Need for Improved Risk Communication and Better Use of Social Media. *Health Physics* 103 (3): 307-310.
- Tyshchuk, Y. et al. Social Media & Warning Response Impacts in Extreme Events: Results from a Naturally Occuring Experiment. 2012 45th International Conference on System Science (HICSS): 818
- Mendoza, M., Poblete, B., and Castillo, C., Twitter Under Crisis: Can we trust what we RT?, SOMA 2010, Washington D.C., USA
- Holmes, W., Crisis Communication and Social Media: Advantages, Disadvantages and Best Practices, Univ. of Tennessee, CCISymposium, 2011, Knowville, USA
- Bruns, A., Burgess, J., Crawford, K. and Shaw, F., #qldfloods and @QPSMedia: Crisis Communication on Twitter in the 2011 South East Queensland Floods, 2012, Brisbane: ARC Centre of Excellence for Creative Industries and Innovation
- Johansson, F., Brynielsson, J., Narganes Quijano, M., Estimating Citizen Alertness in Crises using Social Media Monitoring and Analysis, EISIC 2012, Odense, Denmark
- Nilsson, J. et al, Making use of New Media for Pan-European Crisis Communication, ISCRAM 2012, Vancouver, Canada
- Harrington, S., Highfield, T. Bruns, A., More Than a Backchannel: Twitter and Television, 2012 COST Action ISO906 Transforming Audiences, Transforming Societies
- American Red Cross, The Case for Integrating Crisis Response with

Social Media, White Paper, 2010
- Lee Hughes, A., Palen, L., Twitter Adoption and Use in Mass Convergence and Emergency Events, ISCRAM 2009, Gothenburg, Sweden
- Kwak, H, Lee, C., Park H., Moon S, What is Twitter, a Social Network or a News Media, WWW 2010, Raleigh, USA
- Bruns, A., Stieglitz, S., Towards More Systematic Twitter Analysis: Metrics for Tweeting Activities, Journal of Social Research Methodology, 2013
- Starbird, K., Palen, L., Pass It On?: Retweeting in Mass Emergency, ISCRAM 2010, Seattle, USA
- Bruns, A., Burgess, J., Local and Global Responses to Disaster: #eqnz and the Christchurch Earthquake, 2012 Disaster and Emergency Management Conference, Brisbane, Australia
- Dugdale, J., Van de Walle, B., Koeppinghoff, C., Social Media and SMS in the Haiti Earthquake, SWDM 2012 Workshop, Lyon, France
- Earle, P., et al. OMG Earthquake! Can Twitter Improve Earthquake Response?, Electronic Seismologist 2010
- Nagar, S., Aaditeshwar, S., Joshi, A., Characterization of Social Media Response to Natural Disasters, SWDM 2012 Workshop, Lyon, France
- Backfried, G., Göllner, J.,Quirchmayr, G. et al. Integration of Media Sources for Situation Analysis in the Different Phases of Disaster Management, EISIC 2013, Uppsala, Sweden
- Faustino, J.D., Liu, B., Jin, Y., Social Media During Disasters: A Review of the Knowledge Base and Gaps, Final Report to Human Factors/Behavioral Sciences Division, U.S. Department of Homeland Security, College Park, USA, 2012
- Alert4all, http://www.alert4all.eu on 08/30/2013
- MASSCRISCOM, http://www.masscriscom.eu on 08/30/2013
- AIDR, http://www.qcri.qa on 8/30/2013
- KIRAS-Antrag: Modellbildungs- und simulationsgestützte Entscheidungsunterstützung in der Last-Mile-Katastrophenbewältigung (LMK-MUSE), 28.02.2013, S. 18.
- Lindsay, B., Social Media and Disasters: Current Uses, Future Options, and Policy Considerations, Congressional Research Service,

2011
- DHS Report, Lessons Learned: Social Media and Hurricane Sandy, available at https://communities.firstresponder.gov/DHS_VSMWG_Lessons_Learned_Social_Media_and_Hurricane_Sandy_Formatted_June_2013_FINAL.pdf, 08/30.2013

**Authors**

**Gerhard Backfried, Christian Schmidt, Mark Pfeiffer**
SAIL LABS Technology AG, Vienna, Austria

**Johannes Göllner, Christian Meurers, Andreas Peer**
National Defence Academy, Dept. of Central Documentation, Austrian MoD, Vienna, Austria

**Gerald Quirchmayr**
University of Vienna, Multimedia Information Systems Research Group, Vienna, Austria

**Karin Rainer**
INSET Research&Advisory, Vienna, Austria

**Gert Kienast, Georg Thallinger**
Joanneum Research, Inst. for Information and Communication Technologies, Graz, Austria

## 11th International Conference on Information Systems for Crisis Response and Management

College of Information Sciences and Technology, The Pennsylvania State University, University Park, May 18-21, 2014

The theme for ISCRAM2014 is empowering citizens and communities through information systems for crisis response and management. Through this theme we focus on the local community, the individual and the technologies that can be employed to improve crisis response at the very local level. ISCRAM2014 will reframe first responders as everyday people who provide first aid, transport victims to hospitals in their own cars, and begin search and rescue rather than only the trained emergency response professionals. ISCRAM will reframe information systems for emergency response as socially-distributed information systems, in which information is disseminated within and between official and public channels and entities. ISCRAM2014 will advocate innovative ICT, to leverage the power of the collective intelligence of the citizenry to support natural instincts, which are to search for reliable information using any means possible to optimize for local conditions.

http://iscram2014.ist.psu.edu/

# Cross-media, Multimedia, Multilingual Communication in Open Sources During Crises and Disasters

*Gerhard Backfried, Katja Prinz, Gerald Quirchmayr, Johannes Göllner, Gerald Czech*

**Abstract:** Traditional and social media are known to be of great benefit for crisis- and disaster communication. In the vast majority of cases, however, these media have been collected, processed and analyzed separately. Previous research focused mostly on aspects of communication within a single medium and a single channel only (typically Twitter). Little work has been carried out on the investigation of cross-media communication and communication-patterns during such events. Consequently, individual corpora have been gathered for a single medium (typically a collection of tweets) and for a single language only (typically English). Subsequent processing is likewise often limited to the same single language. To arrive at a more complete picture of events, we argue that the different types of media should be combined and that the resulting cross-media as well as multimedia and multilingual approach will yield superior information and insights compared to approaches based on individual media only. We identify several key issues which merit further attention and investigation. Our interest lies primarily in the communication and -patterns arising before, during and following a disaster involving the full spectrum of media and diversity of languages and how to best link these to allow for effective and efficient crisis-communication and improved situational awareness to first responders.

The following criteria form key elements of our combined media approach:

Cross-media: both, traditional media as well as social media will continue to play fundamental and complementary roles. Their respective strengths can be capitalized on by combining sources and channels from different media, creating added value and allowing for insights not obtainable by any individual medium alone. Links between different media and their patterns during different disaster stages are expected to yield additional valuable, insights.

Multimedia: multimedia in the form of images and video is becoming more common-place with the ubiquity of portable devices. Individuals carrying such devices will often be on-site, delivering visual content and meta-data associated with short comments swiftly rather than typing lengthy texts. As a consequence, multimedia data and sites storing and accumulating them are becoming more interesting to harvest and process for analysis, interpretation and linking of content. These kinds of media require processing capabilities such as visual processing or speech recognition reaching beyond the purely textual ones often present in today's systems.

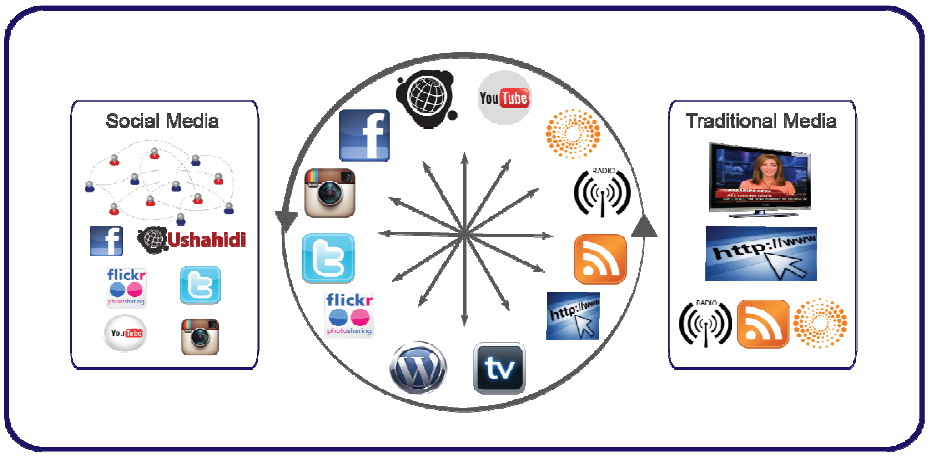
Multilingual: crises and disasters often take place in multinational, cross-border, multilingual and multicultural settings. As a consequence, media in different languages need to be collected and processed. Social media and meta-data created by the crowd can be multilingual and include jargon from different domains, linguistic styles and registers. These factors add additional requirements to the technologies and models involved, such as robustness to deviations from (perceived) standards. Outbound communication likewise has to take this diversity of languages and styles into consideration.

Multi-environment: the vocabulary and language-style (or register) used during crisis- and disaster-communication is likely to differ substantially across the different types of media. Specific, technical terminology and every-day language may overlap or be misused unintentionally. Messages may be phrased in different manners depending on the medium and are likely to require corresponding phrasing for outbound communication. These differences all require different kinds and levels of processing and robustness of technologies.

Motivated by the above criteria and short-comings of current research we introduce a novel approach for cross-media, cross-lingual and multimedia processing of a variety of sources used during crises and disasters. Our approach aims at detecting connections between and across the different types of media – such as hashtags being mentioned on TV, links in tweets to YouTube videos or images on Flickr – and relating these links to phases of disasters and emotional states and needs of the affected population. The goal is to automate this process and to automatically detect and follow such links, integrate and process the linked-to data, make it available for analysis

and to provide the resulting combinations as a basis for situational awareness. Patterns in these connections (e.g. more images on Instagram being linked-to from tweets in the initial phases of a disaster vs more web-content being linked-to in later stages) are expected to yield detailed information. The detection of particular patterns of cross-media communication between traditional and social media is envisaged to allow for more effective and efficient responses and communication by first-responders.

The following figure displays the sources considered in our approach.




The poster introduces the approach itself, the QuOIMA project (started in November of 2012) dealing with the development and implementation of the outlined approach and its current state and application to data gathered during the floods in Central Europe in May and June of 2013 (chosen as the first use-case of the project). The poster furthermore covers the data-collection and corpus-creation process, details the corpus itself, elaborates on the selected use-case, outlines the system architecture and components used (and already in operation) and presents some initial findings and further alleys of research.

**Authors**

**Gerhard Backfried**
Sail Labs Technology AG,

University of Vienna, Multimedia Information Systems Research Group
gerhard@sail-labs.com

**Katja Prinz**
Sail Labs Technology AG
katja@sail-labs.com

**Gerald Quirchmayr**
University of Vienna, Multimedia Information Systems Research Group
gerald.quirchmayr@univie.ac.at

**Johannes Göllner**
National Defence Academy, Dept. of Central Documentation, Austrian MoD
johannes.goellner@bmlvs.gv.at

**Gerald Czech**
Austrian Red Cross
gerald.czech@roteskreuz.at

## International Society of Military Sciences Conference 2014

Austrian National Defence Academy, Vienna, 21- 23 October 2014

The Austrian National Defence Academy, The Royal Military College of Canada, the Royal Danish Defence College, The Finnish National Defence University, the Netherlands Defence Academy, the Norwegian Education Command, the Swedish National Defence College, and the Baltic Defence College established in October 2008 a society intended to further research and academic education in military arts and sciences in the broadest sense. The purpose of this organisation is to build a network for the creation, development, exchange and diffusion of research and knowledge about war, conflict management and peace support efforts. The society will establish an annual conference, and one or more workshops per year.

Activities include communications and publications to support a research network within topics such as: war studies; military history; military technology; command and control, leadership and basic comptence; law &ethics; security, defence policy and stratregy; armed forces and society; and defence economics and management. Participation in conferences and workshops by (outside) researchers, academics and military personnel are welcomed at any time. Conferences are also open for other interested people.

http://www.isofms.org/pagina/home.html

The extended abstract was peer-reviewed and will be presented at the conference, which will be held after the editorial dead line.

# A Meta Risk Model for Supporting Interactive Decision Making in Situation Awarness Centers

*Johannes Göllner; Christian Meurers, Andreas Peer, Klaus Mak, Gerald Quirchmayr, Martin Latzenhofer, Stefan Schiebeck, Stefan Schauer, Christine Schuster*

**Keywords:** Meta Risk Model; Risk Management; Multi-Layer Multiple Vector Model; Z-Model; Human Factors; Motivation and Behaviour Models; Risk Sense; Situation Awareness Centers

**Acknowledgement:** This research is based on the research project „MetaRisk“, supported and partially financed by KIRAS (Austrian National Security Research Programme, http://www.kiras.at/).

## Introduction

In this paper we introduce a meta risk model enabling an abstract view of risk management in general. The underlying open world assumption and the structured method of applying the model allows to consistently integrate various approaches and procedures for e.g. disaster classification, involved roles like first responders, local government, military or administrative personnel. Starting with the recently developed IT-specific model of RiskSense[1], which is using the catalogues of the German IT-Grundschutz, we provide a new possibility for interactive decision making, especially for the needs of Situation Awareness Centers (SAC). In this context, first responders can quickly and effectively gain necessary insights into potential risk factors and their dependencies. Additionally using the structured procedural Z-Model[2], information is gathered and analyzed to identify scenarios, feeding the functional meta risk model to enable transparent decision-

[1] S. Schiebeck, "An advanced risk assessment method for dependency models in critical infrastructures" in: J. Wolby, S. Blahfellner, W. Hofkirchner (Eds.), "Civilisation at the Crossroads, Response and Responsibility of the Systems Sciences", Book of Abstracts, URL: [http://emcsr.net/wp-content/uploads/2014/04/BoA-EMCSR-2014.pdf], Vienna: EMCSR 2014 conference, 2014 pp. 641-645

[2] J. Klerx, J. Göllner, K. Mak, „Horizon Scanning for Emerging Risks in Supply Chains“, presentation 24.04.2014, Vienna: EMCSR 2014 conference, 2014

making.

