Internet Science
Impact of social behavior for critical infrastructure resilience

René Milzarek
Betreuer: Dr. Heiko Niedermayer
Seminar Future Internet SS2013
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: rene.milzarek@in.tum.de

ABSTRACT

Technological progress is considered to be the key factor of our social as well as economic wealth. As new technologies and developments are an ubiquitous part of our daily life their fallibilty becomes more aware to us. E.g., the smart grid technology represents an essential aspect of the future transmission grid and requires the end user's acceptance to assure the resilience of the future power grid. In particular public concerns could threaten the resilience of critical infrastructure due to social amplification proccesses in the perceiption of risks. In this work an introduction to conventional risk analysis is given and its drawbacks are explained using the prospect theory. The conceptual framework of social risk amplification is utilised to describe how minor risks could elicit great public concerns. Finally a use case shows how indicators could measure the social amplification process and which analytic potentials are provided by social media.

Keywords

Risk; risk analysis; risk management; risk perception; social amplification; social media; critical infrastructure; resilience; smart grid

1. INTRODUCTION

New technologies found their ways into almost every part of our daily lives and entailed the developement of new industries and infrastructures (e.g. mobile communication networks). We are to such an extent accustomed to the presence of these technologies, that we are mostly not aware of their fallibility. Especially critical infrastructure - which could "be defined as those elements of infrastructure that, if lost, could pose a significant threat to needed supplies [...], services [...], and communication or a significant loss of service coverage or efficiency" [3] - need to be guaranteed sufficient resilience.

For example the electric power supply represents a critical infrastructure, that is taken for granted more than any other. But several major blackouts in the past years demonstrated that the resilience of today's power supply system is not as reliable as the individual impression assumed it to be [1, 12, 13]. Among others the problem is caused by "increasing load demands", "quickly aging components and insufficient investmens for improvements" [6]. However a new technology - the smart grid - emerged, which could solve the issues within the near future [10]. In general the smart grid is defined as "a network of computers and power infrastructures that monitor and manage energy usage" [10]. The typical structure of a smart grid is illustrated in Figure 1 on the next page, though it should be noted that the communication between the smart appliances and the operational centers (represented by the processors in the figure) is realised with a radio communication or the internet [10].

If the smart grid gets implemented widely, the implications will be an "[enhanced] energy transmission management and [increased] resilience to controlsystem failures and cyber or physical attacks" [10]. But therefore it is absolutely vital that this technology is roled out in a majority of households, as well as energy producing and consuming industries. Due to the design of the future electric distribution network, which assumes that energy production faces a transformation to a more and more locally oriented one, it is required to control the power distribution in a smart way to avoid electricity shortage or overload. Therefore smart appliances - the so called smart meters - have to be installed in every household. This is where the social behavior comes into play, since the acceptance of those appliances determine the successful introduction and consequently the resilience of the smart power grid [6].

Several works on the security and privacy challenges of the smart grid reinforce the impression, that "although deploying the smart grid has enormous social and technical benefits [...]" [10] there are occuring more and more concerns [9, 10]. The social perception of such risks could play a key role in the establishment of a new technology. Therefore the following chapters consider methods to analyse those risks and how social behaviour could influence the perception of risks.

2. THEORIES OF RISK ANALYSIS AND PERCEPTION

The first occurrence of a method, which could be considered the root of risk analysis, goes back to about 3200 B.C. in the area of todays Syria and Iraq. A group called the

