Operations Research for Risk Management in Strategic Foresight

Article · August 2015

CITATIONS
7

READS
2,677

3 authors:

Silja Meyer-Nieberg
Universität der Bundeswehr München
73 PUBLICATIONS **1,067** CITATIONS
SEE PROFILE

Stefan Wolfgang Pickl
Universität der Bundeswehr München
319 PUBLICATIONS **1,918** CITATIONS
SEE PROFILE

Martin Zsifkovits
Rail Cargo Austria
37 PUBLICATIONS **212** CITATIONS
SEE PROFILE

GLOBAL RISK FORUM GRF DAVOS GRF
planet@risk
http://www.planet-risk.org

Operations Research for Risk Management in Strategic Foresight

MEYER-NIEBERG, Silja[a], PICKL, Stefan[a] and ZSIFKOVITS, Martin[a]

[a] Institut für Theoretische Informatik, Mathematik und Operations Research, Fakultät für Informatik, Universität der Bundeswehr München, Germany, e-mail: silja.meyer-nieberg@unibw.de; stefan.pickl@unibw.de; martin.zsifkovits@unibw.de

Abstract – Detecting and identifying future risks is a major issue for public decision makers, especially in the field of the military defence. Decision makers need to identify threats to be able to react to them adequately and so reduce risks. Therefore, we established a general risk management support guideline for public decision makers with a focus on national security. The framework aims for identifying future risks, analysing and evaluating them, so that concrete actions can be set that tackle the potential threat. The risk management framework is based on the core process of the ISO3100 risk management norm and guides the decision maker stepwise through the complex process of forecasting. Therefore we are combining several available techniques and tools to get an overall picture of several scenarios. The focus is thereby put on national security applications of the risk management process.

Keywords – *risk management; operations research*

1. Introduction

The future is complex and uncertain. The modern world is interconnected on a broad scale making it difficult to predict future developments (Haebegger, 2010). There is significant change in the security and military domain: Calling the peace in Europe “fragile”, the Russian president questioned the reliability of the European peace order – of which Russia is an important element – and reminded the nations that there continues to exist a residual military threat in Europe. This risk not only requires their attention and analysis but also their preparations including measures for possible military reconstitution (Buch, 2014).

Nothing will be like in the preceding far more harmonious decade. As of now new risk and threat assessments have to be made concerning potential interventions by Russia in its Western periphery, eventually supported by White Russia. In order to prepare against these renewed risks, nations and their military establishments as well as NATO and EU have to prepare new threat analyses of the cold war type – with the only advantage that Moscow is today in relative terms less powerful, but substantially more exposed (Buch, 2014).

However, an early detection and analysis of developing threats in the area of national security plays is of utmost importance. Strategic foresight is often cited as a tool to inform public policy and decision makers of potential future developments decreasing the chance of harmful surprises. While it stems from the economic sector it has been recently applied more and more in the area of national security (Habegger, 2010). It comprises typically three phases: an early detection and analysis of developments, the generation of foresight knowledge, and the development of policies to cope with threats or to benefit from opportunities (Habegger, 2010). The detection of trends, drivers, and wild cards or horizon scanning is the first step of the strategic planning process, see also (Rademacher, 2009). Based on the data gathered a prediction of potential future developments is made in the second phase. In the third phase, the potential futures are analyzed with respect to their likelihood of occurring and policies are developed to improve the state’s resilience.

In this paper, we introduce a risk management framework for the area of public policy that is designed to take potential future risks into account. The article is structured as follows. After a short introduction into risk management and the ISO3100 norm, the framework proposed is based upon, the three main phases of the framework are described in detail together with the tools that were developed to support the analyst.

2. Risk Management Processes: The ISO3100 Norm

Risk management is the means by which the policy maker keeps risks for humans and their livelihoods as low as possible, or at least within acceptable bounds. This leads to the question of where the level of acceptance can be set.

"How safe is safe enough?" These aspects make the risk management process even more complex and lead to the need of comparisons and planning from a holistic perspective (Federal Office for Civil Protection, 2014: 4). Risk management does not only play a major role for public decision makers, but also for private companies. The management process behind it is similar and comparable over the sectors. The Fraunhofer-Institute conducted a survey on the risk management process in German companies that shows that there are several policies used within companies to respond to risk structurally, especially to technical risk (Zentis et al., 2011: 11ff). This implies that there is also a need for a structured public risk management process that guides decision makers through the identification, evaluation, and treatment of risks in public decision processes.

There is a standardized risk management process structure available, called ISO3100 norm. This generalized process guideline is a promising framework for such a structured process. According to the definition of the ISO31000 risk management process, it is structured as shown in Figure 1 (ISO31000, 2009).

