Internet Science
Risk, Risk Perception, and Cyberwar

Hubert Soyer
Betreuer: Dr. Heiko Niedermayer
Seminar Innovative Internet-Technologien und Mobilkommunikation SS 2013
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: soyer@in.tum.de

ABSTRACT

The rapid speed of computerization in all aspects of life renders us more and more dependent on elements of electronic infrastructure. At the same time, it opens up and widens a space of possible attacks on this backbone of our society. Direct impacts like power outages, water outages or even structural damage on critical systems are not the only consequences of possible attacks. Public reactions to this first level of events can ripple and cause a chain of instances that can even dominate and surpass the original problems. The comparably quick renewal cycle of technology provides an excellent opportunity to rapidly adapt to new technical aspects of security as well as discoveries in psychological and cultural research regarding the public perception of risk.

This paper will utilize the Stuxnet cyber incident and its consequences to point out possible measures that could be incorporated in the design of future systems.

Keywords

Risk, Risk Perception, Cyberwar, Social Amplification of Risk, Psychometric Paradigm, Stuxnet

1. INTRODUCTION

Every day, we voluntarily trick our mind without even consciously noticing it. We reduce the information that is constantly fired at our senses with a set of filters that has been trained by external and internal forces since the earliest days of our childhood.

This interpretation of information starts at a very technical level when a set of small and adjacent pixels becomes an image to our eyes and ends at a very high level where prejudices, opinions and input that is pre-filtered by media shape our perception of public events.

If we watch a movie we usually don't spare a thought for the fact that what we see is actually just a sequence of images played at a sufficiently high speed to make us believe it is movement. With 3D Cinema becoming more and more popular this deception has even entered another dimension and emerging devices like the Oculus Rift which aim at providing the user with an even more credible virtual reality demonstrate how far perception can be moved from reality from a technical point of view.

This gap between perception and reality not only exists at a rather low, technical level. When in March 2011 radioactive material was released by nuclear reactors of the Fukushima Daiichi power plant as a consequence of a fatal earthquake followed by a tsunami, the subject was covered by media all over the world for weeks. The public perception of this catastrophe was influenced so strongly that in Germany, people started buying iodine pills and Geiger counters [1] to protect themselves from the nuclear fallout although this fallout could by no means reach the country which is almost 9000 km away from the location of the accident.

The examples above, whether coming from visual perception or risk perception, illustrate that the human perception of almost anything is in some way filtered and biased. Given appropriate ways of measurement and sensing, perception could be taken into account for the design of future systems, computer programs or infrastructure and for the development of strategies in case of accidents or public events.

In the following, several approaches that aim to explain and measure public perception of risk will be introduced and it will be demonstrated how those approaches can be applied to a scenario often referred to by the media as ”cyberwar”. A psychological approach as well as an anthropological view on risk perception will be described and later, parallels will be drawn to elements of an interdisciplinary approach, the social amplification of risk framework. Further, actual technical risks of attacks on critical infrastructure will be shown next to the perceived threats and a simple set of suggestions that could be taken into account when designing future systems will be provided.

2. THEORIES OF RISK PERCEPTION

”How safe is safe enough?” is the title of a paper by Fischhoff et al. [13] and sums up the basic idea of the measurement of risk perception really well.

The perception of risk is very subjective and different from individual to individual. Objective opinions of experts on the seriousness of a threat often deviate from lay people's views [13]. In order to manage, react to and shape those views and design systems that take this subjectiveness into account right from the start, methods for measuring those perceptions are imperative.

The first methods to assess what subjective risk people perceive go back far beyond the year 0 [8] and have been refined from different angles and inspired by different fields of research ever since. The most prevalent candidates today look at risk from a psychological point of view and an anthropological/cultural point of view. These two directions have

doi: 10.2313/NET-2013-08-1_15

been fused to an interdisciplinary approach, the social amplification of risk framework.
In the following, the basic ideas of the previously mentioned three models of measurement will be covered.