doi: 10.2313/NET-2013-08-1_09

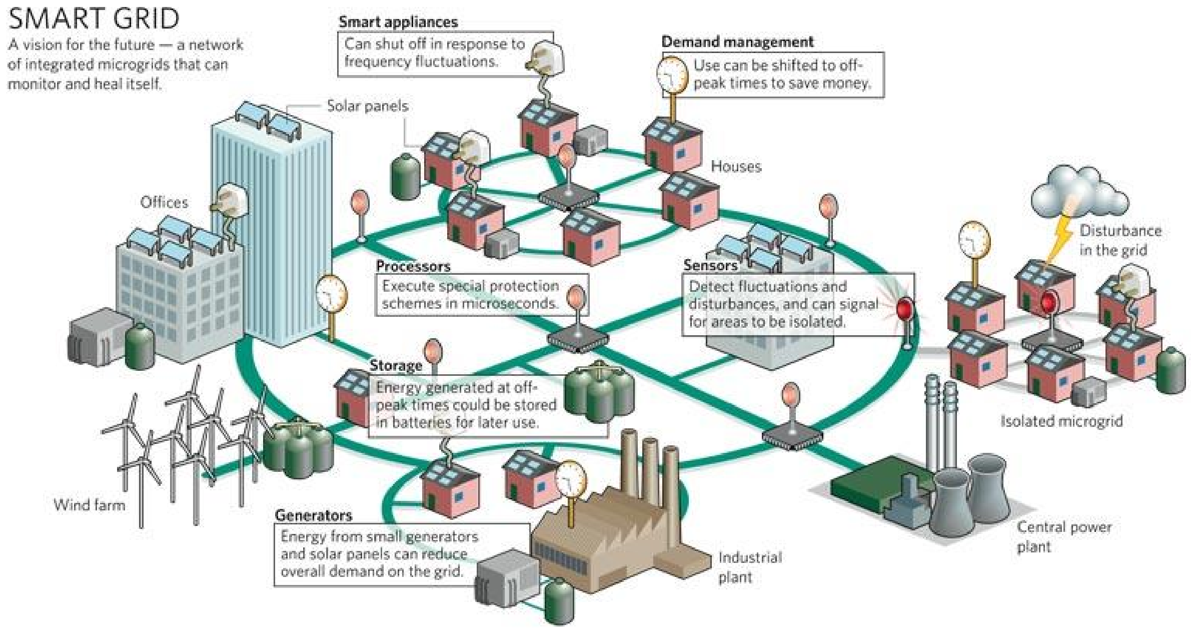
SMART GRID
A vision for the future — a network of integrated microgrids that can monitor and heal itself.
Smart appliances
Can shut off in response to frequency fluctuations.
Demand management
Use can be shifted to off-peak times to save money.
Solar panels
Offices
Houses
Disturbance in the grid
Processors
Execute special protection schemes in microseconds.
Sensors
Detect fluctuations and disturbances, and can signal for areas to be isolated.
Storage
Energy generated at off-peak times could be stored in batteries for later use.
Isolated microgrid
Wind farm
Generators
Energy from small generators and solar panels can reduce overall demand on the grid.
Industrial plant
Central power plant

Figure 1: Basic structure of a smart grid distribution network.

Source: `http://energyinformative.org/wp-content/uploads/2012/01/smart-grid.jpg`

Asipu consulted clients in risky decisions by identifying possible actions and concluding likely results for each alternative. Afterwards they evaluated those options by interpreting signs of god for each one individually [4]. Nowadays profound and science-based techniques apply, especially since the twentieth century when governments in advanced industrialized countries strengthened efforts to establish methods for analysing and managing risk. Despite these activities, which aim to control and diminish risks, the current trends show that people regard themeselves even more exposed to the dangers of technology [8].

2.1 Risk Analysis and Management

This section should give a brief overview of the risk analysis and management methodology. The target of a risk analysis in general is to "[...] identify potential threats to and vulnerabilities of [a critical asset] and the associated risk" [5]. The activity of risk analysis, sometimes also denoted by risk assessment, is one part of an organizational risk management process[14].

2.1.1 Risk Analysis or Assessment

A risk analysis is not intended to be a one-time procedure, which results in a definite assessment for decision makers. It could be applied once, but it is rather an iterative process, which should be regularly executed to assure the observance of changing conditions. "Risk assessments are used to identify, estimate, and prioritise risk [...]" [14]. Therefore the risk is regarded as a scale to measure the degree to which an asset is endangered by a certain event or circumstance [14]. Typically risk is defined by the multiplication of the probability of the harmful event and the magnitude of the triggered adverse effects

$$risk = probability \times magnitude.$$

A risk analysis usually consists of a risk assessment process, a risk model and an assessment approach [14].

Basically, the risk assessment process includes the steps of preparation, conduction, result communication and maintenance. In the following the step of conduction will be reviewed in detail. First of all the threat source and events, vulnerabilities, as well as the predisposing conditions get identified. Afterwards the actual risk is calculated with the before introduced formula, therefore the probability of occurence and the magnitude of impact are needed to be determined. For further details on the other steps please refer to [14].

"Risk models define the risk factors to be assessed and the relationships among those factors" [14]. The risk factors include all variables, conditions or circumstances that somehow affect the level of risk. The factors threat, vulnerability and predisposing condition were already mentioned above, further typical risk factors are impact and likelihood. Since these terms are fundamental properties of the risk analysis methodology, they will be defined in the following.