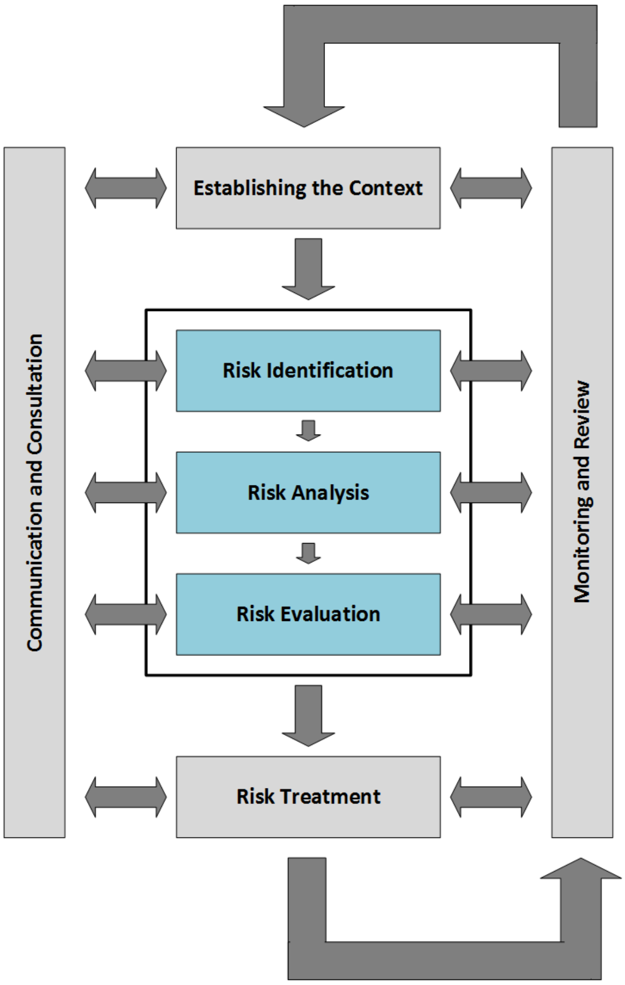


Figure 1: ISO Risk Management Process (ISO31000, 2009)

"Establishing the Context", "Communication and Consultation", "Risk Treatment", and "Monitoring and Review" are interactive tasks that need to be handled by the decision maker continuously. However, the core of the risk management process is the identification, analysis, and evaluation of risks. Therefore we are creating a framework that supports the decision maker and guides through the management core process based on several existing tools that were individually developed. One has to note that the presented and recommended tools need to be selected, analyzed and evaluated for every case separately. Thus, the process needs adaption for each application that might be evaluated. However, the basic structure stays unchanged.

In general, the process is based on the earlier established context of interest and leads to concrete recommendations for responding to the risk. An example therefore is illustrated in Table 1.

Table 1: Establishing Military Context and Treatment

Context	Actions and events that might lead to intervention of the German military[a]
Treatment	Increase the number and preparedness of especially skilled forces for employment in target regions.
a) Peace Support	1.Peace keeping mission (Art. VI UN) or 2.Peace enforcing mission (Art. VII UN) -prepare transportation, deployment and logistics for own troops -upgrade and consolidate CIMIC[b] -prepare support for allied forces with equipment, training and logistics
b) Defense	-prepare national elements of the NATO Response Force and/or contribute to and reinforce Battle Groups of the EU

[a] According to principles guiding decisions of the German government and the Bundestag the German military will be tasked for missions only in the context of decisions taken by the UN, NATO and the EU, as well as – exceptionally – in a "coalition of the willing", e.g. Kosovo war and actually training assistance against ISIS/ISIL.

[b] Civil-military cooperation.

The risk management core process brings together the overall context of the threat and concrete recommendations for the risk treatment on a case by case basis.

3. The Risk Management Framework

As explained above, we concentrate on establishing a framework to support decision makers in the risk management process in its core tasks: risk identification (RI), risk analysis (RA), and risk evaluation (RE) as shown in Figure 2.

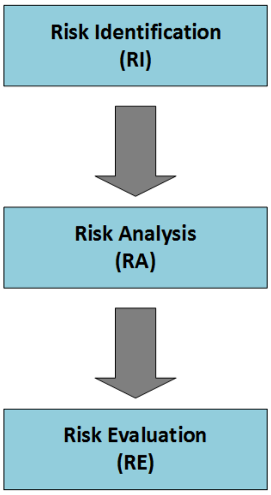


Figure 2: Core Tasks in the Risk Management Process

In the core process, each task is a single unit and needs to be completed before the next step can be handled, as the information from each task is the basis for the following. The documentation of tasks and their findings as well as the transfer of knowledge across several steps thereby play a major role in the overall process. In the military domain these tasks are generally known as "risk assessment".