2.1 Psychological Approach

In 1975, Kahneman et al. [19] introduced a paper on how every human uses heuristics to assess situations that he has only limited information about or where he can not fully process all available information. It is one of the earliest pieces of psychometric research and forms the basis the psychometric paradigm, a psychological framework that is prevalent today.
Kahneman et al. performed a set of gambling experiments and tried to determine how people process probabilities. They found out that their testing subjects used a number of heuristics to handle incomplete information. Since that means applying a rigid set of rules to possibly complex problems, this way of decision finding can be inaccurate in which case a so called ”cognitive bias” arises, a deviation from the best decision caused by an oversimplification and wrong interpretation of information. The identified heuristics were clustered into several groups. The following listing of those groups is not exhaustive but only contains some representatives for each group.

2.1.1 Representativeness

”What is the probability that object **A** belongs to [originates from, is generated by] object **B**”?[19] Confronted with this question, people tend to judge by how similar **A** is to **B** or how representative **A** is of **B**.
When people were asked to guess the occupation of a person based on a description of the person’s character, they assigned that job who’s stereotype best fitted the character profile. For example a quiet, shy person was therefore assumed to be a librarian rather than a salesman. However, ”this approach to the judgment of probability leads to serious errors, because similarity, or representativeness, is not influenced by several factors that should affect judgments or probability” [19]. Kahneman et al. identified a number of factors that don’t have influence on representativeness but on the other hand do have influence on probability.

- Insensitivity to prior probability: Being asked to judge whether someone is a salesman or a librarian based on a description of their personality, people should take into account that there are more salesmen than librarians and it is therefore more likely that the occupation they are supposed to guess is a salesman.
- Misconception of chance: People expect that a process that is supposed to be random will only produced irregular results. For example they will assign a regular appearing sequence of heads and tails in a random coin flip experiment a lower probability than a sequence that doesn’t have obvious regularities.
- Illusion of validity: The confidence that people have in their predictions depends on how representative they think their input was. For example: They have great confidence that a person is a librarian when the description of his character displays all the stereotypical attributes of a librarian although this assumption is based on a very shaky foundation.
- Insensitivity to predictability: People often don’t take into account how much the available information is based on facts and therefore how well they can utilize this knowledge in their predictions. For example: When asked to predict the stock price of companies, a high value was strongly correlated with how much the description of a company was in its favor and how nicely written it was, although there were no facts relevant to the stock price contained in those descriptions.

2.1.2 Availability

When asked to estimate the probability of an event that people are remotely familiar with, they often make their guess based on the number of instances they can recall.
”For example, one may assess the risk of heart attack among middle-aged people by recalling such occurrences among one’s acquaintances” [19]. People draw those conclusions not only from their memory but also based on what they can imagine could make a particular event happen. If people can think of a lot of difficulties that would make for example a project fail, they will estimate a high probability for the project to turn out negative.
Kahneman et al. refer to this phenomenon as availability heuristic.
The availability heuristic has some inherent flaws. Every person usually knows only a very limited set of instances he can draw from and those are mostly heavily biased by people’s individual environment. Even setting this problem aside, Kahneman et al. identified several more biases.

- Bias due to the retrievability of instances: Since our memory works very selectively, we will remember more instances of classes that seem more interesting to us. This introduces a bias if we use the frequency of recallable instances as a measure for the probability of an event. For example familiarity, popularity or salience influence how well we can recall certain instances of an event.
- Biases due to the effectiveness of a search set: Our brain can not recall all terms or instances equally well. When participants were asked whether there are more words starting with the letter ”r” or with the letter ”r” as the word’s third letter in written English, the participants tended towards the first choice since our brain is better at searching for words using the first letter as a criterion. However, there actually are more words containing ”r” as their third letter in written English.
- Biases due to imaginability: When people don’t have a memory of a specific event that they could draw from, they imagine possible instances and evaluate the probability of an event based on their frequency. However, we imagine certain scenarios more easily than others which introduces another bias.