"A threat is any circumstance or event with the potential to adversely impact" [14]. Whereas a vulnerability is defined as a weakness in an asset, that somehow can be exploited by a threat source. If the liklihood of a threat event is influenced by a condition within an organization or company, one speaks of a predisposing condition. "The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences [...]" [14]. Finally the liklihood of occurence derives from the analysis of probability and represents a weighted risk factor to describe the capability of a given vulnerability to be exploited.

After all the assessment approach defines methods of assessing risk and its contributing factors. There are several different approaches to deal with this task. The quantitative assessments define a set of functions, which map the risk to a concrete number. These function are derived from statistical analysis. Therefore they have the advantage of being very efficient, easily applicable and not dependant from subjective perceiption. The qualitative assessments in contrast usually apply a nonnumerical system of categories (e.g. very low, low, high, very high) and therefore rely on the subjective estimation of experts. They compare and prioritise the risks on basis of their individual experience, which on the one hand intensifies the risk communication and on the other hand has the disadvantage of being poorly or not at all repeatable and reproducable. Finally, semi-quantitive assessments combine both methods and employ a set of principles or rules to map the risk to bins or scales (e.g. 0-10, 11-20, ...). Thereby the risks could easily be compared with each other and the role of the expert's subjective judgement gets more comprehensible.

2.1.2 *Risk Management*

As mentioned before, the risk assessment is only one part of the risk management process, which is illustrated in Figure 2. The central component of risk management is the risk management strategy, which has to be setup in each organization individually. This strategy defines how the organization "intend[s] to assess risk, respond to risk, and monitor risk [...]" [14].

Having been identified during the risk assessment the risks have to be evaluated in the context of the particular risk management strategy. The prioritisation of the risks analysis is not ultimate, other factors like budget or relevance for the core business may also influence and change the final priorities.

The next step is to manage these reprioritised risks, by defining actions to respond to them. These actions have to be in accordance with the organisation's risk management strategy. Despite the developement of suitable actions, this also covers the evaluation of alternative actions, as well as the inspection of the compliance with organizational risk tolerances. Finally, the planned respond actions have to be executed.

During the whole execution time, the risk responses have to be measured and controlled to assure their ongoing effectiveness. If they do not come up to their intended risk diminishement or control, they have to be adjusted or replaced by replanned measures. But not only the respond actions have to be monitored, as the risk itself could change over the time due to modified conditions [14].

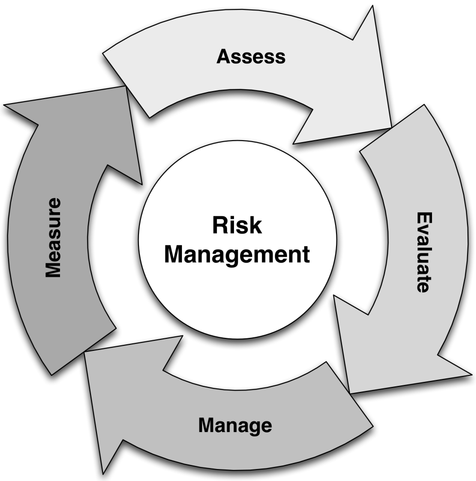

Figure 2: The risk management process.

In summary, the process of risk management requires ongoing efforts to control the impacts of risks. There is a plurality of methods for performing risk assessment and risk management, but as each organization needs to establish a individual strategy, there is no "best practice" method, that covers every deployment optimally [5].

2.2 The Prospect Theory

An essential step of a risk analysis is, as seen before, the determination of the occurrence probability. Except the quantitative assessment, every method relies on an expert's estimation. But there are two phenomena, which deteriorate the human assessment of probabilities. On the one hand there is "[...] the overestimation that is commonly found in the assessment of the probability of rare events" [7]. And on the other hand there is the overweighting which additionally corrupts the estimations and will be examined below. The prospect theory is based on simple decision problems, where students were asked to choose their prefered option.

Option A	Option B
33% chance to win 2500 66% chance to win 2400 1% chance to win nothing	Win 2400 for sure

Table 1: A simple decision problem

Although option A has the expected value of $0.33 \times 2500 + 0.66 \times 2400 + 0.01 \times 0 = 2409$, which is obviously more than the guaranteed win of 2400 in B, 82 percent of the students prefered option B. These studies were also made for decision problems where the options imply loosing money. Several surveys supported the finding that people do not always chose the economically best option, although they know the stated probabilities and hence do not suffer from overestimation.

The prospect theory introduces two effects to describe those biased tendencies. The certainty effect specifies the phenomenon that "[...] people overweight outcomes that are considered certain, relative to outcomes which are merely probable" [7]. The majoritarian selection of option B in the previous decision problem is one example for this effect and it can also be observed, if the gains were replaced with equal losses.