In the upcoming section the three steps of the risk management core process are explained in more detail and several tools are presented for future use and combination in one overall risk management framework.

3.1. Risk Identification: Catalogue of Hazards

After establishing the general context one has to define the problem area itself and analyze it in detail. The objective of this step is to collect and structure as much hazard data as possible in order to create therewith a catalogue of hazards. The catalogue of hazards thereby describes, which threats are existing in the predefined future time horizon. Especially for the field of national security the consideration of several existing qualitative and quantitative methods is a promising approach for finding areas of interest. Originally, foresight focused on only one particular area, e.g. science and technology, health, or environment (Habegger, 2010) neglecting potential interconnections between different sectors. However, restricting the analysis to a single sector may present a risk in itself if the area of national security and public policy is concerned. The risk management process must therefore take several areas into account and must select the particular focus points very carefully. Therefore, qualitative and quantitative methods for future analysis have been identified and analyzed in a project conducted at the Universität der Bundeswehr München and supported by the Planungsamt of the German Federal Armed Forces. The aim is to gain general insight into existing and potential future risks. These first insights and data are of great importance, as the further analysis is based on those findings (such as the definition of keywords, prioritization of regions, etc.). In the area of strategic foresight, this first phase is usually associated with environmental or horizon scanning. Scanning can either be conducted explanatory or be centered on specific issues (Amanatidou et al., 2012). An explanatory scanning has a wide scope and tries to identify signals from various sectors that may be of importance to the organization or the state itself. A bottom-up approach is recommended taking various sources into account and applying several techniques (Amanatidou et al., 2012). Internet searches, scientific or technical publications, social media may alert the analyst to potential developments. While single signals may not appear as important, the coincidence of several signals from different sectors may represent a key issue for the organization. Here, however human judgement is required. Therefore, the information gained has to be analyzed by experts with respect to underlying emerging issues. After the area of interest has been narrowed, an issued-centered scanning is recommended (Amanatidou et al., 2012). In this paper, we propose to use a combination of several approaches, see e.g. Figure 3.

The first is an indicator-based approach. With respect to the area of interest and the emerging issues, indicators can be defined, e.g. the infant mortality rate which is one of the key factor in Goldstone's model on political instability. In some cases, new, specially designed, indicators will have to be used. However, the set of country-based indicators that is provided by the World Bank may already offer sufficient information for many areas of interest. The set of indicators spans several areas ranging from data concerning agricultural and rural development over health, education, and poverty to urban development. In order to allow a structured integration into a risk management process, an early warning tool was developed. The country-based tool enables the visualization of the past development of indicators and a prediction into the future by making use of quantitative methods for future analysis (Masala, Pickl, 2013). Furthermore, explanatory models, as for example the model in (Goldstone, 2005) which addresses the political instability of states are provided. The modular tool considers political, social, and economic indicators from various sources and therewith enables the analyst to detect geographical areas where e.g. political instabilities are more likely to come up in the nearer future than in others.

Additionally, an internet-based horizon scanning, i.e., an analysis of the web, may lead to promising findings in the detection of future threats (Palomino, Taylor, Owen (2012). For this purpose, a topic monitoring tool was developed. The analyst defines high-level keywords that are automatically translated into several languages and the web is screened on articles about this issue (Stutzki, 2014). An example for national security purposes might be screening the web for pages and articles on "terror", "IED", "-bombs", "clashes in demonstrations", "riots", "political revolution" or others. The tool also allows for analyzing the quantity of published articles on a topic as well as the country of origin of the articles (Stutzki, 2014; Hauschild et al. 2014, p. 15). The data gathered for a specific high-level keyword are analyzed for the prevalence of further significant terms. In addition, the tool focuses on the activity in a particular topic and enables therefore the analyst to identify on time-dependent trends and changes.

This method might be very useful combined with Google Trends, a real-time index of the volume of queries that people enter into Google. Especially with full access one can find query-trends in special geographical areas. Thus, the keywords from the trend detection will also be tested for being search engine queries at Google by a larger number of people. This should show, if there are specific geographical areas where such topics are currently more prevailing than in others. Using this tool is already successfully used for detecting economic trends (Choi and Varian, 2011) and the outbreaks and spreads of diseases (Carneiro and Mylomakis, 2009). Therefore, the method might be promising also for detecting outbreaks of political revolutions or riots. Just like in the trend detection tool, detected keywords can be clustered based on their frequency on a geographical map.