2.1.3 Adjustment and Anchoring

When estimating a quantity, people tend to start from an initial, simple guess and adjust this guess to yield the final answer. Usually, this adjustment is not sufficiently large and different starting points lead to different estimations. Kahneman et al. refer to this phenomenon as anchoring.

2.1.4 Experts' Biases

Although experts possess more knowledge on their field than lay people, they still rely on heuristics. Studies investigated in [19] indicate that experts' estimations can suffer from overconfidence regarding the accuracy of the predictions and the experts in those studies often put too much credit in small sets of samples although they certainly knew that due to the size of those sets they were by no means representative of the whole of instances.

2.2 Psychometric Paradigm

> "One broad strategy for studying perceived risk is to develop a taxonomy for hazards that can be used to understand and predict responses to their risks. A taxonomic scheme might explain, for example, people's extreme aversion to some hazards, their indifferences to others, and the discrepancies between these reactions and opinions of experts. The most common approach to this goal has employed psychometric paradigm [...], which uses psycho-physical scaling and multivariate analysis techniques to produce quantitative representations or 'cognitive maps' of risk attitudes and perceptions." [18]

This quote from a work of Paul Slovic, one of the key researchers and developers of the psychometric paradigm introduces the framework quite nicely.
In practice, employing the psychometric paradigm usually means carrying out a survey that aims at collecting information on a set of qualitative properties of risks and analyzing it. Common qualitative properties of risk are for example:

- voluntariness: to what degree take people a particular risk voluntarily?
- controllability: how controllable is the risk?
- immediateness: how immediate are the consequences? Are they delayed?
- danger to future generations?
- global or local consequences?
- · · ·

and many more (see [18, 14, 15] for more examples). Typically, around 20 of those properties are determined and then processed by a dimensionality reduction technique like factor analysis to reduce the number of dimensions to only a few. "The resulting components or factors are given interpretive names (e.g., dread risk, unknown risk) and used as independent variables in regressions to predict mean ratings of riskiness or acceptability." [6]. Using this method, some studies have for example been able to establish a correlation between the controllability of the consequences and the public perception of the risk of an event [18].

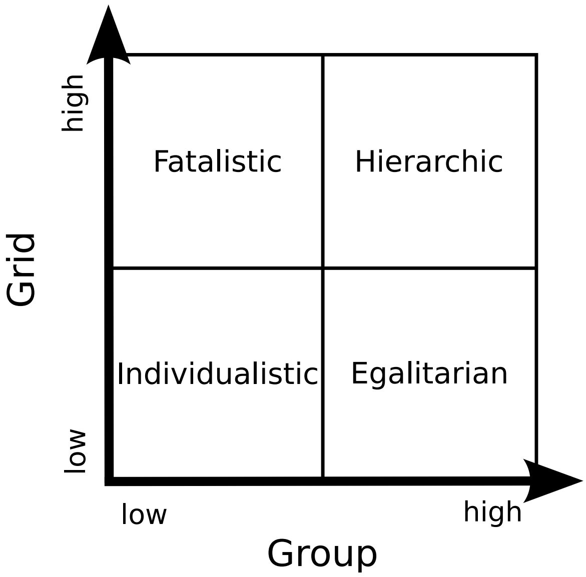

Figure 1: Group-grid scheme [10, 5]

2.3 Anthropological/Cultural Approach

In contrast to the psychological approaches described in the previous chapters, the "Cultural Theory of risk"[11, 10], the most prevalent anthropological view on risk perception focuses on influences of society on individuals' perceptions rather than cognitive aspects.
According to this cultural theory people associate harmful or risky events with changes in society. The aversion of risk therefore originates from an inherent societal desire for stability and individuals or events that have the potential to trigger changes provoke dismissive behavior.
Douglas et al. [10] attribute different perceptions of risk and positions in societal discussions to a group-grid scheme that defines different ways of life based on peoples' view on nature and individualism. Depending on the social group a person belongs to he perceives threats that could lead to a change of the properties of this social group as a risk.
The group-grid scheme is drawn along the axes group and grid as shown in figure 1 where the dimensions are defined as follows