The second one is the reflection effect, which describes the incident, that people avoid the riskier option in the case of gain options, but otherwise seek the riskier option in the case of losses. This should be noted, because the technical concept of risk assumes that "[people] should be indifferent toward a low-consequence/high-probabilty risk and a high-consequence/low-probability risk with identical expected values" [8]. What does that mean for risk analysis? If people are faced with a risk situation, which requires the decision between options, and do not apply the before described risk management methodology, they tend to choose the riskier option [7].

Another aspect from the prospect theory, which is interesting for risk analysis is the weighting function π, illustrated in Figure 3, which tries to mathematically explain the process of overweighting. The function π is not continuous and transforms the stated probability into a weighted probability, which takes the desirability of the expectation and not just its likelihood in consideration. On the boundary of the function's domain it holds $\pi(0) = 0$ and $\pi(1) = 1$. The curve progression indicates, that small probabilties get overweighted and bigger probabilities get systematically underweighted. Therefore π runs above the identity function for very small propabilties and below for high probablities.

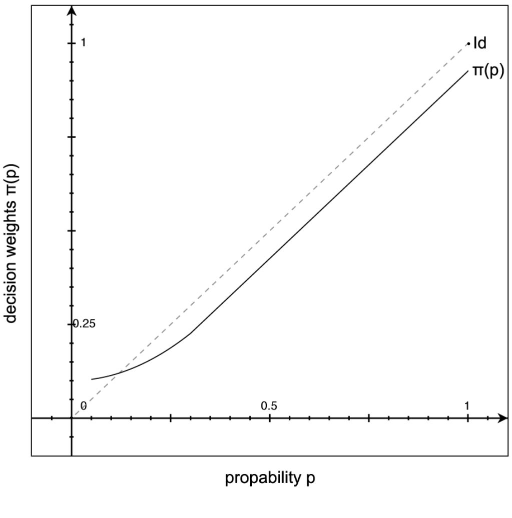

Figure 3: The weightening function of the prospect theory [7].

The in extracts listed conclusions of the prospect theory should make aware of the necessity of a formal risk management methodology to assure an accurate risk assessment. Unfortunately it does not provide methods to address the described effects. Especially in the case of very rare events, the estimation of a risk event's probability as well as its potential impacts is difficult. Aside from that the prospect theory examined decision problems, which were posed once and not multiple times. In this case the economically best option could not be determined by the comparation of the options' expected values, rather through the application of the game theory. Furthermore the impacts of the decisions were only monetary and thus it should be seen critically, if the results could be generalized. However the stated tendencies are valid, it is hard for humans to correctly estimate the probability and impacts of rare risk events. Besides the issues with individual perception of risk there are several "other aspects [...] as voluntariness, personal ability to influence the risk, familarity with the hazard, and the catastrophic potential" [8] that determine its perception. Especially the public perception of risk, which can be increased or decreased by the interaction of risk events "[...] with psychological, social, and cultural processes" [8], is another crucial aspect and will be examined in the next section.

2.3 The Social Amplification of Risk

The technical concept of risk approaches its limits when it comes to individual and public perception of risk. It is not able to explain why "relatively minor risk or risk events [...] often elicit strong public concerns" [8]. Especially the examination of indirect, higher-order impacts exceed the capabilities of technical risk assessment. The role of social amplification and attenuation processes gets often neglected by conventional risk analysis. Thus the concept of social amplification provides a framework to systematically link "[...] the technical asessment of risk with psychological, sociological, and cultural perspectives of risk perception and risk-related behavior" [8]. However the term of social amplification of risk might be misleading, because the actual risk of the risk event does not change. Moreover the public's perceived risk changes throughout the amplification process.

2.3.1 Amplification in Communications Theory

The metaphor of amplification derives from communcications theory and "[...] denotes the process of intensifying or attenuating signals during the transmission of information from an information source, to intermediate transmitters, and finally to a receiver" [8]. Each transmitter encodes received messages and afterwards recodes them for the forwarding to the final recipient. During that process the orginal information gets altered "[...] by intensifying or attenuating some incoming signals, [and] adding or deleting others" [8].