Additionally the use of further quantitative methods is recommended. The question of which methods may be applicable depends on the specific context of the risk management. The reason is, that a maximal possible number of data should be used in order to identify possible future threats. Weaknesses and limitations of single approaches should be compensated by using a selected set of different approaches.

The findings of these steps are finally analyzed using the qualitative method of expert interviews. A group of experts on the established content is confronted with the data gathered in the earlier steps as well as with the resulting geographical maps. On this basis the experts are discussing the results, summarize and evaluate the existing sample of threats and include them in the catalogue of hazards. A graphical illustration of the risk identification process is shown in figure 3.

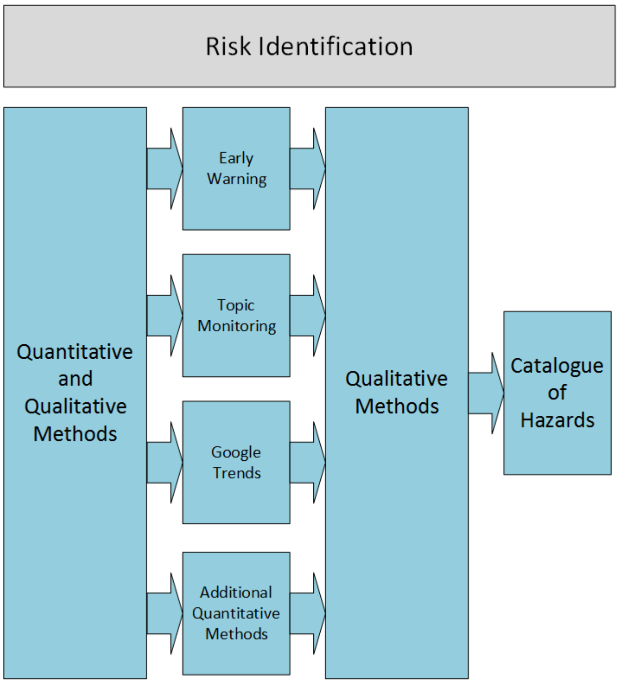
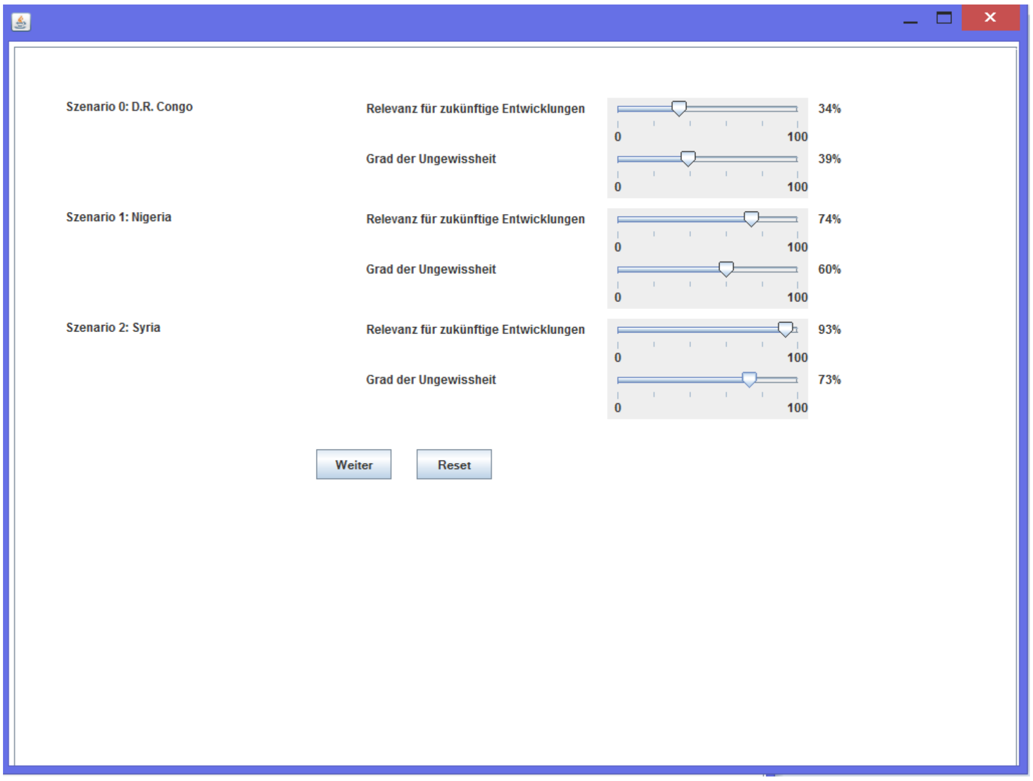