**State of the Art and Frameworks**

When analyzing the current state of the art in knowledge management, risk analysis, IT-related frameworks, and management disciplines a large number of different risk management and assessment models, methods or at least aspects can be found. Those are coming from frameworks or standards like ITIL[3], COSO[4], COBIT[5], IT Grundschutz[6], ISO 31000[7], ISO 27005[8], OCTAVE[9], NIST[10], etc. Furthermore, examining Austrian and European Union legislations (e.g. enterprise law, share law, Solvency II, Basel III, 8th Audit Directive, anti-money laundering directive etc.) as well as scanning for particular risk aspects of motivation, fraud, and business models in the area of social science it can be found that in many cases the so called risk models or risk aspects are sometimes only reduced to the minimal conclusion "risk management has to be applied", without a further description of how this could be achieved or a reference to one of the frameworks or standards mentioned above. In fact, all risk management

[3] Office of Government Commerce (OGC), ITIL Edition 2011, "Information Technology Infrastructure Library", 5 books: Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement, Norwich: The Stationery Office (TSO), 2011

[4] Committee of Sponsoring Organisations (COSO) "Internal Control-Integrated Framework and Appendices", Post Public Exposure Version, New York: Durham, 2013

[5] Information Systems Audit and Control Association, COBIT Framework, "Control Objectives for Information and Related Technology (COBIT) 5", Rolling Meadows, Illinois: ISACA, 2012

[6] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz, Bd. 13. EL, Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2013

[7] International Organization of Standardization, "ISO/IEC 31000 Risk management – Principles and guidelines", Geneva: ISO copyright office, 2009.

[8] International Organization of Standardization, "ISO/IEC 27005 - Information technology -- Security techniques -- Information security risk management", second edition, Geneva: ISO copyright office, 2011.

[9] Software Engineering Institute, Carnegie Mellon University, OCTAVE, "Operationally Critical Threat, Asset, and Vulnerability Evaluation", version 2, Pittsburgh, Pennsylvania: Carnegie Mellon University, 2008

[10] National Institute of Standards and Technology, U.S. Department of Commerce, NIST Special Publication 800-30, Information Security, "Guide for Conducting Risk Assessments", revision 1, Gaithersburg, Maryland: NIST, 2012.

models tend to follow a quite similar but not a real common approach. Consequently, the suggested meta risk model will address the problem of inconsistent and isolated, highly domain-specific models, originating from the lack of a generic risk management approach. Therefore, we used RiskSense[11] as the framework for a situation awareness platform and integrated supporting models like the Multi-Layer Multiple Vector Model[12],[13] or the Z-Model[2]. Additionally, we focused on human risk factors to be integrated into the meta risk model to support scenario analysis by covering social science factors.

**Prototype (Risk Sense)**

In RiskSense Stefan Schiebeck implemented a risk management approach and set up a supporting prototype on the commonly accepted structured model of IT-Grundschutz, allowing the identification, estimation and modeling of dependent organizational assets, protection criteria, threats, safeguards and roles. The main motivation was to provide a simple web tool to support collaborative, interactive decision making. It can be applied as an interactive decision support system aimed at efficiently performing risk management tasks. The method and supporting software prototype has been extensively evaluated by the Austrian Federal Ministry of Defence and Sports and showed high potential for operational deployment.

**Underlying Concepts and Models**

Furthermore, with the Multi-Layer Multiple Vector Model[12],[13] as a basic classification scheme, the Z-Model[2] enables a comprehensive scenario planning process, leading to a functional meta risk model. The developed concept for a generic meta risk model includes all aspects of the studied

[11] S. Schiebeck, "An Approach to Continuous Information Security Assessment focused on Security Measurements", PhD thesis, Vienna: University of Vienna, 2014

[12] J. Göllner, C. Meurers, A. Peer, L. Langer, M. Kammerstetter; „Bedeutung des Risikomanagements für die Sicherheit von Smart Grids“, 13. Symposium Energieinnovation, 12.02.-14.02. 2014, Graz: Austrian Energy Agency, 2014, pp. 282-284

[13] J. Göllner, C. Meurers, A.Peer, G. Povoden, “Hybridisation of Social Network Analysis in Context with other Methods for a Scenario Based Risk Analysis-Case Study: Critical Infrastructure for Energy Security in Austria”, presented at 7th Social Network Conference 2011, London: University of Greenwich, 2011

approaches, methods and models by setting up a general conceptual level. Any specific model should be considered as a particular version of the generic meta model, using a common data representation. By doing so, we harmonize the core aspects and prepare them for a standardized treatment. The ultimate objective is to develop a robust model which can be flexibly applied for different purposes and by different roles.

**Further Work and Outlook**

The "Meta-Risk-Approach" allows to take several models, abstraction layers and parameters into account in order to provide a function-oriented meta risk model. Currently we plan to develop the specifications behind the described high-level processes, their interactions and resulting requirements.

The basic demonstrator requirements are aligned with the RiskSense prototype, allowing the integration of sensors and expert knowledge into the meta risk model. The resulting software demonstrator is planned to be evaluated in the context of Situation Awareness Centers (SAC) by the Austrian National Defence Academy, which is supporting the Austrian Armed Forces in providing domestic aid in the case of natural catastrophes and disasters.

The overall goal of our research concept is the advancement of existing situational reporting capabilities already implemented in RiskSense, by incorporating additional modelling options based on human factors and strategic long-term scenario planning as provided by the Z-Model. Therefore, the meta risk model enables a comprehensive, scalable, generic and domain-independent risk assessment for all layers and parts of an organisation to develop, implement and enhance a common and advanced risk management as basis for a "shared risk awareness".

**References**

- Office of Government Commerce (OGC), ITIL Edition 2011, "Information Technology Infrastructure Library", 5 books: Service Strategy, Service Design, Service Transition, Service Operation,

Continual Service Improvement, Norwich: The Stationery Office (TSO), 2011.
- S. Schiebeck, "An Approach to Continuous Information Security Assessment focused on Security Measurements", PhD thesis, Vienna: University of Vienna, 2014.
- S. Schiebeck, "An advanced risk assessment method for dependency models in critical infrastructures" in: J. Wolby, S. Blahfellner, W. Hofkirchner (Eds.), "Civilisation at the Crossroads, Response and Responsibility of the Systems Sciences", Book of Abstracts, URL: [http://emcsr.net/wp-content/uploads/2014/04/BoA-EMCSR-2014.pdf], Vienna: EMCSR 2014 conference, 2014 pp. 641-645
- Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz, Bd. 13. EL, Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2013.
- International Organization of Standardization, "ISO/IEC 27005 - Information technology -- Security techniques -- Information security risk management", second edition, Geneva: ISO copyright office, 2011.
- Information Systems Audit and Control Association, COBIT Framework, "Control Objectives for Information and Related Technology (COBIT) 5", Rolling Meadows, Illinois: ISACA, 2012.
- National Institute of Standards and Technology, U.S. Department of Commerce, NIST Special Publication 800-30, Information Security, "Guide for Conducting Risk Assessments", revision 1, Gaithersburg, Maryland: NIST, 2012.
- Software Engineering Institute, Carnegie Mellon University, OCTAVE, "Operationally Critical Threat, Asset, and Vulnerability Evaluation", version 2, Pittsburgh, Pennsylvania: Carnegie Mellon University, 2008.
- International Organization of Standardization, "ISO/IEC 31000 Risk management – Principles and guidelines", Geneva: ISO copyright office, 2009.
- Committee of Sponsoring Organisations (COSO) "Internal Control-Integrated Framework and Appendices", Post Public Exposure Version, New York: Durham, 2013
- C. Meurers, J. Göllner, S. Schauer, S. Schiebeck, A. Peer, M. Stierle: Meta Risk Model for Critical Infrastructures, in: J. Wolby, S. Blah-

fellner, W. Hofkirchner (Eds.), "Civilisation at the Crossroads, Response and Responsibility of the Systems Sciences", Book of Abstracts, URL: [http://emcsr.net/wp-content/uploads/2014/04/BoA-EMCSR-2014.pdf], Vienna: EMCSR 2014 conference, 2014 pp. 616-621
- J. Göllner, C. Meurers, A. Peer, L. Langer, M. Kammerstetter; „Bedeutung des Risikomanagements für die Sicherheit von Smart Grids", 13. Symposium Energieinnovation, 12.02.-14.02. 2014, Graz: Austrian Energy Agency, 2014, pp. 282-284
- J. Göllner, C. Meurers, A.Peer, G. Povoden, "Hybridisation of Social Network Analysis in Context with other Methods for a Scenario Based Risk Analysis-Case Study: Critical Infrastructure for Energy Security in Austria", presented at 7th Social Network Conference 2011, London: University of Greenwich, 2011
- J. Klerx, J. Göllner, K. Mak, „Horizon Scanning for Emerging Risks in Supply Chains", presentation 24.04.2014, Vienna: EMCSR 2014 conference, 2014

**Authors**

**Johannes GÖLLNER, Christian MEURERS, Andreas PEER, Klaus MAK**
Department of Central Documentation & Information, National Defence Academy of the Austrian Federal
Ministry of Defence and Sports, Vienna, Austria
johannes.goellner@bmlvs.gv.at, andreas.peer@bmlvs.gv.at,
christian.meurers@bmlvs.gv.at, klaus.mak@bmlvs.gv.at

**Gerald QUIRCHMAYR, Martin LATZENHOFER**
Research Group Multimedia Information Systems, University of Vienna, Vienna, Austria
gerald.quirchmayr@univie.ac.at, martin.latzenhofer@univie.ac.at

**Stefan SCHIEBECK, Stefan SCHAUER**
Safety & Security Department, Austrian Institute of Technology, Vienna, Austria
stefan.schiebeck.fl@ait.ac.at, stefan.schauer@ait.ac.at

**Christine SCHUSTER**
Institute for Empirical Social Studies, Vienna, Austria
christine.schuster@ifes.at

# EGPL/EPLO 2014

**2014 Annual Reunion of the European Group of Public Law (EGPL)**

*New Challenges of Democracy / Les nouveaux défis de la démocratie*

Anargyreios Korgialeneios School, Spetses, Greece, 12-14 September 2014

European Scientific Council of the EPLO,

# New opportunities and challenges for participation in crisis and disaster relief

*Karin Rainer, Ines Levy, Julia Schmid, Katharina Götsch, Gerald Quirchmayr, Johannes Göllner, Nina Forst, Gerhard Backfried*

The QuOIMA project as example for interaction, participation and privacy protection in disaster management

**Abstract:** Crises and disasters occur all over the world with the highest impact on the most vulnerable in society. Generating a thorough and trusted status of information about the situation is apriority for effective and coordinated disaster management and relief measures delivered by governmental organizations (GOs) and non-governmental organizations (NGOs) in the surroundings of a critical event. . Information gathering, processing, visualization and (internal as well as external) dissemination for decision support and mitigation is performed via a number of different channels and media, among them various social media channels. The QuOIMA-project, funded by the Austrian Security Research Program KIRAS by the Austrian Ministry of Transport, Innovation and Technology, focuses on the various possibilities to use publicly available, open source data generated in the sphere of traditional (online distributed) and social media. These data can be used on the one hand as a vital input for situation awareness and decision support of disaster management; on the other hand they can be used to initiate and maintain active, bidirectional, participatory involvement of community members in case of a serious event – under the prerequisite precondition of a trusted, reliable, and privacy safeguarding framework. Subsequently, relevant core issues of privacy rights and the Privacy Impact Assessment applied in the course of the project QuOIMA are discussed.
But even before crises occur, precautions can be taken by monitoring social media sources such as Facebook, Twitter or specific blogs. Risk indicators can be identified more quickly, structures and work plans for disaster management can be set up. One of those means that will be outlined in this context is the new and emerging crowd tasking approach, a promising and high potential area for the involvement of community members.

**Keywords:** QuOIMA, participation, disaster management, disaster resilience, privacy protection, privacy impact assessment, trust in society, trusted information, enhancement of inclusion, crowd tasking

**Acknowledgement:** The QuOIMA project (2012-2014) is supported by the Austrian National Security Research Programme KIRAS by the Ministry of Transport, Innovation and Technology.

## 1 Introduction – The QuOIMA-approach[1]

Crises and disasters are constantly covered and accompanied by today's media. While traditional media have a long history in covering disasters and crises, recent examples of natural as well as man-made disasters show that social media provide useful, effective, additional and complementary information and can help improve situational awareness. Social media interact with traditional media in various ways – sparking off initial coverage, providing different and sometimes unfiltered angles, or amplifying information. Together they produce a wide spectrum of data about an event. As helpful as all of this information may be, it usually comes in various formats from multiple media sources, in different languages and levels of reliability, and is generally unstructured and inhomogeneous.

To meet the challenges of using such data, the KIRAS project QuOIMA aims at developing a cross-media content analysis framework and at extending existing technologies to improve the situational awareness of decision makers. The cross-media, multimedia and multilingual approach adopted by QuOIMA is expected to allow early identification of risk indicators and factors for efficient crisis and disaster management as well as the early detection of emerging threats and trends. Improvements of situational awareness are expected and will lead to faster reaction times. From a technical viewpoint, QuOIMA is based on the SAIL LABS Media Mining System for open source information (OSINF) and on the insights gained from a previous KIRAS project, MDL. Strategically, QuOIMA is based on a five-stage disaster management model developed by the Austrian National

[1] QuOIMA - Integrated Open Source Multimedia Analysis (*German*: Quelloffene Integrierte Multimedia Analyse). Following excerpts from the project information and dissemination material of QuOIMA

Defense Academy (Backfried et al. 2013). These technical and strategic foundations form a powerful basis for improving situational awareness during natural disasters.

The investigation and development of such methods consequently form core activities within QuOIMA. Components for the analysis and selection of quality-assured scenarios for the deployment of the developed technologies as well as additional requirements posed by crisis communication within the context of enhanced early warning and resilience are further areas of activity. The comprehensive, cross-media, multimedia and multilingual approach represents unique and innovative research for crisis and disaster management. Research on sociological and legal aspects (in particular data protection, see section 4) complements and extends these activities.

Specifically, the vital factor of directly and indirectly concerned persons' trust towards official disaster management organizations and their activities during crisis situations are tightly connected with the appropriate channels and types of information distribution and thus the acceptance of communication and compliance to necessary measures (Siegrist et al. 2014). Taking into account the complex interactions and interdependencies in dynamic crisis scenarios, trust and its related phenomena and effects can only be defined as a continuum created over a long period of reliable information exchange and interaction between official disaster management organizations.

Long-term reliability as an objective criterion of information and the consistent external and internal appearance of disaster management organizations can be seen as a prerequisite for the development of trust. Even if there might be relevant and significant cross-cultural differences, the building of high-reliability organizations (Horsley 2012) and the effecting benefits for reliable internal and external information and knowledge development for effective disaster response has to be developed timely and continuously.

## 2. Communication and trust as reciprocal relationship for effective disaster response

Subsequent to the elaborated importance of intra-organizational develop-

ments in order to grant reliable information and knowledge management, interoperating components of a disaster response system, like the interaction with a potentially affected community, have to be taken into account. Specifically, the vital but often non-reflected issue of facilitating and promoting the social model of "trust" (Misztal 1996, Siegrist et al. 2007) and thus representing the capacity to fulfil specific expectations, stands for disaster response organizations in a reciprocal relationship with reliable external information management and the authentic and ongoing interaction of organization and public.

In the case of disaster response organizations, this issue seems even more crucial as the effective facilitation of relief and support measures strongly rely not only on timely, but also on target group orientated communication as Reynolds et al. (2005) summarize for the health sector. Taking into account the above mentioned, internal processes of information and knowledge development measures, the prerequisites for the development of an externalization of effective procedures can be supported. Several factors seem to be of importance for this transportation and transformation of reliable information and continuous interaction to create framework parameters enabling trust in the community.