- Group: "group refers to whether an individual is member of bonded social units and how absorbing the group's activities are on the individual" [5]
- Grid: "grid refers to what degree a social context is regulated and restrictive in regard to the individuals' behavior" [5]

2.4 Interdisciplinary Approach: Social Amplification of Risk Framework

While the psychological approach mainly focuses on people as individuals, the cultural theory of risk concentrates on persons as part of a society. Research proves that both approaches are legitimate but yet don't seem to fully cover all factors involved in risk perception. To broaden the view

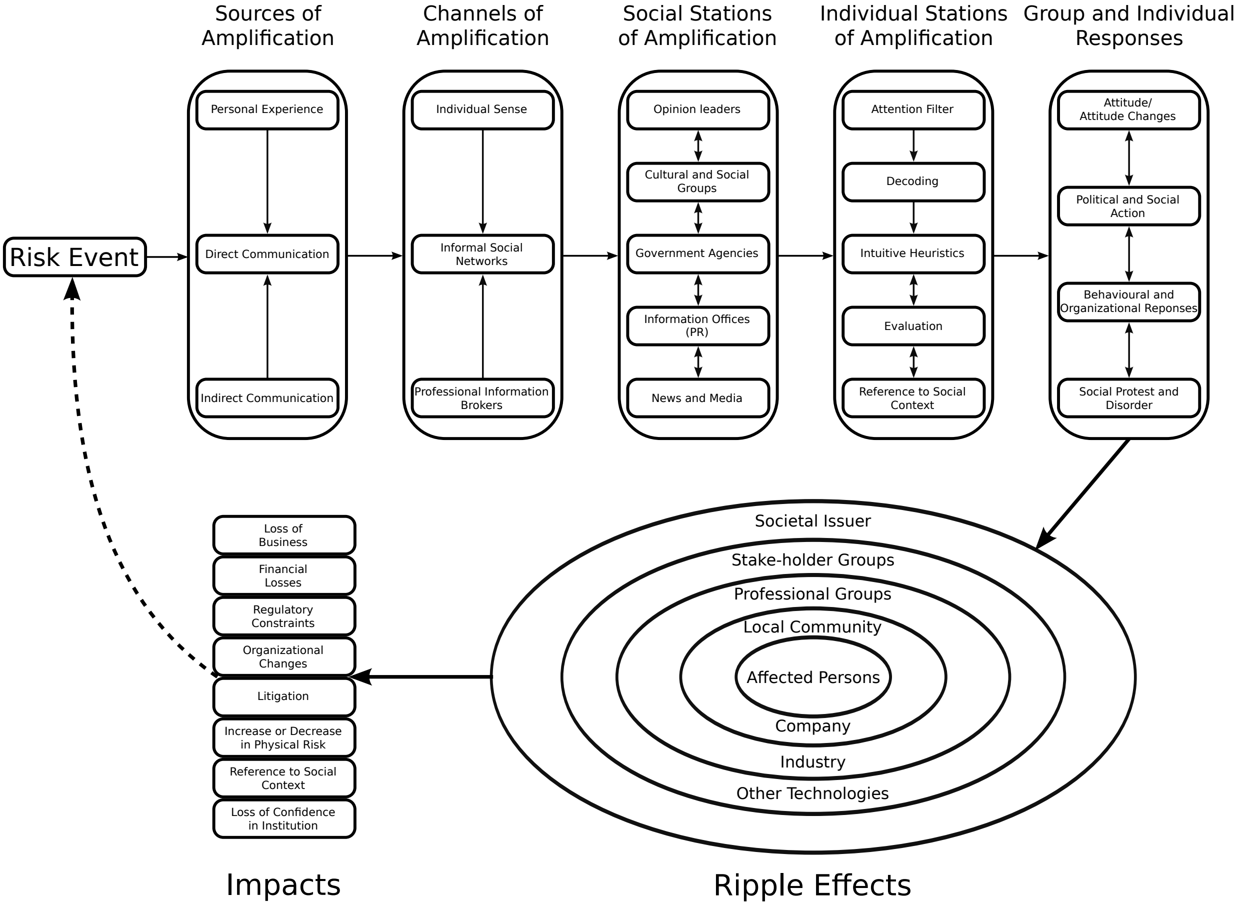

Figure 2: Detailed schematic of the Social Amplification of Risk framework [16]

Kasperson, Slovic (one of the key researchers behind the psychometric paradigm) and colleagues introduced the social amplification of risk framework [16] which integrates many different backgrounds including psychological, cultural and communication theoretical ideas.

> The main thesis is that hazards interact with psychological, social, institutional, and cultural processes in ways that may amplify or attenuate public responses to the risk or risk event. [...] The amplified risk leads to behavioral responses, which, in turn, result in secondary impacts."[16].

Along the way of information from objective evidence to its final receiver, Kasperson et al. [16] identify several stages where the meaning of a message can be intensified or attenuated.
Signals and their senders and receivers are not independent. When a message is passed along a chain of senders and receivers, each station interprets the contained information in a sociocultural context that depends on its own prejudices, its perception of the sender and other cultural influences. It decodes the message, links it to its own values and reencodes it before forwarding it to the next receiver thus possibly changing the view on the underlying factual evidence. Whether for example news or opinions on an event originate from respected, independent entities or parties that are in some way involved in this event strongly influences the credibility of those news. Facts repeated by multiple sources are perceived as more important. There are many factors that can shape the perception of information, "amplification of signals occurs during both transmission and reception" [16]. In [16] the authors hypothesize that at each social amplification station, risk information is processed in the following manner