Figure 3: Risk Identification Process

The identification of trends is an important achievement. However an identified trend has to be further analyzed and correlated with other trends, which is a major


Szenario 0: D.R. Congo

Relevanz für zukünftige Entwicklungen 0 100 34%

Grad der Ungewissheit 0 100 39%

Szenario 1: Nigeria

Relevanz für zukünftige Entwicklungen 0 100 74%

Grad der Ungewissheit 0 100 60%

Szenario 2: Syria

Relevanz für zukünftige Entwicklungen 0 100 93%

Grad der Ungewissheit 0 100 73%

Figure 4: Software Prototype for Scenario Analysis – Rating of Scenarios

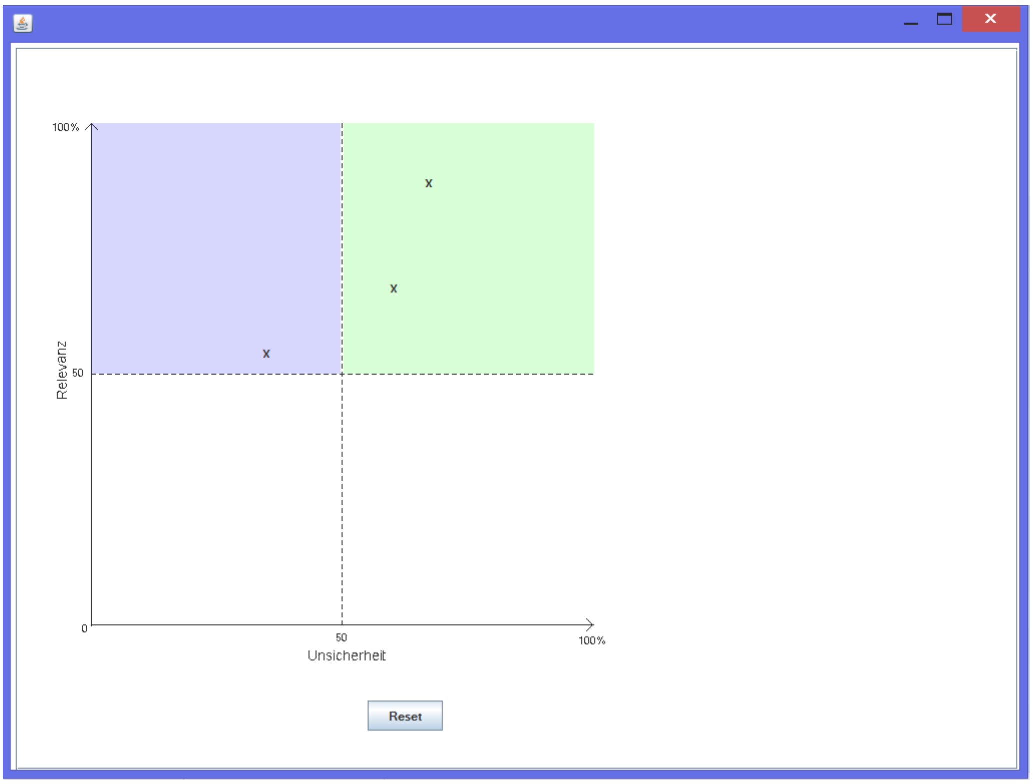


Figure 5: Software Prototype for Scenario Analysis – Rating of Scenarios

challenge and requires computer based analyses. The documentation of the risk identification process is therefore a key issue for the further steps of managing risks. The whole documentation and the catalogue of hazards is now passed into the next step of the process, the risk analysis.

3.2. *Risk Analysis: Define and Analyze Scenarios*

Based on the detected existing and potential threats and their graphical representation in geographical maps, future scenarios are identified. Ideally the experts from the qualitative expert interviews are now picturing future scenarios based on the available data. Thereby, the scenarios are firstly just collected on a broad range. So far, no rating of scenarios based on whatever criteria was needed. In a further step the scenarios are clustered based on their relevance and their uncertainty of occurrence. Therefore, the prototype of a software tool was designed that detects the most relevant scenarios needing further analysis based on the experts' ratings. The selection criteria are based on the subjectively estimated relevance for the decision maker and the perceived uncertainty coming with each scenario. The benefit of the software support is on the one hand, that the decision maker is forced to think about uncertainties and the relevance, and on the other hand this information is transferred without interruption to the next steps of analysis. Even if experts or decision makers change over steps, the information and data stays stored in the tool. The manual rating of scenarios is shown in Figure 4.