In the context of social amplification a message may contain several meanings, which can be altered during the transmisson or decoding. The actual content as well as the source of the message represent the factual meaning, the possible conclusions of the message refer to the inferential meaning and, in addition, a message could contain cultural symbols which are linked with strong value implications (e.g. terrorism, high technology, cyber security). Those meanings and information have to be decoded by the transmitters or recipient and afterwards checked for reliability. Especially messages from credible sources have a high chance of successfully passing the selection filters. But "reference to a highly

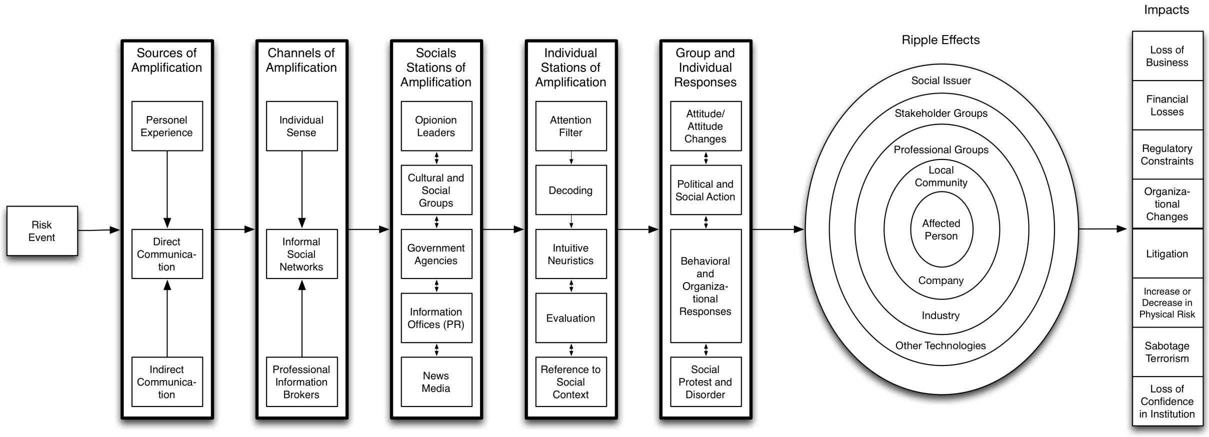

Figure 4: ”Detailed conceptual framework of social amplification of risk“ [8].

appreciated social value” [8] or a distinguished communication source may increase the tolerance for factual irrelevant or unproven messages.

2.3.2 *The Process of Social Amplification of Risk*

”Social amplification of risk denotes the phenomenon by which information processes, institutional structures, social-group behavior, and individual responses shape the social experience of risk [...]” [8]. Figure 4 illustrates how a risk event may be amplified through the processing by several amplification, social and individual stations. To pick up the smart grid technology example from the introduction, a potential path through the stations is described in the following. Imagine a hypothetical computer scientist, who has a new smart meter installed in his household and is aware of potential security issues. His investigations discover a severe security vulnerability, which allows an attacker to remotely access the smart meter and turn off the electrical power supply. Being ourtraged by his findings the scientist publishs them on his private blog and spreads a link to the entry via a social network. Friends, who are also concerned about the topic of cyber security share the post again, but with some added comments, which emphasize the fatal consequences of such a vulnerability. This example shows how easily a risk information gets filtered and selectively itensified, but there are more key amplification steps, which were originally hypothesized in [8]:

- Filtering of risk signals
- Decoding of the signal
- Processing of the risk information
- Attaching social values to the information
- Collective interpretation and validation of the signals
- Evolvement of behavioral intentions to tolerate the risk or take actions against it
- Engaging in group or individual actions

The filtering is a psychological phenomenon. People tend to selectively perceive information, which is in accordance with their personal prospect, and ignore or attenuate the remaining information. In the example above especially friends, who already established a refusing attitude towards the smart grid technology, tend to perceive only the negative aspects. Additionally the feeling of loosing control and privacy may be connected with cyber security, which will be automatically attached to the information and amplify the perceived risk. The intensity of the amplification and attenuation naturally depends on the given situation and may be more or less distinct.

But the amplification process continues and ”[...] will spawn behavioral responses, which, in turn, will result in secondary impacts” [8]. Several worried people could get together, form a group and protest against the introduction of smart meters, which possibly attracts strong media attention and results in third-order impacts and so forth. ”The impacts thereby may spread, or ripple, to other parties, distant locations, or future generations” [8]. This rippling effect implies that amplification can elicit tremendous temporary and geographically extended impacts and is not a phenomenon which is limited in time or space. In summary the social amplification of risk consists of two major steps - ”the transfer of information about the risk or risk event, and the response mechanisms of society” [8] which will be examined in Section 2.3.4.