Making internal quality markers and their benefits visible for the public can be one step in the generation of trust-supporting knowledge within the community. Another impetus of the implementation of trust and the compliance and cooperation of citizens as a core systemic factor in disaster response can be the application of an adapted and simplified version of knowledge development and monitoring on the community level. These approaches can be implemented in the prevention and initialization phase (Backfried et al. 2013) of the 5-phase disaster model. In this phase a trusted communication and interaction network between the various stakeholders of complex disaster response (Currao 2009) – including the community – can be facilitated. Only with this early provision and introduction of information flow, a resilient and efficient communication structure can be established that persists under the pressure of dynamically changing disaster surroundings.

These structures and mechanisms have to be initialized, tested and optimized to be ready for the operational intervention and management phase

(Backfried et al. 2013) in particular for the critical pre-execution and execution phase framing the impact of a critical event. Referring to traditional and new media approaches in crisis communication (Rainer et al. 2013, Lindsay 2011) timely and target group oriented communication can be identified in these phases as structural pillars of efficient disaster response. Various channels (Utz et al. 2013) and possibilities of the multiple modes of information exchange between stakeholders and actors (Rainer et al. 2013, Backfried et al. 2013) can be used for this purpose. Information gathering via open sources, supporting situation awareness and visualization of the event, communication as the one-directional delivery of instructions and advice or the interactive collaboration following the crowd tasking approach are some of these approaches. In the study SMD4Austria (Rainer et al. 2013), funded by the Austrian National Security Research Program KIRAS by the Ministry of Transport, Innovation and Technology, these structures were made visible for social media services:

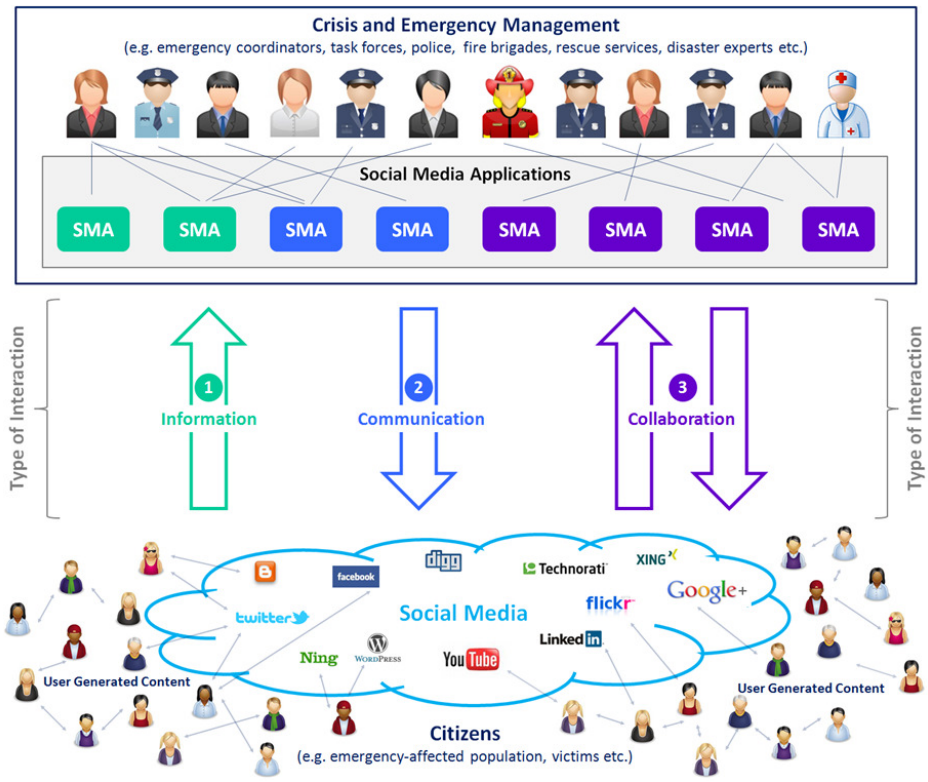



**Fig. 1: The major fields of social media services assistance to crisis managers (Rainer et al. 2013)**

For this highly dynamic, incoherent (regarding quality and reliability of information), and participatory sphere of information exchange the question of trust, trusted information and reliable data has to be considered closely by disaster response organizations and public entities. These aspects represent some of the most pressing current challenges of this high potential topic.

## 3. The communication and decision support model of QuOIMA

Transferring the generic approach of communication and interaction possibilities (as visualized in figure 1) to the specific approach of the QuOIMA project, it becomes clear that next to trusted information a dynamic model as the backbone of an integrated communication and decision support is

necessary. In this context the active participation and integration of community members in relief activities of crisis management professionals can be incorporated into the communication and action cycle.

Figure 2 shows a cyclic, adaptive, and dynamic system with four basic continua and four main processes representing the information and activity flows. The visualized model takes into account the analytic framework of QuOIMA and the role and actor concept developed with the Central Documentation Department of the National Defense Academy. Its relevance and usability for other organizations in the field of crisis and disaster management will be tested and validated in further research.

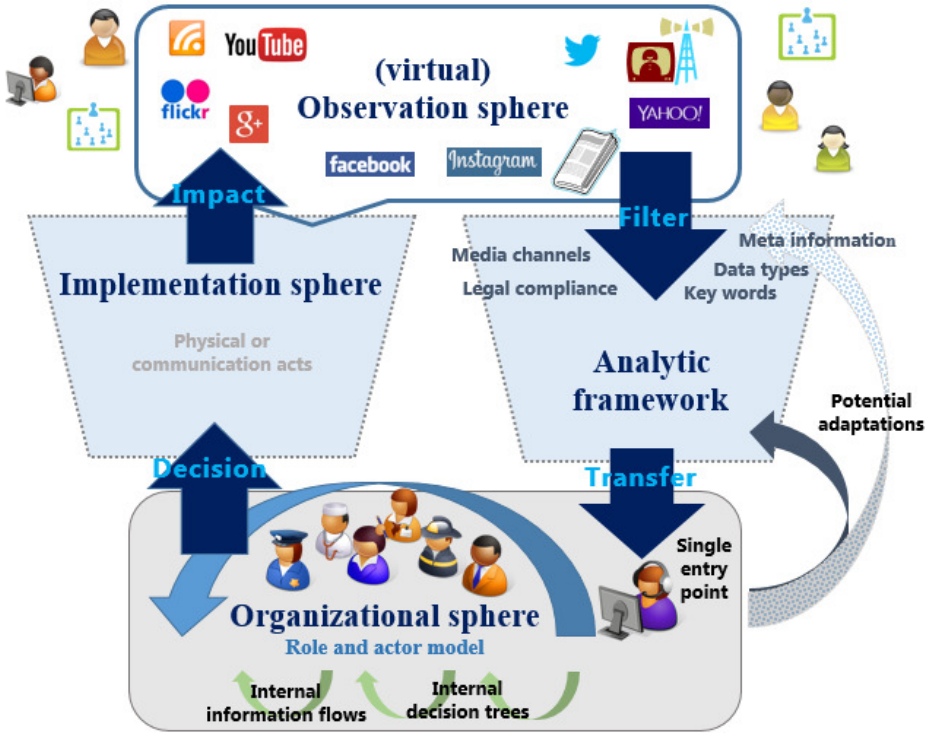



**Fig. 2: Communication and decision support model of QuOIMA**

Using the virtual observation sphere where online communication and information acts of the community via social media or by professional media organizations "serve as an arbitrary starting point, the collectivity of mani-

festations undergoes a pre-set filter process. In an initial setting the filters need to be tailored to the particular organization. In a running cycle it can be adapted regarding the current necessities and requirements of the setting, event or organization status. The filter settings can have different qualities and quantitative thresholds and refer e.g. to technical as well as to topic or source related factors. Even reliability parameters can be taken into account given that the required framework parameters can be provided to the filter layer.

The communicated data – consisting of the already filtered manifestations passing the gatekeeper – are handled regarding the QuOIMA logic in the analytic framework and brought into a given structure including refined and ongoing developing visualizations (Backfried et al. 2013). In a next step the information is transferred to a predefined entry point of the regarding organization or integrated management unit.

In this organizational sphere the internal processes of data and information management take place. Regarding the type of incident respectively the generic issue of observation, the pre-defined steps of further data procession, forwarding and – if necessary with suitable adaptation of the filter process and the analytic framework – extension are realized. In this subsystem the processed information flows into decision support structures and tools. Automated, software assisted or traditional decision trees are fed by this input and lead – after possible adaptations and shifts of filter parameters and other additional measures – to a continuous optimization of situation awareness.

The operational decision process leads to the implementation sphere. Physical acts, e.g. of disaster relief, or communication acts are facilitated and have impact onto the virtual manifestations of communication in the observation sphere. One specific form of implementation acts is crowd tasking. Having a very prominent position in the scientific and experimental use of social media in crisis and disaster management (Wetzstein et al. 2014), this major aspect and potential development scope of the QuOIMA components will be outlined in section 0. Of high importance for this practical use of open access data from social media sources is the implementation of and compliance to given legal standards and framework conditions regarding privacy and data protection (Grubmüller et al. 2013, Götsch et al.

2013). This will be discussed in the following section.

## 4. Aspects of privacy rights observed in QuOIMA[2]

As already mentioned, besides the technical, sociological and communication oriented prerequisites privacy has a major impact on the transfer of project approaches like QuOIMA into practice. Privacy has to be safeguarded as trust between the public and also governmental entities and is crucial when dealing with crises and disaster management. Therefore, legal standards and framework conditions were set up to meet these requirements.

The central article for privacy matters – regarding the implementation of QuOIMA components for example – when crises occur is §48a of the Austrian Data Protection Act (DSG). These regulations were created to allow organizations to take necessary steps and measures to support affected persons and their families in compliance with data and privacy protection. §48a thus regulates the use of data in the event of a disaster as *Lex Specialis*. This provision now allows public bodies explicitly to use personal information for the following purposes:

- assistance to persons directly affected by a disaster;
- identification of a missing or deceased person;
- information of next of kin;
- participation in a joint information system, if necessary for the rapid coping with a disaster;
- data transmission to and use of data by organizations as part of their duties, to the extent necessary to overcome the disaster.

Once data for the fulfillment of a specific purpose in the context of disaster management are no longer needed, they must be deleted immediately. The following points should be noted regarding the admissibility of data transfer or data transmission:

A data transfer or transfer abroad (cross-border transfer) is permissible if it is necessary to deal with a disaster. Similarly, the participation in a joint

[2] Translation following excerpts from Quirchmayr (2014).

information system is allowed in this case. The transmission for identification purposes and sensitive information for identification purposes to such a system may only take place if there is concrete evidence that the missing person is likely to be deceased.

Data that incriminates only the person affected shall not be transferred unless such measures are strictly necessary to identify the individual case.

When crises occur, one important point is information for and specific inquiries from next of kin. The transmission of data of next of kin is only permitted in pseudonymous form. For this kind of request specific regulations come into force and have to be considered specifically. The Austrian Law provides regulations that, for instance, social security institutions are obliged to support clients of public entities and aid in verifying data of possibly missing or deceased persons. Furthermore, clients are authorized to transmit data on travel in and out of disaster areas. Close family members of clients of the public sector and aid organizations may provide eventually sensitive data. They can also be transmitted directly by the affected persons. Prerequisite is that they can prove their identity and their loved ones' property and the information to protect its rights.

Also, data may only be transferred out of or in countries without adequate data protection level if the legitimate confidentiality interests of the planned traffic concerned are safeguarded adequately and abroad.

A transfer or assignment must then be omitted if there is reason to believe that the recipient does not ensure the necessary protection of the confidentiality interests of those affected or will disregard explicit data protection requirements of the client.

The Austrian Data Protection Commission has to be informed immediately of the originated transfers and assignments and the surrounding circumstances of the event giving facts of the crisis occurred.

The Austrian Data Protection Commission may prohibit data transfers or assignments if the protection of the rights of those affected is not guaranteed and the infringement of the fundamental right to privacy by the particular circumstances of the disaster situation is not justified.

## 5. QuOIMA and the Privacy Impact Assessment (PIA)[3]

To meet the conditions set up in the previous section, it was considered helpful in the course of the QuOIMA project to apply the five-step plan of the Privacy Impact Assessment (PIA)[4]:

1. Project description: Broadly describe the project, including the aims and whether any personal information will be handled.
2. Mapping the information flows and privacy framework: Describe and map the project's personal information flows and document all relevant legislative and organizational rules.
3. Privacy impact analysis: Identify and analyze the project's privacy impact.
4. Privacy Management: Consider how to manage any privacy impact, particularly options that will improve privacy and still achieve the project's goals.
5. Recommendations: Produce a final PIA report covering the above stages and including recommendations.

It is therefore proposed to perform this analysis as the next step for the scenarios developed in the project. For the following aspect and potential of the use of open source data management it would be a prerequisite to apply the assessment. Under this prerequisite and the implementation of the recommended outputs a big step towards the legally correct use of data in the sphere of disaster management but also for preventive measures is accomplished.

As discussed in the next section, this will be a major point for the compliance and the general active use and practical appliance of the communication and decision support model.

[3] Translation following excerpts from Forst (2014).

[4] http://www.oaic.gov.au/privacy/privacy-archive/privacy-resources-archive/privacy-impact-assessment-guide#_Toc144200856 (retrieved: July 29, 2014)

## 6. Participatory potential of disaster management: crowd tasking

Compiling the singular aspects of QuOIMA, developing this approach even further and taking into account the crucial importance of reliable, trusted, and specially filtered information, this leads to the growing potential of participatory interaction of disaster management and the community members in case of crises.

The initial communicative act builds the backbone of crowd tasking. It aims at raising awareness, mobilizing, and integrating willing and able community members and digital volunteers (Starbird 2012a) to support a variety of relevant measures. Levels of crowd sourcing as Poblet et al. (2014) describe them (see Fig. 3) show the virtual area of a broad range of possible means of involvement of users in case of serious crisis events.

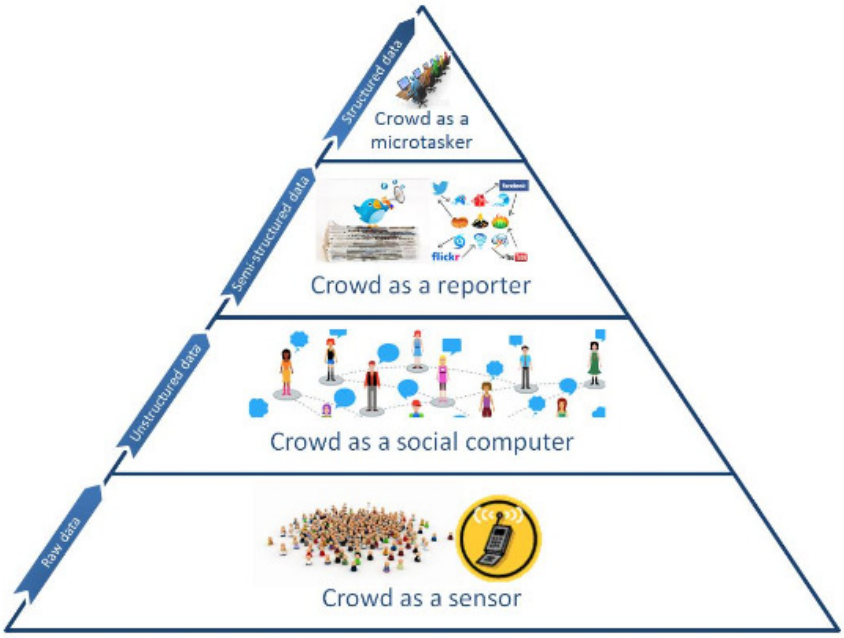



**Fig. 3: Crowdsourcing roles based on user´s involvement and level of data processing (Poblet et al. 2014)**

This role model can be relevantly enlarged by subsequently transgressing the virtual sphere and involving a local hands-on approach of crowd tasking. Thus, a development or enhancement of "crowds as knowledge generators", crowd-map generators and resource locators (Dietrich et al. 2013) towards active, ad-hoc volunteers and helpers can take place.