The chosen, described and rated scenarios are now plotted in a graph, where the scenarios above a 50% relevance are seen as being relevant for further analysis. These scenarios are further divided into more (≥50%) and less (<50%) uncertain scenarios as shown in Figure 5. The boundary values can also be changed according to the decision makers' preferences.

The scenarios being detected as relevant should be analyzed in more detail in a further step. Interconnections to several external influences as well as interconnections between scenarios might give additional insights into the scenario's network. Therefore, based on the approach of Vester (2000) each scenario is illustrated in a network based on existing influences (positive [+] and negative [-]). This also allows for getting additional insights into relevant reinforcing factors in the scenarios. An exemplary illustration of such a network is shown in Figure 6 which shows how several factors ranging from the raging Ebola epidemic to economic crises may affect the baseline scenario.

Hereby, the „Communication and Consultation“ as well as the „Monitoring and Review“ in the general risk management framework are of great importance, as newly identified impact factors should be further analyzed in following steps of analysis in the risk identification phase. Thus, in the next cycle of analysis e.g. additional keywords are to be analyzed in the tools used for trend detection. Furthermore, the network might be useful in the final step, the risk evaluation. Especially, if simulation is chosen to be the ideal tool for the risk evaluation.

The graphical overview of the risk analysis as single part within the risk management core process is illustrated in Figure 7.

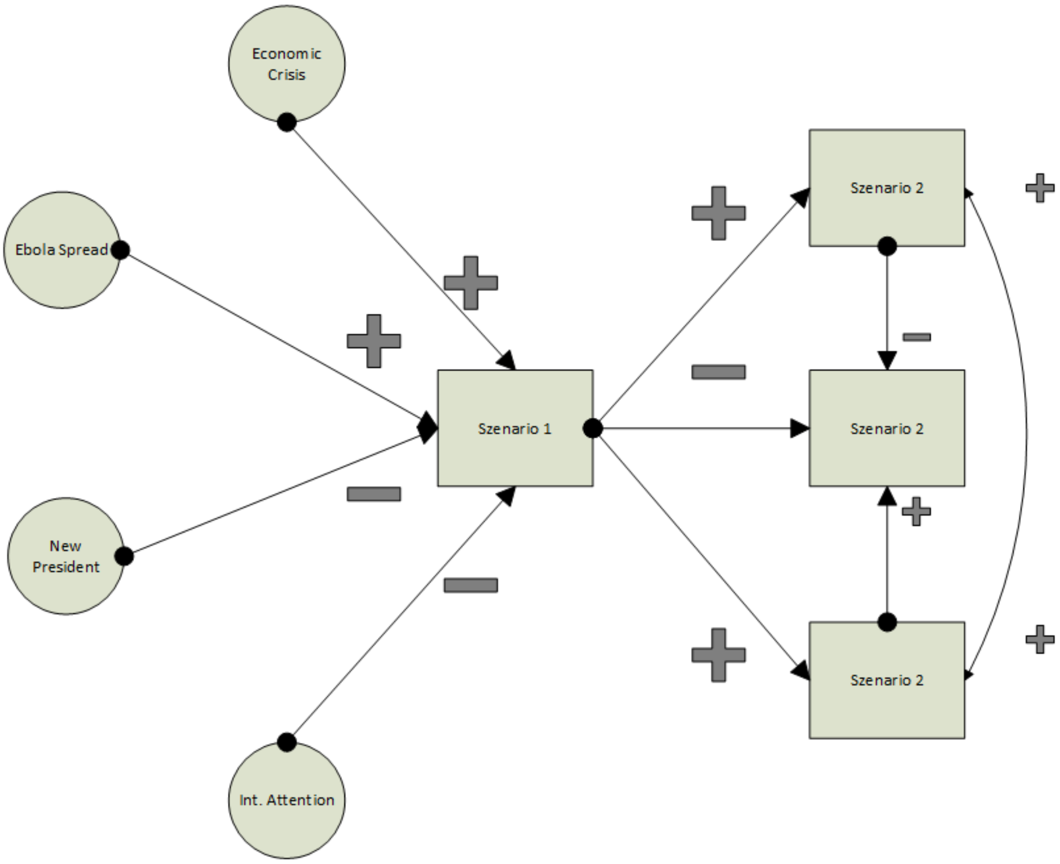


Figure 6: Networked Thinking

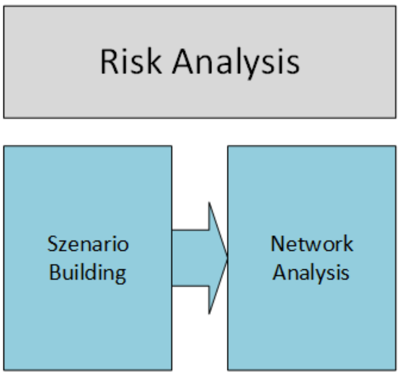


Figure 7: Risk Analysis Process

3.3. *Risk Evaluation: Define and Analyze Scenarios*

As the hazards were already detected and analyzed in detail, as well as relevant scenarios designed, the final step of the risk management tool deals with the evaluation of the scenarios. Therefore, the underlying findings and data from earlier steps need to be considered in order to decide, which approach fits best for an analysis. Depending on the availability of data, we present three promising tools that are able to give meaningful results and managerial implications for the decision maker.