- Filtering and decoding of a signal
- Processing of risk information (using heuristics to estimate chances and probabilities that go along with the information, see chapter 2.1)
- Attaching social values to the information
- Interacting with their social groups and environment about the information
- Considering possible behavioral responses
- Acting on the previously considered behavioral intentions either in groups or individually

The final stage in this process, acting out behavioral responses, has the potential to itself become a new risk event and pose a threat which in turn may trigger a similar process as the one it originated from. Kasperson et. al refer to those events as "secondary impacts" [16]. Examples of secondary impacts include

- Local impact on sales or property value
- Governments reacting to a threat by enacting or altering regulations
- Changes in insurance costs
- Influence on the perception of public institutions

Those secondary impacts undergo the same processing as the first-order impacts and can again result in new impacts. This course can repeat over and over and "spread, or 'ripple' to other parties, distant locations, or future generations" [16]. Learning, social interactions and experience make the social amplification of risk a very dynamic concept. Figure 2 illustrates a detailed schematic of this process.

3. CYBERWAR: RISK AND REACTION

The Oxford dictionary defines *cyberwar* as

> The use of computers to disrupt the activities of an enemy country, especially the deliberate attacking of communication systems.

However, the word cyberwar is often also understood not only in the context of attacking communication systems but technical infrastructure in general. With more and more systems becoming computerized and being made "smarter", the number of potential targets for this kind of attacks has been increasing steadily and ranges from local company computer networks via critical systems in entities responsible for basic services like water to huge emerging infrastructural elements like the intelligent smart grid power supply network.