The facilitation of an active involvement as Wetzstein et al. (2014) introduce, seems to be an evolving factor in crisis management but also in taking the opportunity of enhancing participation and thus self-reliability as an important means for effective interaction of GOs, NGOs and communities. Even if we take into account the still existing and unsolved question of the digital divide (Easton 2014) and related challenges of a broad and equal inclusion of community members in emergency situations, crowd tasking as piloted in several national and international projects and discussed by Neubauer et al. (2013) is a means of high potential.

Not only in the hot phase of crisis and disaster handling but also in prevention of critical events the inclusion and participation of citizens and the pro-active interaction and exchange with relevant organizations (see Fig. 1) lead to an enhancement of trust. This again is one of the major factors of compliance of necessary measures in disaster relief as e.g. evacuations and also for the development of a trusted network of ad-hoc volunteers that can be included in crowd tasking activities.

## 7. Conclusions

New trends and developments in recent years such as crowd tasking and the use of open source data such as the ones collected and generated in the QuOIMA project might be supportive for filling current gaps in future disaster management to optimize efficiency and the use of scarce resources. A systemic, integrative social media communication and decision support model as discussed here might support the understanding and further steps of development and implementation of the generated components into broader practical use.

Aspects as potential development and enhancement of inclusion and trust in society seem specifically crucial in crisis and emergency situations where compliance of directly and indirectly (e.g. virtually) affected persons is a

major factor for effective and efficient disaster relief. Also the areas of privacy and data protection, which are inherent elements of the QuOIMA progress, and which are considered as crucial issues for the sensible everyday use have to be further observed and have to accompany developments regarding the use of open source data.

Although there are still several questions unanswered and challenges to be tackled and still emerging like the digital divide, the stability of the critical infrastructure communication, the reliability of information or questions of privacy and data protection in connection with the mission of disaster relief and mitigation actions, it is evident that the QuOIMA approach and its framework models can contribute to an enhancement and leverage of participation and a trustful, active relationship of community members and crisis management organizations.

**References**


- Backfried, G., J. Göllner, G. Quirchmayr, K. Rainer, G. Kienast, G. Thallinger, C. Schmidt, A. Peer (2013): *Integration of Media Sources for Situation Analysis in the Different Phases of Disaster Management*. The QuOIMA Project. 2013 European Intelligence and Security Informatics Conference. EISIC 2013.31, 143-146.
- Currao, T. J. (2009): *A New Role for Emergency Management: Fostering Trust to Enhance Collaboration in Complex Adaptive Emergency Response Systems*. Master Thesis. Monterey: Naval Postgraduate School.
- Dietrich, C., P. Pawlak (2013): *Crowd-sourcing – crisis response in the digital age*. European Union Institute for Security Studies. Issue Alert 39.2013.
- Easton, C. (2014): *The digital divide, inclusion and access for disabled people in IT Supported Emergency Response Systems: A UK and EU-based analysis*. In: Proceedings of the 11th International ISCRAM Conference – University Park, Pennsylvania, USA, May 2014. S.R. Hiltz, M.S. Pfaff, L. Plotnick, and P.C. Shih (eds.), pp. 280-283.
- Forst, N. (2014): *Ein Vorgehensmodell zur Identifikation datenschutzrechtlich relevanter Informationsflüsse bei der Verwendung von Sozialen Medien im österreichischen Krisen- und Katastrophenschutz*. University of Vienna (Master thesis, in review).

- Götsch, K., Grubmüller, V., Pejic, I. (2013): *The UniteEurope Project. Social Media Analytics for Policy Making and Decision Support*, CeDEM – Conference for eDemocracy and Open Government 2013, Krems/Austria.
- Grubmüller, V., Krieger, B., Götsch, K. (2013): *Social Media Analytics for government in the light of legal and ethical challenges*, CeDEM – Conference for eDemocracy and Open Government, Krems/Austria.
- Horsley, S. (2012): *Crisis-Adaptive Public Information: A Model for Reliability in Chaos*, in: W. T. Coombs, S. J. Holladay (Eds.): The Handbook of Crisis Communication. Chichester: Wiley-Blackwell, pp. 550-567.
- Lindsay, B. R. (2011): *Social Media and Disasters: Current Uses, Future Options, and Policy Considerations.* Congressional Research Service, 2011. http://www.infopuntveiligheid.nl/Infopuntdocumenten/R41987.pdf retrieved: 11.07.2014.
- Misztal, B. (1996): *Trust in Modern Societies: The Search for the Bases of Social Order*. Cambridge: Blackwell.
- Neubauer, G., A. Nowak, B. Jager, C. Kloyber, C. Flachberger, G. Foitik, G. Schimak (2013): *Crowdtasking – a new concept for volunteer management in disaster relief*. In: Environmental Software Systems. Fostering Information Sharing. IFIP Advances in Information and Communication Technology Volume 413, 2013, pp 345-356.
- Nilsson, S., J. Brynielsson, M. Granasen, C. Hellgren, S. Lindquist, M. Lundin, M. N. Quijano, J. Trnka (2012): *Making use of New Media for pan-European Crisis Communication*. Proceedings of the 9th International ISCRAM Conference–Vancouver, Canada, April 2012, L. Rothkrantz, J. Ristvej, Z. Franco, eds.
- Poblet, M., E. García-Cuesta, P. Casanovas (2014): *IT Enabled Crowds: Leveraging the Geomobile Revolution for Disaster Management*. In: Proceedings [!] of the Sintelnet WG5 Workshop on Crowd Intelligence: Foundations, Methods and Practices. Marta Poblet, Pablo Noriega and Enric Plaza (eds.) Barcelona, Catalonia. January, 8-9 2014, pp. 16-23.
- Quirchmayr, G. (2014): *Datenschutzrechtliche Aspekte – Analyse der derzeitigen Situation*. Internal document of the QuOIMA project (not public).

- Rainer, K., V. Grubmüller, I. Pejic, K. Götsch, P. Leitner (2013): *Social Media Applications in Crisis Interaction.* Systems. Connecting matter, life, culture and technology, 2013, 1, 1, 110-127.
- Reynolds, B., M. W. Seeger (2005): *Crisis and Emergency Risk Communication as an Integrative Model.* Journal of Health Communication, 10:43-55.
- Siegrist, M., A. Zingg (2014): The role of public trust during pandemics: Implications for crisis communication. European Psychologist, Vol 19(1), 2014, 23-32.
- Siegrist, M, T. C. Earle, H. Gutscher (Eds.) (2007): *Trust in Cooperative Risk Management: Uncertainty and Scepticism in the Public Mind.* London: Earthscan.
- Starbird, K. (2012a): *Crowdwork, Crisis and Convergence: How the Connected Crowd Organizes Information During Mass Disruption Events*. Thesis submitted to the Faculty of the Graduate School of the University of Colorado.
- Starbird, K. (2012b): *What "Crowdsourcing" obscures: Exposing the Dynamics of Connected Crowd Work during Disasters.* University of Colorado Boulder, Proceedings, CI 2012.
- Utz, S., F. Schultz, S. Glocka (2013): *Crisis communication online: How media, crisis type and emotions affected public reactions in the Fukushima Daiichi nuclear disaster.* Public Relations Review 39, 40-46.
- Wetzstein, I., V. Grubmüller, K. Götsch, K. Rainer (2014, forthcoming): *Crises and social media: A meta-study on pertinent research and practice.* In: Community Resilience in Crises: Technology and Social Media Enablers special issue of Human Technology: An Interdisciplinary Journal of Humans in ICT Environments.

**Authors**

**Karin Rainer**
Dr. Karin Rainer (Project Coordinator for AEI), Project Manager at AEI, graduated with distinction at the Philosophic Department of the University of Vienna, postgraduate training in social research and thorough research and communication experience. Ms. Rainer worked in public administration, at the Research Institute of the Red Cross, INSET Research & Consulting, for a PR agency and as a freelancer in training, moderation and

consulting. Ms. Rainer´s core expertise covers the fields of Sociologic Research, Innovation Cycles, Crisis-, Disaster and Risk Management, and user-focused topics such as human factor analyses, social media analytics, evaluation, gender issues, usability, training, and needs assessment. She has experience in the successful scientific handling and administrative coordination of several national and international projects with strong innovation focus (FP7 UniteEurope, FemSMA, benefit SECONET, FP7 CAST, KIRAS SMD4Austria, QuOIMA, SimRad.NBC & COMP…).

**Ines Levy**
Ines Levy, B.A. is staff member at AEI and responsible for scientific research and project support. She has an economic background and holds a B.A. from the University of Vienna in social sciences with specific focus on policy research, evaluation, crisis research and urban sociology. She is experienced in qualitative and quantitative sociologic methods and analysis including technologic supported analyses. She is currently working on a national research project focusing on Crisis Management and Social Media impact (KIRAS QuOIMA).

**Julia Schmid**
Mag. Julia Schmid, is staff member at the Austrian Ministry of Finance (BMF) and responsible for project management. She holds a Master's Degree in Law with special focus on international law from the University of Vienna and the University of Oslo. Ms. Schmid has also worked as an advisor for the Permanent Mission of Austria to the United Nations in New York City with a special emphasis on economic, legal and social committees and topics. She has experience on project management and conference management through various UN student-level conferences and as a lawyer working for international law firms in Austria.

**Katharina Götsch**
Dr. Katharina Götsch is a political scientist and holds a PhD from the University of Vienna. She has been working in social science research for several years within national and international projects (FP7, JPI UrbanEurope, KIRAS etc.) mostly related to social media and public policy. Her research areas are social media, international relations and political theory and she publishes extensively in her fields of expertise. She currently works at the University of Vienna as a Project Coordinator and Lecturer and the

AEI (QuOIMA project).

# DEXA 2010

## 21st DEXA Conference

*Understanding the Human Genome: A Conceptual Modeling-Based Approach*
Bilbao, Spain, University of Deusto, 30 August - 3 September 2010

Information systems and database systems have always been a central topic of computer science. Additionally the integration of knowledge, information and data justifies its today's attractiveness. Since 1990 DEXA is an annual international conference, located in Europe, which showcases state-of-the-art research activities in these areas.

DEXA 2010 was held in Bilbao, Spain, during August 30 - September 3, 2010. It continues to provide a forum for presenting research results in the area of database and intelligent systems and discussions on advanced applications and issues related to these areas. It offered the opportunity to extensively discuss requirements, problems, and solutions in the field. The workshop and conference should inspire a fruitful dialogue between develop ers in practice, users of database and expert systems, and scientists working in the field.

http://www.dexa.org/previous/dexa2010/files/CfP_dexa_9.Feb_last.extension.pdf

The peer-reviewed paper was published in the conference proceedings:
David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell, Moni Naor, Oscar Nierstrasz, C. Pandu Rangan, Bernhard Steffen, Madhu Sudan, Demetri Terzopoulos, Doug Tygar, Moshe Y. Vardi, Gerhard Weikum, Kim Normann Andersen, Enrico Francesconi, Åke Grönlund, Tom M. van Engers (Hrsg.), Electronic Government and the Information Systems Perspective, First International Conference, EGOVIS 2010, Bilbao, Spain, August 31 – September 2, 2010. Proceedings

# Intellectual Capital Management using Knowledge Scorecards: The Austrian National Defence Academy Showcase

*Johannes Göllner, Klaus Mak, Robert Woitsch*

**Abstract:** This paper discusses the applicability of knowledge scorecards and intellectual capital management for monitoring and steering of knowledge-driven organizations based upon a practice project at the Austrian Defence Academy (in particular the School for Atomic, Biological and Chemical Defence). Within this project the model-driven approach PROMOTE® has been applied to develop the knowledge scorecard at the Austrian National Defence Academy. The paper presents the knowledge scorecard architecture, the method and the findings.

**Keywords:** Intellectual Capital Management, Knowledge Scorecard, Knowledge Management, PROMOTE®

## 1 Introduction

New regulations for academic institutions[1] changed the reporting responsibilities for knowledge assets within the Austrian National Defence Academy (LVAk), committing them to issueing intellectual capital reports. The concept of knowledge scorecards assures compliance with the legal reporting obligations and enables furthermore the initial step to monitor and manage the intellectual capital.

The School of Atomic, Biological and Chemical Defence (ABCAbwS) has been selected for the project, since there was pre-existing work in the domain of knowledge management that could be reused. This work consists of a committed knowledge management concept, the specification of a quality management system, initial knowledge management projects such as the acquisition of skill profiles and the definition of knowledge management processes.

[1] Universitätsgesetz 2002 Online at: http://archiv.bmbwk.gv.at/universitaeten/recht/gesetze/ug02/Universitaetsgesetz_20027727.xml

Beside the work on knowledge management that is seen as the fundament for intellectual capital management, there is an important aspect that makes the school an interesting testbed. The school not only consists of teaching parts, but also of a research part and a force provision part. This means this school combines research on ABC topics, the teaching within and outside the Austrian military but also the actual force provision in case of earthquake, water flood or other operations.

This rare constellation of research, teaching and application of knowledge within one organisation in a very complex, high-risk and dynamic environment made the application of an intellectual capital management system an interesting challenge. The project was accompanied by the LVAk as the highest military training- and research institution of the Austrian Armed Forces. It acts as the "brain trust" of the Austrian Armed Forces, and serves the forces and the Ministry of Defence with approx. 240 employees.
In the following some conceptual background will be provided to discuss existing approaches, introduce the idea of the "knowledge product" and outline how the intellectual capital management can be implemented with PROMOTE® [2] by defining the "knowledge product" as the centre point. The paper concludes with an outlook.

## 2 Conceptual Background

This section discusses related work and introduces three adaptations that were necessary in the aforementioned complex environment. The adaptations are (1) the introduction of the "knowledge product", (2) the rearrangement of the balanced scorecard as well as (3) the holistic architecture of the intellectual capital monitor.

### *2.1 Related Work*

Monitoring of knowledge management initiatives and application scenarios within a company is not something unusual, representing just a current hype.