1. If there is sufficient statistical data available, the future methods catalogue might be screened for promising tools for analysis. Especially the statistical methods might be considered for evaluation and analysis. The catalogue describes approaches and gives an idea on their usage. Another approach that might be considered is simulation (although it is also named in the catalogue, we consider it separately in this step). Thereby, the problem description itself and the available data gives an idea which approach to choose.
2. If the problem allows an analysis from the macro view and the prior conducted network analysis already shows meaningful insights, System Dynamics modeling might be chosen as shown. An application of a System Dynamics model can be found in (Hauschild et al. 2014) where it was used to analyze scenarios concerning the effects of the demographic change on the personnel structure and recruitment of the German Federal Armed Forces.
3. However, if there is data on a micro level available and agents' actions can be estimated, Agent-Based modeling might be the most promising tool for evaluating the future scenarios and getting an idea of future likely changes. This model type is used to depict the behavior of autonomous agents, describing the potential actions and interactions between them and the environment. They are typically employed to analyze the collective, emergent behavior of the system under interest (Macal and North, 2010). Agent-based models have been used in the social and political sciences for several years addressing topics as diverse as epidemics or ethnic conflicts (Epstein, 2008, p. xii). (Hauschild et al. 2014) describes e.g. the development of an Agent-

Based Model for analyzing social conflicts and unrest in Guinea.

If there is sufficient data available for more than one approach, a combination of two or more should be the objective, as limitations of the results might be reduced.

However, if the techniques presented so far cannot be used, a Fuzzy-Logic analysis might be conducted. Therefore, a list of several future scenario outcomes is developed and their relevance is weighted. In the field of application at hand, we might consider human, ecological, economic, supply security, and immaterial factors. Therefore, possible outcomes need to be defined, such as:

Human

1. Killed population
2. Injured population
3. Needy population (up to 14 days)
4. Needy population (more than 14 days)

Ecological

1. Damage of protected land such as wildlife sanctuary
2. Damage of living environment in water bodies
3. Damage of ground water
4. Damage of agriculture and forestry

and several more.

Based on the defined parameters, the scenarios are divided into sections and possible future extreme scenarios are identified and illustrated. The data is then compared to boundary values that define the heaviness of the outcome on a five-point scale. The outcomes themselves can furthermore be weighted regarding their relevance. Furthermore, the probability of occurrence for every event needs to be estimated.

Finally, the influences are summarized using fuzzy logic and according to a membership function, the scenarios can be evaluated based on the final matrix. The matrix compares the estimated damage and the probabilities of occurrence and therewith gives deeper insights into the scenarios. A generally valid Fuzzy-Logic analysis tool for military application is going to be designed in future research, so that at least the Fuzzy Logic Analysis can be used as a standardized tool. The general risk evaluation process is shown in Figure 8.