2.3.3 *Influencing Attributes of Social Amplification*

The social amplification process is based on personal experience with risk, which can be made directly or indirectly. The greater part is experienced indirectly through the treatment of risk by other persons or the media. There are several attributes of perceived information which shape our experience. The first one is the volume of information, which measures the quantity of media coverage. The more often an event is addressed in media, the more familiar people get with it, what in turn results in a greater awareness of its risks. The second attribute is ”[...] the degree to which information is disputed” [8]. This issue was already discussed in the previous section and in short is mostly influenced by the credibility of the information source. The third attribute, dramatization, is often extensively utilized by the media and "[...] is undoubtedly a powerful source of risk amplification" [8]. Whether it is a sensational headline or a shocking picture, both serves the purpose of attracting more audience regardless of the consequences. The fact that "people's estimates of the principal causes of death are related to the amount of media coverage they receive" [8] represents only one of them. And the final attribute is the symbolic connotation, which just means that "[...] specific terms or concepts used in risk information may have quite different meanings for varying social and cultural groups" [8].

2.3.4 Response Mechanisms of Social Amplification

The last component of the social amplification process is represented by the response mechanisms. They determine how the information is interpreted, analysed and evaluated. There are again four major types of response mechanisms hypothesized in [8], which should be briefly described. As people are not able to fully receive and process all surrounding information, they use heuristics and values to simplify the evaluation, which also applies to risk assessment. Individuals learn those values during their childhood by adopting socially acknowledged behaviour, experienced in their social enviroment. Sometimes these processes may introduce biases to their interpretation of or behaviour in a certain situation. Another aspect which affects the response mechanisms is the influence of social and political groups. They have the ability to bring risk issues "[...] to more general public attention, [which is] often coupled with ideological interpretations of technology or the risk-management process" [8]. Moreover the perceived seriousness and potential to higher-order impacts of an event is determined by its signal value. A fatal car accident for example carries a smaller signal value than a minor incident in a nuclear power plant. This effect is based on the fact, that unfamiliar systems or technologies have a higher potential to create great public concerns, as the situation is perceived as not controllable or manageable. Finally, stigmatization describes to which extent a social group, individual or technology is associated with a negative image. "Since the typical response to stigmatized persons or enviroments is avoidance, it is reasonable to assume that risk-induced stigma may have significant social and policy consequences" [8].

The understanding of this conceptual framework is essential "for assessing the potential impacts of projects and technologies, for establishing priorities in risk management, and for setting health and environmental standards" [8]. Furthermore it could help to explain why "[...] minor risks or risk events often produce extraordinary public concern and social and economic impacts" [8]. In the next section the process of social risk amplification should be analysed with empirical measures on the basis of an example from the internet enviroment.

3. SOCIAL RISK AMPLIFICATION IN THE INTERNET ENVIRONMENT

It is crucial to understand how the process of social amplification generally works, but the actual goal is to establish measures or indicators that allow an early recognotion and thus treatment of potentially amplified risk events.

The study [2] examines a tunnel construction project, started in 1992, for a high-speed railway in South Korea, which was several times stopped due to the protest of environmentalists. They claimed that the construction harms the mountains ecosystem, which is the habitat of 30 protected species. Several hunger strikes and a filed claim interrupted the project multiple times and led to an delay of at least one year. The Korean Supreme Court finally dismissed the claim in 2006. It has to be noted, that the construction project was "approved by the official process of assessing need, feasability, and environmental impact" [2]. Nonetheless the responsible authorities did not cover the case, which led to the experienced huge public concerns.

As the headline suggests this study focuses on the role of internet in the amplification process. In our today's information society this could play a key role, because the "[...] internet can be used effectively to mobilize public attention to risk issues [due to] its universal accessibility and quite low cost." [2]. But the downside is that also information with disputable credibility can easily be made availaible to thousands of people and remarkably shape the societal response to a risk issue. The evaluated data was "[...] collected from the online edition of a major newspaper" [2], the attached comments and "message boards on the websites of public and nonprofit organizations" [2]. Theses sources functioned as social stations as introduced by the conceptual framework. Their content was filtered by the inclusion of at least two of the following search terms: "Mt. Cheonseong", "Jiyul" and "high speed railway". The indicators used to measure the attentation amplification process were: The number of newspaper articles and message board posts, content of the newspaper comments and number of visits to the message board posts [2].