---

[2] Woitsch R, Karagiannis D.: Process Oriented Knowledge Management: A Service Based Approach. J. UCS 11(4): 565-588 (2005)

There are various concepts for managing intellectual capital, such as the Skandia Navigator[3], the Intangible Assets Monitor[4], the Intellectual Capital Navigator [5], or more general concepts like the market-to-book ratio[6] , [7] or the comprehensive company value[8]. Moreover different approaches have been implemented over the years in order to provide an instrument for evaluating the intellectual capital and can be considered as a holistic management philosophy[9] or can be seen as novel approach bringing competitive advantage[10]. The aims for developing and implementing such an instrument may vary from realising more knowledge management friendly point of view where such tools are used to steer the initiatives as depicted in Aidermark and Sterner[11], to events where such an approach is only used to perform precise calculations of the overall asset value of the company – this view is discussed in [12]. The first obstacle on the road to creating a presentable intellectual capital balance is to perform valuing of the specific knowledge assets. There are many different approaches that tackle the concern of defining the value of the knowledge assets by applying different methods. These methods include valuing of the knowledge assets based on "Tobin's *q*" - which uses the ratio between a company's market value and

---

[3] Edvinsson, L.: Developing Intellectual Capital at Skandia, Long Range Planning, Vol. 30, No. 3, pp. 366 to 373, 1997, Elsevier

[4] Sveiby, K.E. 1997: The New Organizational Wealth, Berrett-Koehler Publishers, San Francisco.

[5] Stewart, T.A. 1997: Intellectual Capital, Nicholas Brealey Publishing, London.

[6] North, K. 1998: Wissensorientierte Unternehmensführung, , Gabler Verlag, Wiesbaden.

[7] Andriessen, D. 2004: Making Sense of Intellectual Capital, Elsevier Butterworth Heinemann, Oxford.

[8] Lev, B. 2004. Sharpening the Intangibles Edge.Harvard Business Review, vol. 2004, no. June, pp. 109-116.

[9] Johannesse, J-A., Olsen, B. and Olaisen, J.: Intellectual capital as a holistic management philosophy: a theoretical perspective, International Journal of Information Management 25 (2005) 151–171, Elsevier

[10] Chen, Y-S.: The Positive Effect of Green Intellectual Capital on Competitive Advantages of Firms, Journal of Business Ethics (2008) 77:271–286, Springer

[11] Aidemark, J. and Sterner, H.: A Framework for Strategic Balancing of Knowledge Management Initiatives, IEEE, Proceedings of the 36th Hawaii International Conference on System Sciences, 2003

[12] García-Meca, E. and Martinez, I.: The use of intellectual capital information in investment decisions - An empirical study using analyst reports, The International Journal of Accounting 42 (2007) 57–81, Elsevier

the replacement value of its physical assets to calculate the value (as depicted in the[13]) - evaluation based on the combination of Fuzzy Linguistics and MCDM14 method[15], etc.

The next step after the initial measurement method that has been chose and applied is to include the results in a reporting and monitoring mechanism – lately the trend has gone towards the presentation in the adapted balance scorecards (to be inline with the "business" part of the balance sheet). An overview on how these metrics can be connected to business strategy (in form of IC BSC) is depicted in [16].

Studies on how intellectual capital is being monitored/reported in 19 Danish enterprises can be seen in [17], a similar study concerning Finish companies can be found in [18], and UK companies in [19]. Additional reports from Slovenia[20] discussing IC from a two-tier view – customer and non-customer relationships – , the report from Taiwan evaluating what importance levels are assigned to different IC forms by company employees[21]

---

[13] Wilkins, J., van Wegen, B. and de Hoog, R.: Understanding and Valuing Knowledge Assets: Overview and Method, Expert Systems With Applications, Vol. 13, No. 1, pp. 55-72, 1997, Elsevier

[14] MCDM - multiple criteria decision-making

[15] Tai, W-S. and Chen C-T.: An Intellectual Capital Performance Evaluation Based on Fuzzy Linguistic, Proceedings of the Third International Conference on International Information Hiding and Multimedia Signal Processing (IIH-MSP 2007) - Volume 02, IEEE

[16] Fairchild, A.M.: Knowledge Management Metrics via a Balanced Scorecard Methodology, Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 8 - Volume 8, Page: 243, IEEE

[17] Bukh, P.N., Larsen H.T. and Mouritsen, J.: Constructing intellectual capital statements, Scandinavian Journal of Management, 17 (2001) 87-108, Elsevier

[18] Vuontisjarvi, T.: Corporate Social Reporting in the European Context and Human Resource Disclosures: An Analysis of Finnish Companies, Journal of Business Ethics (2006) 69:331–354, Springer

[19] Striukova, L., Unerman, J. and Guthrie, J.: Corporate reporting of intellectual capital: Evidence from UK companies, The British Accounting Review, (2008) 1-17, Elsevier

[20] Nemec Rudez, H and Mihalic, T.: Intellectual capital in the hotel industry: A case study from Slovenia, Internationa Journal of Hospitality Management 26 (2007) 188–199, Elsevier

[21] Lai, M-C, Lin, H.T. and Wu-Der, T.: The Evaluation of Intellectual Capital in a Taiwan Hospital, Proceedings of the Second International Conference on Innovative Computing, Informatio and Control, Page 385, 2007, IEEE

and the historical report on intellectual capital management/reporting from Scandia can be found in[22] – providing insights on development and valuing of the company's own IC.

*2.2 Required Adaptations of existing approaches*

The first challenge of measuring intellectual capital is to identify knowledge in such a form that it can be assessed. As the authors follow the slogan of Karagiannis "knowledge is humanised information" the knowledge needs to be specified in an explicit form. The concept of the "knowledge product"[23] has been introduced that defines the knowledge in a consumable way. The PROMOTE® approach identifies three types of knowledge products: (a) service: implicit knowledge is provided for implicit usage like an expert, trainer or the like, (b) information product: explicit knowledge is provided for implicit usage like books, magazines, and other forms of publications as well as (c) application: explicit knowledge is provided for explicit usage like expert systems, glossaries and the like.

The definition of the "knowledge product" and the identification of services, information products and applications enables to specify the knowledge of the organisation, and hence the intellectual capital in a consumable way. The assumption is that only the consumable and hence applicable knowledge is of interest, therefore the knowledge products have been identified to be the central point of intellectual capital management approach.

The concept of the Balanced Scorecard[24] provides a balanced and flexible steering approach. The second challenge was to measure the intellectual capital using this scorecard approach with the focus on knowledge products.

---

[22] Edvinsson, L.: Developing Intellectual Capital at Skandia, Long Range Planning, Vol. 30, No. 3, pp. 366 to 373, 1997, Elsevier

[23] Mak K.; Woitsch R.: Der Einsatz des prozessorientierten Wissensmanagementwerkzeuges PROMOTE® in der Zentraldokumentation der Landesverteidigungsakademie : Entwicklungslinien der ZentDok und die Implementierung von PROMOTE®. – Wien

[24] Kaplan R., Norton D:The Balanced Scorecard: Translating Strategy Into Action. Harvard Business Press, 1996

Therefore the structure of the knowledge scorecard is defined as follows

- Product Perspective: Goals, indicators and measures for the actual knowledge products provided by the organization
- Processes and Structure Perspective: Goals, indicators and measures in relation to processes executed (core processes, supporting processes and management processes) to create the knowledge products.
- Human Capital, Relations and Competences Perspective: Goals, indicators and measures of human capital and competences required to create the knowledge products.
- Resources and Support Perspective: Goals, indicators and measures of budget, infrastructure, material and tools (incl. structural capital) as well as information access that is seen as the basic resources.

These perspectives have been derived by analysing available measurement criteria and validating them against literature in the domain[25]. These perspectives have been evaluated according to their applicability in a series of workshops and internal reviews. The third challenge was to extend the aforementioned horizontal views with vertical pillars to provide architecture for realising a knowledge scorecard.

[25] Heisig Peter, Wissensbilanz – Made in Europe. In: Wissensmanagement – Das Magazin für Führungskräfte, Heft 4/2008

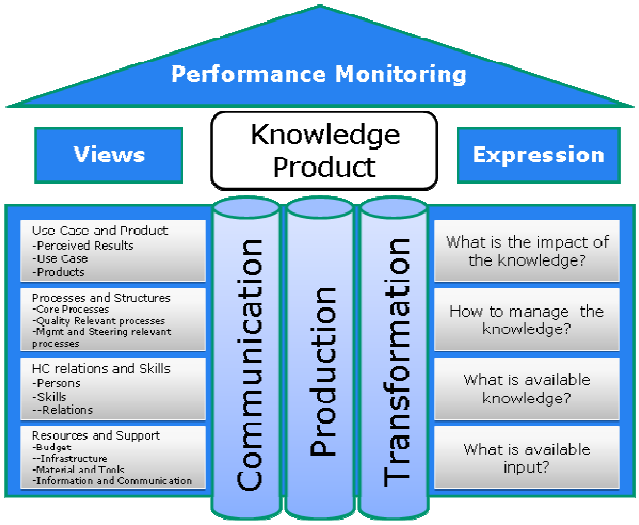



**Figure 1 PROMOTE® Knowledge Scorecard Architecture**

Figure 1 depicts the developed architecture for the Knowledge Scorecard[26]. Starting point is the knowledge product that needs to be produced, disseminated and continuously improved through transformation. These three pillars are analysed according their impact, their management processes, the available vs. required skills and the available vs. required input. This matrix has been used as a guideline to identify the critical success factors, the knowledge goals and measurement criteria.

## 3 The Show Case: Knowledge Scorecards at the Austrian National Defence Academy

In the following the best practice project for knowledge scorecards based upon the PROMOTE® approach is described giving insights in the project results and implementation steps.

### *3.1 Definition of the Initial Situation.*

The knowledge product model has been structured according three main

[26] Göllner, J., Mak, K., Trattnig, G., Woitsch, R., „Wissensmanagement und Wissensbilanz im ÖBH am Beispiel der ABCAbwS & ABCAbw“, Wien, 2008,

categories: *Research-, Training- and Force Provision Products*. *Research Products* establish the grounding of knowledge related work (e.g. scientific publications in different domains, maintenance of e-Learning, etc.). *Training Products* are the main area within the organization comprising all courses and training products necessary to maintain a long-term availability of forces. *Force Provision Products* are products that are provided when military actions take place. Competences have been mapped by relating the provided knowledge products to the organizational models. By adding identified competences necessary for the provision of products by the organizational unit the analysis concluded with a competence matrix. There are about 950 competences identified, whereas between ten and twenty of these competences are annotated in average to one working place. That approach enabled the identification of competences per workplace, the availability of competences within the organisation and enabled a direct relation of provided knowledge products and the according required and available competence.

### *3.2 Specification of Critical Success Factors*

This step was the most time consuming and most difficult task it aimed to identify the critical success factors and externalise relevant knowledge on steering the school from the management team using the aforementioned architecture of the Knowledge Scorecard. Existing management instruments (Process Management, Balance Scorecard, Quality Management in accordance with ISO9001:2005, CAF[27], Continuous Improvement, Cost accounting) have been investigated.

### *3.3 Definition of Goals and their Cause and Effect Relations*

Based upon the critical success factors identified in the previous phase, the goals have been grouped according to a set of similar success factors. Cause and effect relations between goals have been identified and enhanced by measurable criteria. The cause-and-effect diagram as depicted in Figure 2 has been defined in multiple discussion rounds condensing the initial goal

[27] Common Assessment Framework, http://www.eipa.eu/en/pages/show/&tid=67, access 25.10.2008

definition to a final set of concrete goals.
The image shows the four perspectives marked with A, B, C and D as well as indicates the three pillars marked with 1, 2 and 3.

### *3.4 Quantification of Goals*

The identified goals had been detailed described by measurable criteria. A set of indicators were identified that are already subject to operational data available in different systems such as HR management tools, financial controlling systems, etc. In addition to those indicators, criteria have been identified where operational data sources are not yet available and need further investigation. These elements have been highlighted within the model and are out-of-scope for the implementation of the knowledge scorecard at this stage. For the operational indicators a detailed specification has been derived giving all necessary information for the reporting and monitoring system.

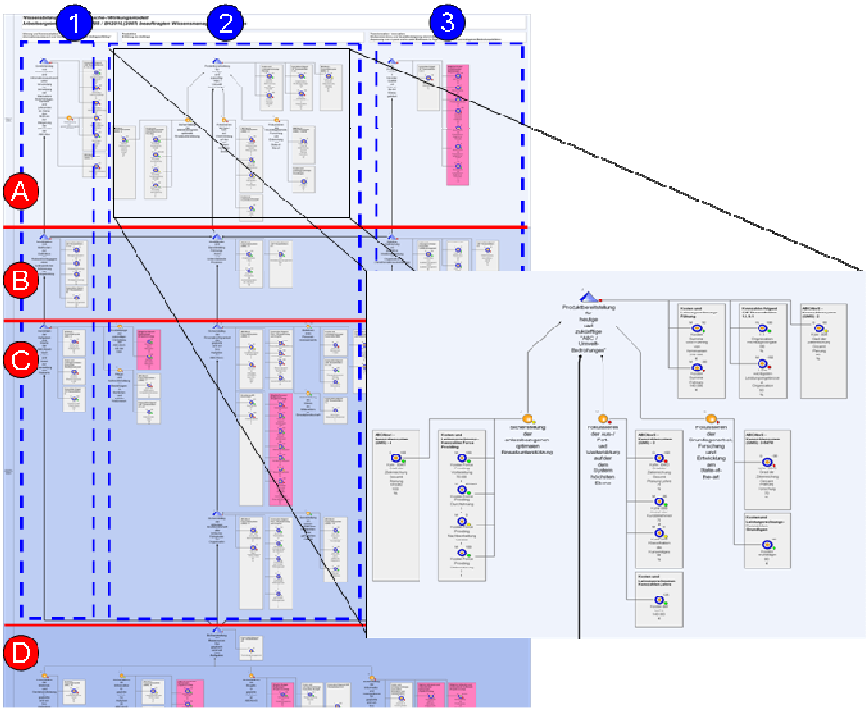



**Figure 2 Cause-And-Effect Diagram**

The detailed view of Figure 2 indicates the knowledge goal "Provision of knowledge products for current and future ABC issues" as the blue pyramid. Below there are three sub-goals represented as orange circles for the research, training and force provision. Each of the goals is measured by criteria represented as blue targets that range from concrete financial criteria like "Costs for Research" to fuzzy criteria like "Estimated degree of knowledge goal achievement".

### *3.5 Operational Data Coupling*

The next phase considers the operationalisation of the knowledge scorecard through the coupling of the designed models with operational datasources. For concrete criteria the operational data sources are typically data warehouse applications, databases in general or spreadsheets that are updated on a regular basis. For fuzzy criteria there is a range of instruments like self-assessments, management assessment, client assessment, questionnaires or the like that provide representative values. The calculation capabilities within the modelling tool allow the definition of complex indicator structures and combine indicators to be used.

### *3.6 Steering and Management based on Knowledge Scorecard*

As a reporting and performance monitoring tool, the controlling cockpit has been used to visualize the results of the knowledge scorecard to the targeted audience and provide interactive analysis and reporting functions. The reports generated by the knowledge scorecard provide the decision makers with the necessary information.