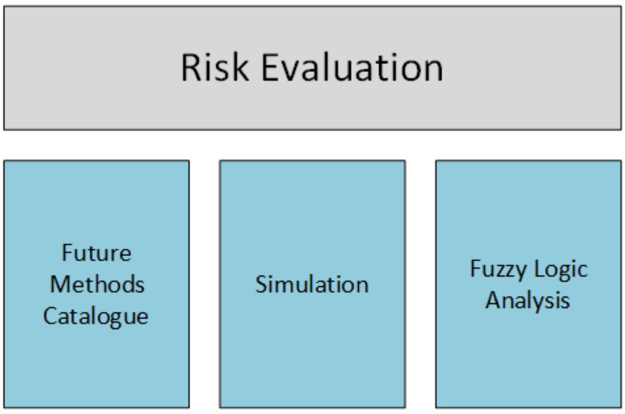


Figure 8: Risk Evaluation Process

4. Conclusions

The article at hand analyses the risk management process in more detail and presents a general framework that allows coping with several factors of risk for public decision makers in a structured process. Especially the context of national security was considered in the development of the framework. Hereby one has to note that the risk management process is a continuous process that does not deliver concrete values, but in general supports decision makers through showing possible scenarios and outcomes based on the underlying decisions made. As the decision is - at best - just as good as the data available, especially the risk identifications stage plays a major role and combines several approaches. Therewith, we want to compensate limitations of single approaches and get a broad sphere of influencing factors. The qualitative approach allows for correcting implausible or unlikely trends in the data and adds another, very important view on the topic. However, the review and communication all through the risk management process is a key factor for success. Especially for combining the different methods and implementing a framework that considers learning effects from the different approaches used, further research is needed. For example the analysis of online trends using Google trends and the topic monitoring framework should be connected and based on a database of keywords that are of interest. Furthermore, this database should be further developed based on findings in other tools such as the network analysis. If one finds that another influencing factor might play a key role in the network analysis, this factor should be considered in the analysis of the next round.

The presented framework is therefore a promising approach for guiding decision makers through the risk management process and providing additional and deeper insights. The framework is kept very general, so that various contexts can be analyzed based on it. However, a modification for special analyses might make sense in several cases, so that the process gets an active, learning, and adaptive framework.

5. Acknowledgements

The support by the Planungsamt der Bundeswehr is gratefully acknowledged.

References

Amatidou, E., et al. (2012): On Concepts and Methods in Horizon Scanning: Lessons from Initiating Policy Dialogues on Emerging Issues, Science and Public Policy 39, pp. 208–221.

Buch, H. (2014) Interview with Heinrich Buch, Dipl.Pol.,Oberst a.D., Senior Advisor at COMTESSA.

Choi, H., Varian, H. (2011): Predicting the Present with Google Trends, Special Issue: Selected Papers from the 40th Australian Conference of Economists, Vol. 88, pp. 1–9.

Carneiro, H.A., Mylonakis, E. (200) Google Trends: A Web-Based Tool for Real-Time Surveillance of Disease Outbreaks, Surfing the Web, Vol. 49, pp. 1557-1564.

Epstein, J. (2008): Generative Social Science. Studies in Agent-Based Computational Modelling. Princeton University Press,.

Federal Office for Civil Protection (2014) Integrated Risk Management, Bern, Switzerland.

Goldstone, J.A. et al. (2005): A Global Forecasting Model of Political Instability, in Annual Meeting of the American Political Science.

Grundmann, T. (2008): Wertorientiertes Risiko-Management für Industrie und Handel, Gabler Verlag, Wiesbaden.

Habegger, B. (2010): Strategic foresight in public policy: Reviewing the experiences of the UK, Singapore, and the Netherlands, Futures 42, pp. 49–58.

Hauschild, D., Leopold, A., Lohmann, S., Masala, C., Meyer-Nieberg, S., Pickl, S., Plenk, S., Tepel, T., Zsifkovits, M. (2014): Quantitative Methods of Future Studies, Final Report, Universität der Bundeswehr München.

ISO31000 (2009) Risk Management – Guidelines for principles and implementation of risk management.

Masala, C., Pickl, S. (2013): Foresight Analysis: Quantitative Methoden der Zukunftsanalyse, Wehrwissenschaftliche Forschung – Jahresbericht 2013, pp. 58-59.

Macal, C. M. and North, M. J. (2010). "Tutorial on agent-based modelling and simulation." Journal of Simulation 4(3): pp.151–162.

Palomino, M.A, T. Taylor, T. and Owen, R. (2012): Towards the Development of an Automated, Web-based, Horizon Scanning System, Proceedings of the Federated Conference on Computer Science and Information Systems, p. 1009–1016.

rahs-bundeswehr.de (2014): Risk Assessment and Horizon Scanning (RAHS) - Die Plattform für sicherheitspolitische Zukunftsanalysen; `https://www.rahs-bundeswehr.de/`, Accessed on the 19th. of September 2014.

Rademacher, M. (2009): National Security Strategy of the Netherlands. An Innovative Approach. INFORMATION & SECURITY, 23 (1), pp. 51-61.

Stutzki, J. (2014): Multilingual Trend Detection in the Web, Proceedings of the 4th Student Conference on Operational Research SCOR 2014, OASICS, Vol. 37, pp. 16-24.

Vester, F. (2000): Die Kunst vernetzt zu denken: Ideen und Werkzeuge für einen neuen Umgang mit Komplexität; DVA Stuttgart.

Zentis, T., Czech, A., Prefi, T., Schmitt, R. (2011): Technisches Risikomanagement in produzierenden Unternehmen, Apprimus Verlag, Aachen.

Citation

Meyer-Nieberg, S., Pickl, S. and Zsifkovits, M. (2015): Operations Research for Risk Management in Strategic Foresight. In: Planet@Risk, 3(2): 1-4, Davos: Global Risk Forum GRF Davos.