The examined time period was divided into four parts, whose beginnings were marked by the four hunger strikes. The total number of articles and posts, as well as the number of comments and visits reached a local maximum, when a hunger strike occured. Both indicators measured "[...] a similiar pattern of amplification with a different intensity" [2] and clarified that there was a strong correlation between the occurrence of those events and the selected measures. Furthermore the level of those peaks increased from one to the next hunger strike and altogether "[...] showed a pattern of impulse waves with increasing amplitudes" [2]. These waves visually illustrate the before mentioned rippling effect, while the scope of the risk event expands. The study also measured the public attentation on each station's website independently and discovered that they "[...] showed different patterns in terms of time and intensity" [2]. For a detailed view on the individual analysis of the station, please refer to [2].

The risk signals are another interesting aspect, which were used to transmit the risk to people in an easy understandable manner. The first risk signal was the "endangered species" which was stressed by the cry for help to preserve the protected species, living in the mountain's ecosystem. The second risk signal, the moral sancity of nature, even reinforced the first one, by emphasizing that the tunnel construc-

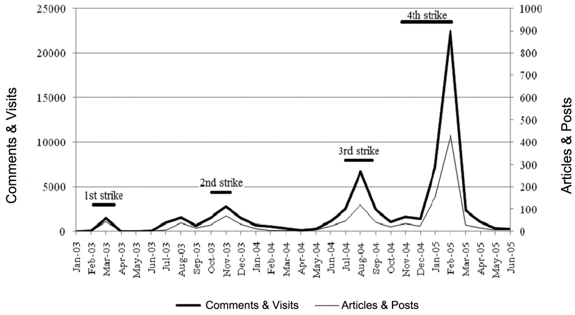

Figure 5: Amplification of public attention [2].

tion will destroy the salamanders' habitat. Where at the salamander served as representative for the 30 endangered species. The election campaign of the president promised to cancel the construction project, but did not come up to that promise. So the third signal, namely political distrust, evolved from this situation. Finally the last signal, a more spiritual one, was motivated by Jiyul who went into a hunger strike for four times and ultimately announced that she will sacrifice her live in order to save the salamander, which gave this signal the denotation "Jiyul and Salamander-Oneness". The consequence of this dramatic event was that the public attention amplified by a shift of the public concern from "Save the salamander" to "Save Jiyul" [2].

This research impressively shows that the internet, strictly speaking, a online newspaper and several organizational message boards, could act as social stations and the interactions among them "[...] clearly demonstrated an amplifying process of public attention" [2]. "Due to its interactive openness, the internet allowed lay publics to become active communicators whose voices are critical to risk amplification" [2]. This amplification process expanded from local to national levels and caused more and more public concern. However it could be discussed, if the delay of a tunnel construction project represents a significant threat to the resiliece of the railway infrastructure. Nevertheless this use case reveals the role of the internet as a social station in the amplification process and succesfully identified several indicators.

Furthermore the distribution of information is a fundamental aspect of the internet. It allows to easily collect and spread knowledge, e.g. about risk events. But without an expert, who is able to exploit a vulnerability, public attention will be attracted less or not at all. However the internet also simplified the exchange of information about vulnerabilities, tools and potential attack methods. Hence it does not only play a role as social station in the amplification process of the perceived risk, it also enhances the actual risk through providing more information about attack methods and thus creating more expertise.

4. INFLUENCES OF SOCIAL MEDIA ON RISK PERCEPTION

In the time of social media networks there are barley obstacles which could limit the distribution of risk information. Everybody could easily create posts and share arbitrary information with a huge, possibly international, scope. The next step of the hypothetical example in Section 2.3.2 could be the attraction of news and media to the security issue of the smart meter. Thus the ripple effect would already have reached a national, at least regional, scope. In the context of social media other indicators have to be utilitzed to measure the impacts or amplifying effects. The already explained concept of the number of articles, comments and views can easily be transfered to the social media context. But there is more potential beside these indicators, social networks often provide the possibility of geo-tagging on their smart phone applications, which additionally makes the current position of the user available. Hereby future studies have the chance to analyse the geographical amplification process with the help of real position information. Whereas geographical amplification describes the ripple effect from a local to a more global scope. Furthermore the network of friends provide the possibility of understanding how risk information spreads over the direct and indirect connections between friends and at which connection level the ripple effect reaches its limit.