## 4 Conclusion

The implementation of the knowledge scorecard at the ABCAbwS resulted in a comprehensive instrument for steering the service provision processes within the organization and built up a transparent framework for evaluation of knowledge assets. The implementation is regarded as a best practice application within the LVAk that proves that evaluation of knowledge assets and continuous monitoring could improve the reaction capabilities and learning structures of Austrian Armed Forces, leading to an increased readiness for duty in the case of military actions.

## 5 Acknowledgement

We would like to thank Bgdr. Loidolt, and o. Univ Prof. Karagiannis for supporting the project as well as Bgdr Fürstenhofer, Kdt ABCAbwS, for the possibility to execute the project and the quality feedback.

## References

- Aidemark, J. and Sterner, H.: A Framework for Strategic Balancing of Knowledge Management Initiatives, IEEE, Proceedings of the 36th Hawaii International Conference on System Sciences, 2003
- Andriessen, D. 2004: Making Sense of Intellectual Capital, Elsevier Butterworth Heinemann, Oxford.
- Bukh, P.N., Larsen H.T. and Mouritsen, J.: Constructing intellectual capital statements, Scandinavian Journal of Management, 17 (2001) 87-108, Elsevier
- Chen, Y-S.: The Positive Effect of Green Intellectual Capital on Competitive Advantages of Firms, Journal of Business Ethics (2008) 77:271–286, Springer
- Common Assessment Framework, http://www.eipa.eu/en/pages/show/&tid=67, access 25.10.2008
- Edvinsson, L.: Developing Intellectual Capital at Skandia, Long Range Planning, Vol. 30, No. 3, pp. 366 to 373, 1997, Elsevier
- Fairchild, A.M.: Knowledge Management Metrics via a Balanced Scorecard Methodology, Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 8 - Volume 8, Page: 243, IEEE
- García-Meca, E. and Martinez, I.: The use of intellectual capital information in investment decisions - An empirical study using analyst reports, The International Journal of Accounting 42 (2007) 57–81, Elsevier
- Göllner, J., Mak, K., Trattnig, G., Woitsch, R., „Wissensmanagement und Wissensbilanz im ÖBH am Beispiel der ABCAbwS & ABCAbw“, Wien, 2008,
- Heisig Peter, Wissensbilanz – Made in Europe. In: Wissensmanagement – Das Magazin für Führungskräfte, Heft 4/2008

- Johannesse, J-A., Olsen, B. and Olaisen, J.: Intellectual capital as a holistic management philosophy: a theoretical perspective, International Journal of Information Management 25 (2005) 151–171, Elsevier
- Mak K.; Woitsch R.: Der Einsatz des prozessorientierten Wissensmanagementwerkzeuges PROMOTE® in der Zentraldokumentation der Landesverteidigungsakademie : Entwicklungslinien der ZentDok und die Implementierung von PROMOTE®. – Wien
- Lai, M-C, Lin, H.T. and Wu-Der, T.: The Evaluation of Intellectual Capital in a Taiwan Hospital, Proceedings of the Second International Conference on Innovative Computing, Informatio and Control, Page 385, 2007, IEEE
- Lev, B. 2004. Sharpening the Intangibles Edge.Harvard Business Review, vol. 2004, no. June, pp. 109-116.
- Nemec Rudez, H and Mihalic, T.: Intellectual capital in the hotel industry: A case study from Slovenia, Internationa Journal of Hospitality Management 26 (2007) 188–199, Elsevier
- North, K. 1998: Wissensorientierte Unternehmensführung, , Gabler Verlag, Wiesbaden.
- Kaplan R., Norton D:The Balanced Scorecard: Translating Strategy Into Action. Harvard Business Press, 1996.
- Woitsch R, Karagiannis D.: Process Oriented Knowledge Management: A Service Based Approach. J. UCS 11(4): 565-588 (2005)
- Stewart, T.A. 1997: Intellectual Capital, Nicholas Brealey Publishing, London.
- Striukova, L., Unerman, J. and Guthrie, J.: Corporate reporting of intellectual capital: Evidence from UK companies, The British Accounting Review, (2008) 1-17, Elsevier
- Sveiby, K.E. 1997: The New Organizational Wealth, Berrett-Koehler Publishers, San Francisco.
- Tai, W-S. and Chen C-T.: An Intellectual Capital Performance Evaluation Based on Fuzzy Linguistic, Proceedings of the Third International Conference on International Information Hiding and Multimedia Signal Processing (IIH-MSP 2007) - Volume 02, IEEE
- Universitätsgesetz 2002 Online at: http://archiv.bmbwk.gv.at/universitaeten/recht/gesetze/ug02/Un

iversitaetsgesetz_20027727.xml
- Vuontisjarvi, T.: Corporate Social Reporting in the European Context and Human Resource Disclosures: An Analysis of Finnish Companies, Journal of Business Ethics (2006) 69:331–354, Springer
- Wilkins, J., van Wegen, B. and de Hoog, R.: Understanding and Valuing Knowledge Assets: Overview and Method, Expert Systems With Applications, Vol. 13, No. 1, pp. 55-72, 1997, Elsevier

**Authors**

**Johannes Göllner, Klaus Mak**
Landesverteidigungsakademie, Zentraldokumentation (ZDok),
Stiftgasse 2a,1070 Vienna, Austria
{klaus.mak, mba.ukm}@bmlv.gv.at

**Robert Woitsch**
BOC Asset Management GmbH,
Bäckerstraße 5,
1010 Vienna, Austria
{robert.woitsch}@boc-eu.com

# NATO-RTA 2011

## NATO-RTA 2011

*Understanding the Human Genome: A Conceptual Modeling-Based Approach*
NATO, Research and Technology Organisation
Oslo, Norway on 7-8 November 2011

Information superiority is one of the primary issues for military dominance. To achieve situational awareness in a joint/combined coalition, the meaning of the exchanged information and the purpose of the information exchange must be understood identically everywhere and at all times. Recent research and development trends suggest that NATO Network Enabled Capability (NNEC) will provide a means for establishing the desired information superiority. The NNEC builds on the idea of a common information space where all participating elements and organizations have the opportunity to supply and retrieve information according to their particular roles in the operation. Information must be conveyed in a secure and trusted way. This includes the idea that the meaning of the information and the purpose of the information exchange are understood identically everywhere and at all times. This level of understanding between all elements participating in joint/combined operations requires a broad attention to the context of information and the concepts contained within the information. True understanding of the concepts within the information can be equated to understanding the semantics of the information. Several major attempts in the area of syntactic/semantic interoperability were undertaken that can be comprised into two major tracks: one track focuses on knowledge-based means that analyze and convert information by using ontologies. Relevant projects were conducted by e.g. IST-094 "Framework for Semantic Interoperability" and NC3A's "SI Factory". For the second track, concentrating on the modeling aspects of information domains, relevant representatives are "Multilateral Interoperability Programme" and IST-084 "Domain-based Intereroperability". Of course there are more approaches that aim on interoperability between heterogeneous organizations. They mostly concentrate on non-technical criteria like for instance social, cultural interoperability or ergonomics.

http://www.cso.nato.int/

The original version of this material was published by the Research and

Technology Organization, North Atlantic Treaty Organization (RTO/NATO) in Meeting Proceedings RTO-MPIST-101" Semantic and Domain-based Interoperability" in November 2011.

# The Austrian Armed Forces (AAF) Knowledge Performance System (KPS) – An Enabler for Interoperability?

*Klaus Mak, Johannes Göllner, Robert Woitsch*

(Designed, Developed and Tested by CentDoc/NDA and BOC)

**Abstract:** The paper at hand discusses the applicability of the Knowledge Performance System (KPS) of the Austrian Armed Forces. The Knowledge Product Model is seen as the enabling concept for interoperability of knowledge-driven organisations and has been developed in a series of Knowledge Management Projects for the AAF at the Austrian Defence Academy.

**Keywords:** Knowledge Performance System, Knowledge Management (KM), Knowledge Modelling, Model Based KM, Process Oriented KM, Knowledge Product, Organisational Capability Development, Measurement, Aspects of Interoperability.

## 1.0 Introduction

In today's information and knowledge driven society existing knowledge within organisations is the decisive resource applied in the service delivery process.

The challenges in military organisations are more comprehensive. They have to execute national and international military and CIMIC joint operations combined with an adapted education and training system. Also the research and development programme has to be matched with the planning and lessons learned section of the MoD and JOC of the AAF. This complex transformation scenario has to be supported by an optimized logistic system and business organisation. Therefore interoperability has to be assured at all levels.

Knowledge in all available forms as the basic resource for decision instances has to be managed in optimised form. The "Learning Organisation" has

to be managed and evaluated in real time. While highly structured processes have been automated by applying business process management principles to allow concrete measurement in order to raise efficiency and effectiveness, weakly structured processes are different.

"**Knowledge Products**" are defined as consumable knowledge. This point of view focuses all KM-activities on accessible and applicable knowledge. Hence those products are the output of process-oriented knowledge work – including all forms of production processes. Applying the well known principles of production to knowledge enables the application of similar methodologies, instruments and tools.

The Knowledge Performance System Methodology has been used as a roadmap-model for defining knowledge products, knowledge resources and knowledge processes that are used within reporting mechanisms applying a model-driven mechanism in the implementation process and in relation to the different aspects of interoperability in a military and organisational context.

The approach mentioned above was applied in a series of KM-projects within the Austrian NBC Defence School, an organisation heavily dependent on the knowledge and expertise of its employees in order to maintain the necessary level of security and sustainability in critical domains available at any point in time.

## 2.0 Challenges of KM in the Austrian Armed Forces (AAF)

All specifications of KM tasks in the AAF are defined in the "Military Strategic Concept" and organisational guidelines. The guidelines for the detailed specifications are determined in a cross-section operational concept: "KM in the AAF". Three main challenges are focused in our work and preceded to be solved.

Following these challenges, we focused on answering those questions and solving the problems with a new holistic approach of KM.

*2.1 Support for Capability Development*

Capability is the entirety of a system that delivers an output or effect. It will most likely be a complex combination of:

- Doctrine,
- Organisation,
- Training,
- Material,
- Leadership,
- Personnel,
- Facilities.

Our questions regarding "Product View":

Is it possible to define the capabilities which are the entirety of output or effect as a product/knowledge product?

Is it possible to define a military operation as a product/knowledge product?

*2.2 Enabler for Interoperability*

All levels of interoperability have to be supported by KM:

- Political
- Legal
- Organisational
- Semantically
- Technical

Our Business Process Model related questions:

Is a "Business Process & Model Based KM" – approach appropriate to support analysing, planning, documenting, managing and evaluating of military planning and operational tasks?

Which are suitable tools and methods to support the solution of interoper-

ability problems?

*2.3 Improvement of the Evaluation Quality*

A business process management approach with "Specification of Goals" in the fields of:

- Resources – "What is available input?"
- Human Capital – "What is available knowledge?"
- Processes – "How to manage the knowledge?"
- Use Cases – "What is the impact of knowledge?"

("Four Perspectives of a Scorecard")

combined with KM.

Our questions regarding Managing and Evaluating knowledge:

Is the "Balanced Scorecard Technique" a practicable approach to create a "Knowledge Scorecard"?

What is the available knowledge input (Resources)? What is the available personalized knowledge (Human Capital)? Do we know how to manage the knowledge (Processes)? What is the impact of knowledge (Use Cases)?

Is our generic "Roadmap" executable in the CBRN Use Case?

**3.0 Common Denominator for Challenge 1, 2 & 3**

The "Knowledge Product" ("If you can't measure it – you can't manage it!") and the "Four Perspectives of the Scorecard" represent in combination the "Architecture of the Knowledge Performance System (KPS)". This architecture with its "12 dimensions" represents a "Meta Layer" for:

- Analysing,
- Planning,
- Modelling,
- Documenting,

- Managing,
- Evaluating

a system, an organisation or an operation.

Our answer:
The "Architecture of the KPS": suitable as a "Meta Layer" (Fig.4) for a combined organisational and knowledge-related view.

## 4.0 Conceptual Background

### *4.1 Related Work*

Monitoring the KM initiatives and application scenarios within a company or military organisation is not something unusual, representing just a current hype.

Over the years different approaches have been implemented in order to provide an instrument for military capability development and evaluation as well as for defining the interfaces of system elements and system components for an organisational interoperability concept based on a holistic management philosophy.

### *4.2 Knowledge Performance System (KPS): Architecture and Design*

After the definition of the knowledge management strategy, the KPS has been designed. For a transparent, quality and process orientated transformation and implementation of KM, model orientated concepts have been successful or in advantage.

This section presents the modelling of KM and offers a reference model, which is based on the business-process-oriented knowledge management approach. It gives a clue about the intentional goals, the definition and classification of business processes, the evaluation of results, as well as their interpretation for setting new goals.

One of the tasks of any KM is the direct or indirect support of business

processes. In order to obtain a clearly defined and practical tool for linking business processes and knowledge management, we introduce the concept of a "K**nowledge Product**".
Knowledge products are the results of KM used in business processes. The presented reference model (Fig.1) explains how such knowledge products are created. „**Knowledge Product – the anchor-point of business process orientated KM.**"

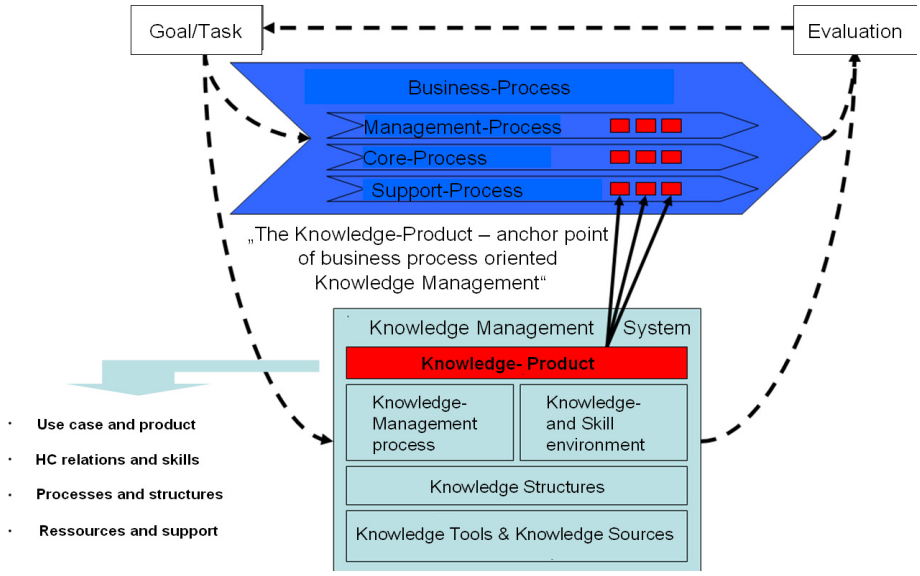



**Figure 1: „Knowledge Product"**

*4.3 The Methodology to Develop a KPS*

The 5 phases in the procedure model are identified as follows:

Phase 1: Goal Definition: The overall goal of the KM project is defined using application scenarios. The KPS supports a set of application scenarios like Process-Oriented KM, KM Process Optimization, Skill Management and Knowledge Monitoring and Reporting. This phase represents all system definitions and descriptions. **Goal definitions are directly linked to political interoperability as well as aspects of legal and cultural interoperability.**

Phase 2: KM introduction steps: After defining the goal of the KM project, the second phase is concerned with the actual KM introduction steps. The scenario selected is in details described by an analysis of input/output relations and related knowledge management processes. **This phase includes all knowledge processes and is therefore directly connected to organisational interoperability.**

Phase 3: Knowledge Operationalisation: The results of the KM are formalized regarding operational and execution systems. Models are further enhanced by adding knowledge resources and tools to the overall knowledge landscape. **This phase includes semantic, syntactic and technical interoperability.**

Phase 4: Knowledge Execution: For the actual application of the KM system in real-work context, i.e. employees accessing the system and fulfilling day-to-day operations accordingly.

Phase 5: Knowledge Evaluation: In the feedback loop of the provided KM system its effectiveness is evaluated in order to influence the definition phases for continuous improvement representing a dynamic procedure in transforming and adapting interoperability.

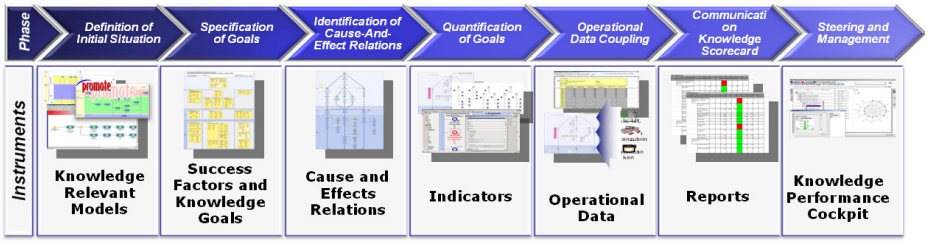



**Figure 2: "Roadmap to Performance Monitoring".**

**During these steps of analysing and modelling the system all questions of interoperability have to be discussed and established. Therefore a firm basis for practical solutions is provided!**

*4.4 Knowledge Performance Systems (KPS) for Units of the Austrian Armed Forces*

The intellectual capital management scenario uses mechanisms and con-

structs of controlling frameworks and establishes these frameworks in the domain of knowledge management. Consequently the PROMOTE® approach of our partner BOC is regarded as the basis for building up knowledge scorecards.

The original concept of Balance Scorecards (Kaplan and Norton) sets up 4 generic perspectives (financial, customer, business process and learning/growth perspective) and sets those in context with each other using cause and effect relations targeting comprehensive controlling and monitoring objectives within an organisation.

The knowledge scorecards use the same principles, but focus on knowledge management aspects. Therefore the structure of the PROMOTE® based knowledge scorecard is defined as follows:

- Product Perspective: Goals, indicators and measures for the actual product provided by the organisation

- Processes and Structure Perspective: Goals, indicators and measures in relation to processes executed (core processes, quality-relevant processes, management processes, etc.)

- Human Capital, Relations and Competences Perspective: Goals, indicators and measures of human capital and competences

- Resources and Support Perspective: Goals, indicators and measures of budget, infrastructure, material and tools (structural capital)

These perspectives have been derived within the best practice project and validated against literature in the domain resulting in a reference architecture for knowledge scorecards on a generic level.

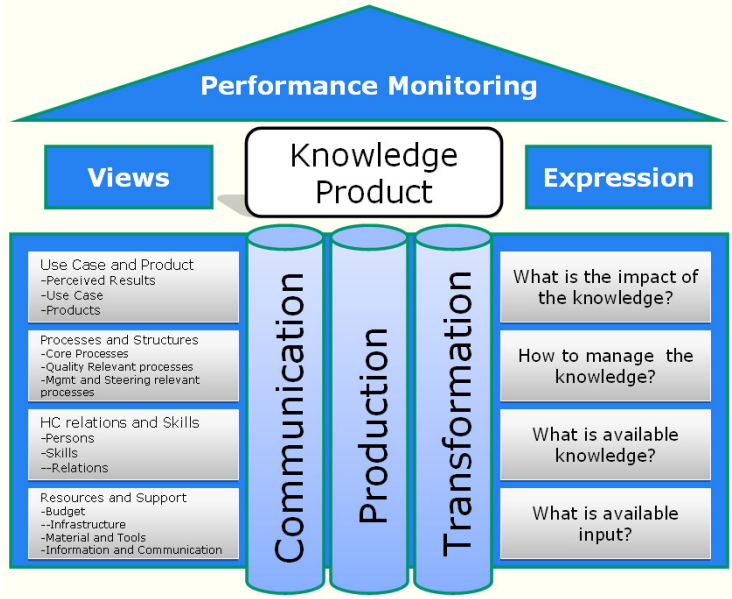



**Figure 3 Architecture of the KPS**

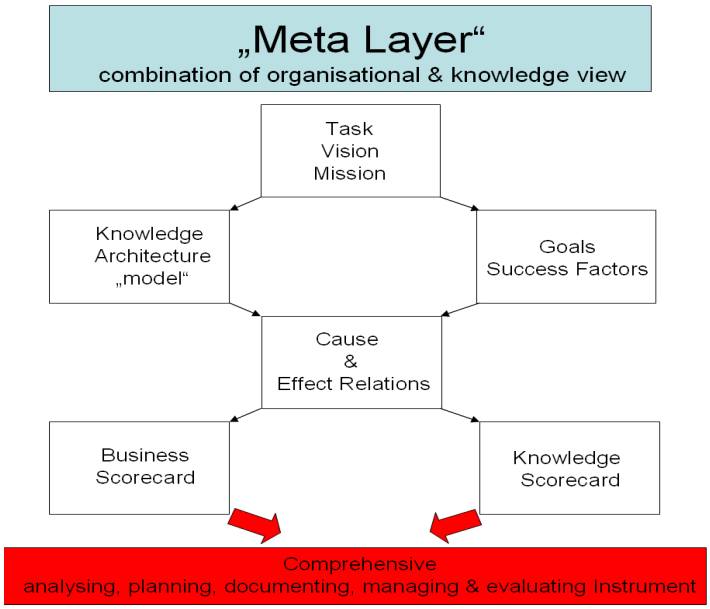



**Figure 4 Meta Layer**

## 5.0 Use Case KM Project: Knowledge Performance System at the Austrian NBC Defence School

In the following the best practice project for a KPS based on the PROMOTE® approach is described in detail delivering insights into the project results and the steps performed. The section describes the problem statement and motivation for the best practice project, presents project results based upon the conceptual description above and concludes with lessons learned from the perspective of the project partners.

- Action tasks: Force Providing / NBC Company
- Training & Education
- Research & Development

The best practice project has been executed according to the roadmap for implementing the knowledge scorecards based upon the PROMOTE® approach. The results derived and accomplished in step 1 are described below.

### *5.1 Influence Factors for the Organisation*

In this step the Scenario with the influence factors for the organisation has to be defined. In our use-case external factors and internal preconditions have to be defined in three assignments:

- For the CBRN-mission-portfolio,
- For the CBRN-training-portfolio and
- For the CBRN-R&D-field.

All questions of political interoperability with clear political objectives and legal necessities have to find its expression in clear mission assignments.

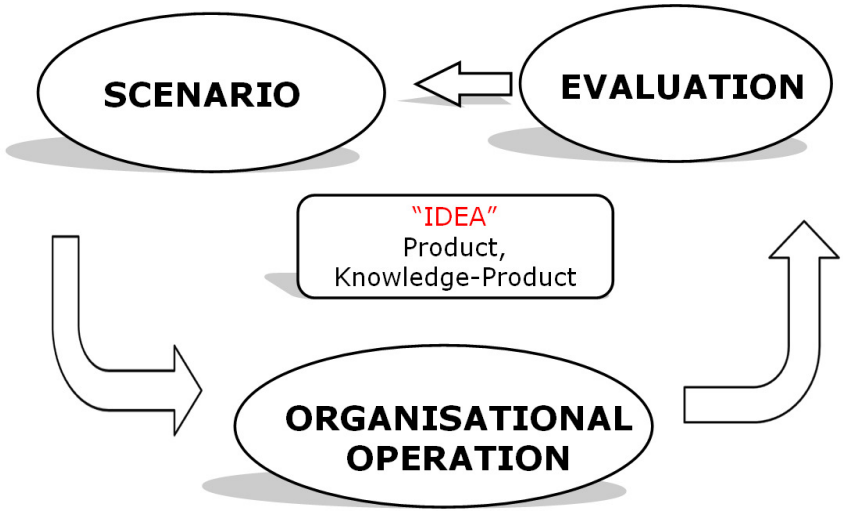



**Figure 5 KM System Paradigma**

These planning guidelines are the preconditions for the operating organisation, within all business perspectives:

- Product Catalogue for Mission, Training and R&D
- Processes and Structures
- Environment, Employees (HR- Resources),
- Capability Catalogue and Resources

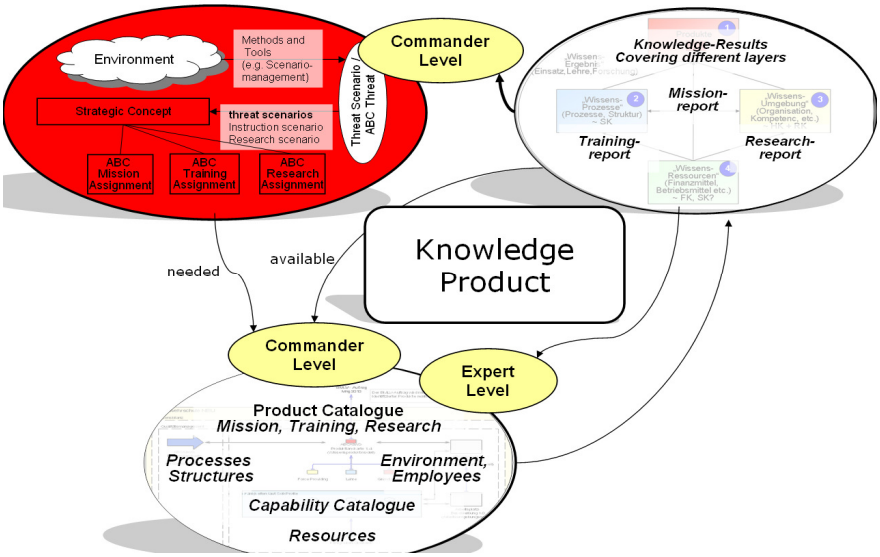



**Figure 6 NBC-KM-System-Overview**

### *5.2 Model of the NBC Defence School*

Supported with PROMOTE a Knowledge Map of the organisation is produced. All relevant modules describe the organisation, the input and output factors and the interfaces. Skills and capabilities combined with the task are documented.

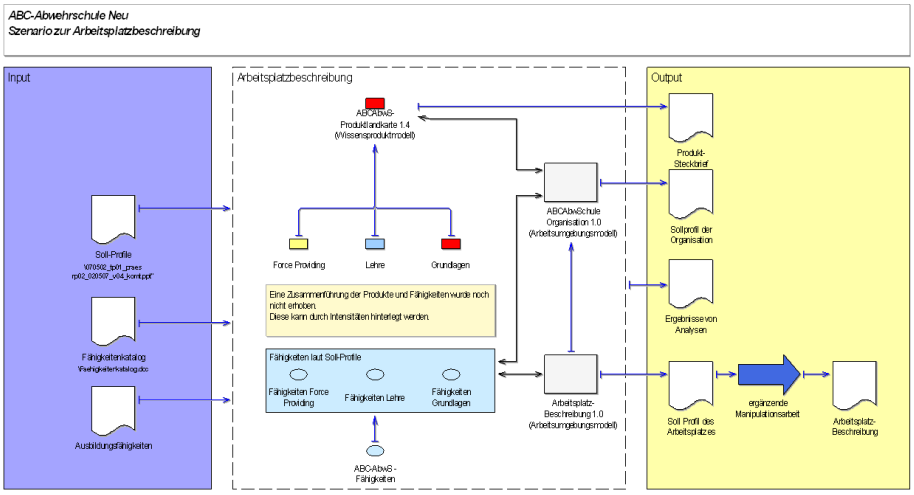



**Figure 7 Knowledge Landscape as Orientation**

The knowledge product model at the NBC Defence School has been structured according to the application area of the products.

Three main categories have been identified: R&D, Training and Force Providing Products. R&D establishes the grounding of knowledge related work (e.g. scientific publications in different domains, maintenance of e-Learning, etc.). Training Products are the main area within the organisation comprising all necessary courses and training products maintaining a long-term availability of forces. Force Providing Products are products that are provided when military actions take place and expert knowledge is required within the organisation.

Each of the boxes in the model represents a concrete Knowledge Product that can be consumed by any requesting organisational unit.

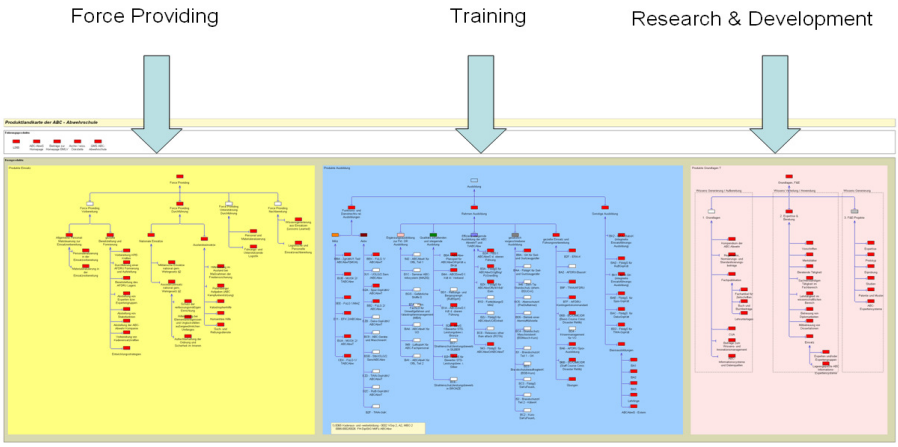



**Figure 8 Knowledge Product Model**

In a next step within this phase competences have been mapped by relating the provided knowledge products to the available organisational models. By adding identified competences, necessary for the provision of products by the organisational unit, the analysis is concluded with a competence matrix.