5. CONCLUSION

By recapitulating the smart grid example from the introduction the necessity of a profound method to measure and especially forecast social amplification processes becomes obvious. Many companies invest a huge amount of capital in the development of this new technology and governments support the implementation of the smart grid, since a quick change to green energy is planned, which greatly depends on the successful establishment of the smart power grid technology to ensure the resilience of the whole future power grid. If the exemplary concerns of the computer scientist would have further amplified and eventually reached a global scope, the impacts of such an event would not be possible to predict. But for a useful application of the conceptual framework of social risk amplification more indicators are needed to accuratetly measure the amplification process throughout all the different channels. I propose to term these indicators social risk indicators (SRIs), in analogy to the key performance indicators (KPIs) from the business studies. In general a key performance indicator is a number, which denotes the success, performance or workload of a single organizational unit or a machine [11]. They are mainly used to forecast a company's development, to reveal problems and steer the company. In accordance to this definition SRIs could be used to forecast the development of a risk event and interfere its impending course. The detection of more SRIs and espically their forecasting quality is future work.

Another subject, which has to be discussed in the future, is what to do if an amplification process or its trend was recognized? How could the impacts of such an event be diminished or extinguished? The framework of social risk amplification mainly focuses on the explanation of how minor risk events could cause unpredictable impacts. Besides that it is also important to establish methods to reduce the risk that an amplification process arises. It has to be stated out, that the expert's probability estimation of the risk event might be wrong, but the perceived risk of the general public might differ even stronger from the real probability. One possible solution is to replace the public's uncertainty with more profound risk estimations of scientists, which are ideally not involved in the specific event or project. With this help lay people could determine the real benefits and drawbacks of a project. Consequently a following discussion allows to establish a scale of risks, which should be adressed stronger with technical solutions.

In conclusion the conceptual framework of social risk amplification represents an essential extension of the conventional risk analysis, especially with regard to the influence of social networks on the amplification processes, but the methods to actually measure and forecast the risk amplification are not sufficiently matured to be applied in practice and further research is necessary.

6. REFERENCES

[1] Andersson, G. and Donalek, P. and Farmer, R. and Hatziargyriou, N. and Kamwa, I. and Kundur, P. and Martins, N. and Paserba, J. and Pourbeik, P. and Sanchez-Gasca, J. and Schulz, R. and Stankovic, A. and Taylor, C. and Vittal, V. Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance. *Power Systems, IEEE Transactions on*, 20(4):1922–1928, November 2005.

[2] I. J. Chung. Social amplification of risk in the internet environment. *Risk Analysis*, 31(12):1883–1896, 2011.

[3] R. L. Church, M. P. Scaparra, and R. S. Middleton. Identifying critical infrastructure: The median and covering facility interdiction problems. *Annals of the Association of American Geographers*, 94(3):491–502, 2004.

[4] Covello, Vincent T. and Mumpower, Jeryl. Risk analysis and risk management: An historical perspective. *Risk Analysis*, 5(2):103–120, 1985.

[5] Department of Health and Human Services - USA. Basics of risk analysis and risk management. *Centers for Medicare & Medicaid Services*, 2(6), 2005.

[6] Fangxing L. and Wei Q. and Hongbin S. and Hui W. and Jianhui W, and Yan X. and Zhao X. and Pei Z. Smart transmission grid: Vision and framework. *Smart Grid, IEEE Transactions on*, 1(2):168–177, Sept. 2010.

[7] Kahneman, D. and Tversky, A. Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2), March 1979.

[8] Kasperson, Roger E. and Renn, Ortwin and Slovic, Paul and Brown, Halina S. and Emel, Jacque and Goble, Robert and Kasperson, Jeanne X. and Ratick, Samuel. The social amplification of risk: A conceptual framework. *Risk Analysis*, 8(2):177–187, 1988.

[9] Liu, Deepa Kundur Xianyong Feng Shan and Butler-Purry, Takis Zourntos Karen L. Towards a framework for cyber attack impact analysis of the electric smart grid. 2010.

[10] P. McDaniel and S. McLaughlin. Security and privacy challenges in the smart grid. *Security Privacy, IEEE*, 7(3):75–77, May/June 2009.

[11] D. Parmenter. *Key performance indicators (KPI): developing, implementing, and using winning KPIs.* John Wiley & Sons, 2010.

[12] Public Safety and Emergency Preparedness Canada. *Ontario–U.S. Power Outage—Impacts on Critical Infrastructure.* Incident Analysis, Edmonton, 2006.

[13] Sanaye-Pasand, M. and Dadashzadeh, M. R. Iran national grid blackout, power system protection point of view. In *Developments in Power System Protection, 2004. Eighth IEE International Conference on*, pages 20–23. IEEE, April 2004.

[14] U.S. Department of Commerce and National Institute of Standards and Technology. Guide for conducting risk assessments - revision 1. *NIST Special Publication*, 800(30), September 2012.