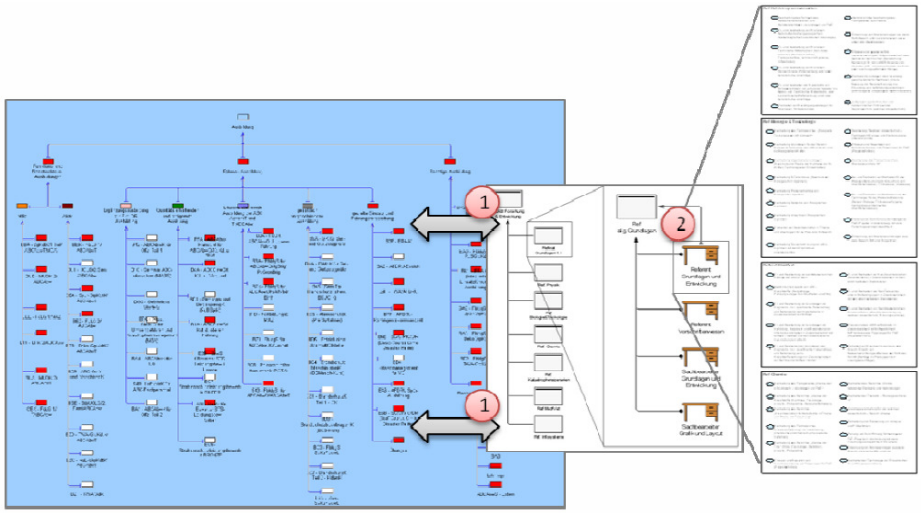



**Figure 9 Workplace skills required by Knowledge Products**

The "Task-based view" on a "Skill-house" is the interactive capability model of the NBC Defence School.

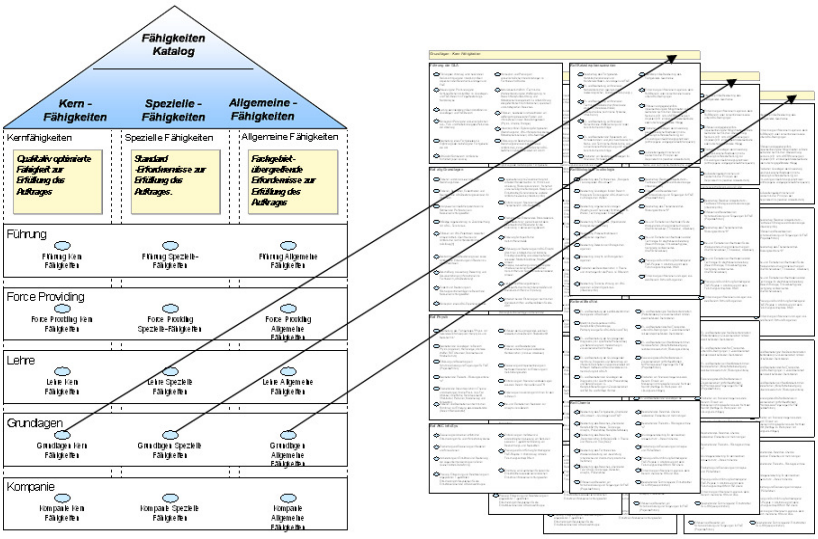



**Figure 10 Organsational Unit related Skills**

The steps of "Specification of Goals", "Identification of Cause-And-Effect-Relations", "Quantification of Goals", "Operational Data Coupling", "Communication Knowledge Scorecard" and "Steering and Management" are realised:

**Specification of Goals**. The step is focused on deriving the target user group and the expected results for a knowledge scorecard system (internal vs. external communication, updating mechanisms). Existing management instruments (Process Management, Balance Scorecard, Quality Management in accordance with ISO9001:2005 [29], CAF [30], Continuous Improvement, Cost accounting) have been investigated and integrated in the knowledge scorecard approach accordingly to enable a comprehensive monitoring and management approach.

**Definition/Identification of Cause-And-Effect Relations**. Based upon the goals identified in the previous phase, cause and effect relations between goals have been identified and enhanced by measurable criteria. The cause-and-effect diagram as depicted in Figure 11 has been defined in multiple discussion rounds condensing the initial goal definition to a final set of concrete goals.

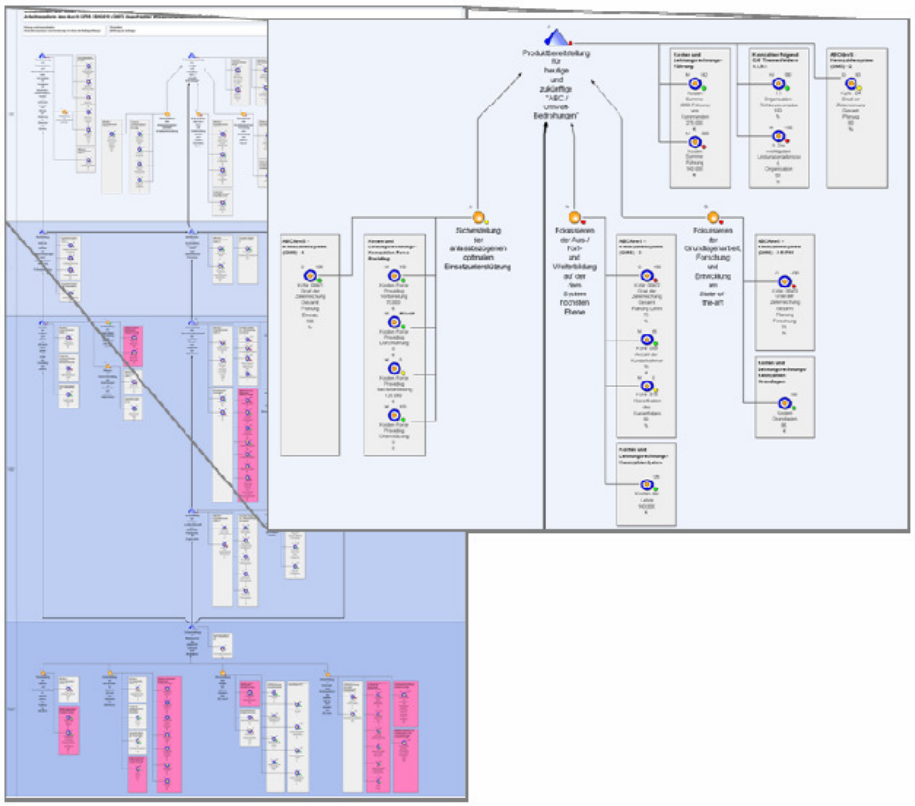


**Figure 11 Cause-and-Effect Diagram**

**Quantification of Goals**. During the analysis process and discussions various indicators were identified, subject to operational data available in different systems such as Human Resource Management tools, financial controlling systems, etc. Additionally to those indicators, criteria for operational data sources, which are not yet available and need further investigation, were identified. These elements have been highlighted within the model and are out-of-scope for the implementation of the knowledge scorecard at this stage. For the operational indicators a detailed specification has been derived giving all necessary information for the reporting and monitoring system.

**Operational Data Coupling**. The next phase considers the operationalisation of the knowledge scorecard through the coupling of the designed

models with operational data-sources. Operational data sources used as input are typically data warehouse applications, databases in general or spreadsheets that are updated on a regular basis. The calculation capabilities within the modelling tool allow the definition of complex indicator structures and combines indicators to be used.

**Communication of the Knowledge Scorecard and Steering and Management based on Knowledge Scorecard.** As a reporting and performance monitoring tool, the controlling cockpit has been used to visualize the results of the knowledge scorecard to the targeted audience and provide interactive analysis and reporting functions. Figure 12 shows the resulting performance cockpit listing traffic light coded goals and indicators for status evaluation as well as traditional analysis functions such as spider diagram to set indicators and goals in context to each other.

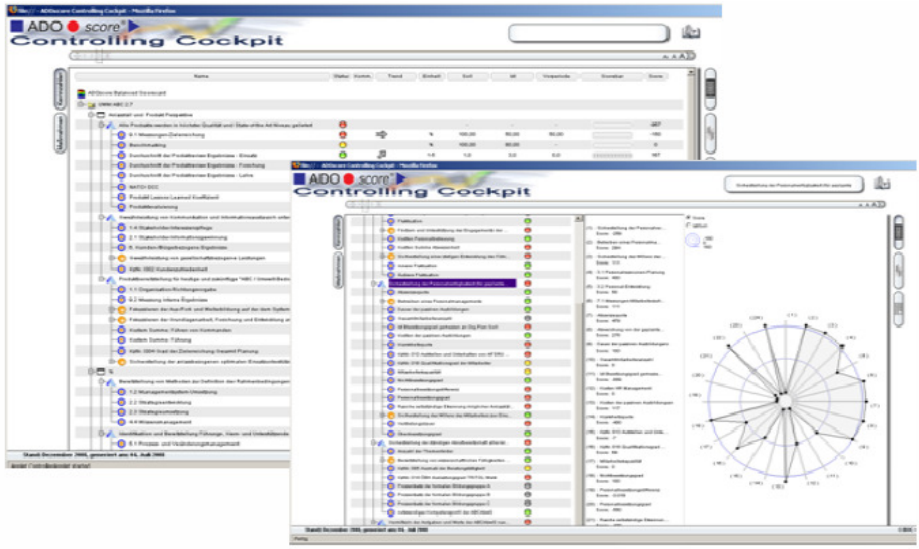



**Figure 12 Adoscore Cockpit**

The reports generated by the knowledge scorecard provide the decision makers within the NBC-Defence-School with the necessary instrument to have an overview on the overall performance of the organisation and the current knowledge base to reach the defined goals.

As a result the operating "KPS" is formalized in the next model: The "Simulation Model".

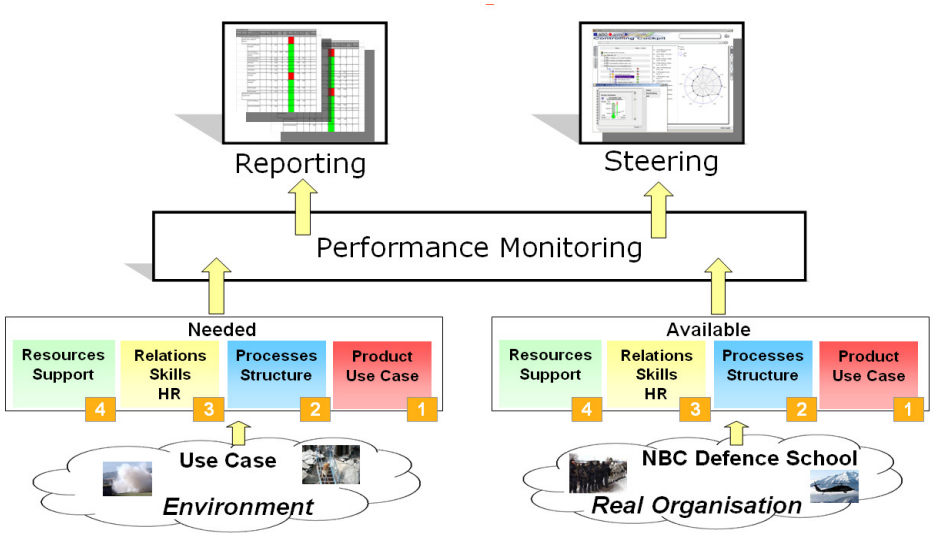



**Figure 13 KPS Simulation Model**

Fig.13 Introduces the Simulation Model by applying the same Roadmap and Models not only for the existing and hence available NBC Defence School but – based on simulated possible events – also for the four main organisational components.

## 6.0 Conclusion

The implementation of the KPS at the NBC Defence School resulted in a comprehensive instrument for steering the service provision processes within the organisation and built up a transparent framework for assembling and evaluating knowledge assets.

Regarding support of capability development it has been proven that a product oriented view on knowledge is not only possible but exceedingly feasible as knowledge becomes identifiable, documentable and hence manage- and measureable.

Regarding enabler for interoperability using business process- and KM

models it has been proven that the use of "Construction Plans" for KPS enables the in-depth analysis of organisational, technical as well as domain specific interfaces.

Regarding improvement of evaluation quality applying balanced scorecard principles has been proven to establish a holistic management and measurement framework for steering the existing organisational unit and for simulating possible future demanded resource.

The implementation is regarded as a show case application within the Austrian NBC Defence School that proves that evaluation of knowledge assets and continuous monitoring could improve the reaction capabilities and learning structures of the Austrian Armed Forces, leading to an increased readiness for duty in the case of military operations.

**Authors**

**Klaus MAK, Johannes GÖLLNER**
c/o National Defence Academy of the Austrian MoD
Central Documentation & Information Service (CentDoc)
Stiftgasse 2a
1070 Vienna
AUSTRIA
lvak.zentdok.wm@bmlvs.gv.at
klaus.mak@bmlvs.gv.at
johannes.goellner@bmlvs.gv.at

**Robert WOITSCH**
c/o BOC Asset Management GmbH
Bäckerstrasse 5
1010 Vienna
AUSTRIA
robert.woitsch@boc-eu.com

## Herausgeber

**Dipl.-Ing. Johannes Göllner, MSc,**
Leiter Hauptreferat Wissensmanagement/Zentraldokumentation

Dipl.-Ing. Göllner ist Leiter des Hauptreferates Wissensmanagement in der Zentral-dokumentation der Landesverteidigungsakademie. Er ist Experte für Risiko-, Krisen-, Katastrophen-, Wissensmanagement und Szenarien-Development, strategische und operative Organisationsentwicklung und –steuerung sowie Lektor für Risiko-, Krisen-, Wissensmanagement und Szenarien-Entwicklung an der Landesverteidigungsakademie Wien des ÖBH, der Universität für Bodenkultur Wien, der Universität Wien und Donau Universität Krems, und war und ist Projektleiter oder -mitarbeiter in zahlreichen BMLVS-internen und externen, nationalen und EU- Forschungsprojekten, unter anderem Szenarioplanung & WM, KIRAS MDL, KIRAS QuOIMA, KIRAS (SG²), KIRAS Cloud Sicherheit, KIRAS RSB und FOCUSPROJECT.

**Ing. Mag. Klaus Mak, ObstdhmfD,**
Ltr ZentDok, EU-zertifizierter Informationsexperte

Klaus Mak ist Berufsoffizier und seit 1993 Leiter der Zentraldokumentation an der Landesverteidigungsakademie in Wien und wurde im Rahmen des EU-Projekts »Certidoc« als »Informationsexperte« zertifiziert. Er führt Lehr- und Vortragstätigkeit sowie Beratungs- und Evaluierungsprojekte an verschiedensten in- und ausländischen Bildungseinrichtungen für Informationsberufe und Wissensmanagement durch und ist verantwortlich für Konzeptentwicklung und Projektsteuerung und -durchführung von Wissensmanagementprojekten im Rahmen der Forschung und Entwicklung im BMLVS.

**Dipl.-Ing. Christian Meurers,**
Referent Multimediadokumentation und Situation Awareness Center, Hauptreferat Wissensmanagement/Zentraldokumentation

Dipl.-Ing. Meurers ist verantwortlich für die Multimediadokumentation und die Betreuung des Situation Awareness Centers an der Zentraldoku-

mentation der Landesverteidigungakademie. Er ist Absolvent des Studiums der Informatik an der TU Wien und beschäftigt sich darüber hinaus intensiv mit den Themengebieten Cyberwar, Informationskrieg, Technik und Gesellschaft. Er war bei der ITP Consulting, der EDVg und der TU Wien tätig und ist seit 2009 an der Landesverteidigungsakademie, wo er in zahlreiche Projekte, unter anderem KIRAS MDL und KIRAS QuOIMA, eingebunden war.