The concept of warfare via information infrastructure was for the first time discussed almost as early as the first systems started incorporating technology elaborate enough to be potentially vulnerable.
Since then, the topic of cyber attacks has gained more and more momentum. Already in 2001, Ralf Bendrath wrote

> 'Cyberwar' has become a growth market in the US. While ten years ago the term would hardly have made sense to any expert, in the meantime attacks on computer networks and their implications for national security have received broad coverage in the media. In the broad range of service providers from technical security solutions to policy advisory groups, a whole cottage industry has sprung up. [4]

Nowadays, most countries consider cyber attacks a serious threat and have erected their own cyber defense forces. While military and political leaders started monitoring cyber activity very early on, there have been only comparably few reports on the actual execution of events that could be interpreted as strategic acts of cyber war. Even less so have those activities reached the main stream media and come to broad public attention.
The lack of main media coverage and information in the civilian population has made case studies not very appealing. To the knowledge of the author, no large scale systematic surveys on the public perception of risk in context of cyber warfare or attacks have been carried out to date.
Numerous reasons might have contributed to this lack of research.
Viewed in a historical context cyber warfare is a very recent development and differs in many aspects from traditional warfare. "Compared to the traditional security threat, which consists of the dimensions actor, intention, and capabilities, 'cyberwar' threats cannot easily be categorized"[4]. Effective techniques to cover up tracks often render victims unable to identify their attackers or even their locations. An attack could originate from a single individual, a group of activists or the military of a foreign nation. Only very few indicators, like the level of sophistication, might help narrow down the list of possible offenders but by no means far enough to pin down the perpetrator with certainty. Without knowing the attacker determining his intentions is generally not possible either and causes the attackers capabilities to remain unclear as well. While differing from traditional warfare, cyberwar shares some factors with terrorism like the anonymity with which attackers can act or the difficulty to determine the leaders coordinating the strikes.
Denial of Service attacks between 2007 and 2009 on the former Soviet Union states Kyrgyzstan, Georgia, and Estonia, where the attacker flooded infrastructure with a large number of requests it couldn't handle, have made it to the front pages of a number of high profile, high circulation news papers [9]. But arguably the most famous act of cyberwar has been the Stuxnet incident in 2010.
Exemplified by the Stuxnet incident and the measures taken at a UK water company as a consequence of that incident, it will discussed what vulnerabilities Stuxnet exploited and conclusions on what aspects should be taken into account when designing and implementing new critical infrastructure will be drawn.

3.1 Technical Aspects of Stuxnet

Stuxnet [17] is a computer worm, a program that infects computers and from there, spreads to other systems and computers. It was first discovered by the security company VirusBlokAda in 2010 and has since been spreading and circulating in several variants. The origin of this malware has never been confirmed officially but evidence is piling up that the United States of America and Israel designed and developed Stuxnet to delay the Iranian nuclear program. The sophistication and the fact that Stuxnet only attacks a very specific set of targets imply that it was tailored for a very specific purpose.
Details on how Stuxnet works will illustrate and support this hypothesis.

1. Stuxnet's first stage of infection are Windows PCs. It exploits four zero-day security holes. Zero-day security

holes are vulnerabilities in software that have been exploited for the first time in this worm and have not been publicly known previous to that. This makes them very valuable and thus the use of four of those exploits in one worm is very uncommon. Stuxnet can enter computers through various different means like USB drives, a local network or the Internet. The worm acts on both, the user and the kernel level of Windows. To avoid raising any flags when entering the kernel-mode by registering as a device-driver, the driver was signed by previously stolen, official certificates from well known companies.
Stuxnet spreads quickly, yet never distributes itself to more than 3 computers from each machine and stays relatively harmless and inactive if the Windows system does not meet very specific configuration requirements.

2. The second stage consists of finding and infecting project files of the Siemens SCADA control software on the affected Windows PCs. Stuxnet manipulates those files in a way that enables the worm later on to intercept the communication between the Windows PC and a Siemens programmable logic controller (PLC) and install another malware on the PLC.

3. In the third and final stage, the malware on the PLC device activates if particular criteria match which apply to certain pumps or gas centrifuges controlled by those PLCs. It modifies the frequency and thereby affects the rotation speeds of the controlled motors possibly leading to their destruction.

The vast majority (60 %) of infected systems were reported in Iran. This fact and the specificity of targets, the high degree sophistication and the obvious benefit of a delayed nuclear program in Iran for the USA and Israel leads experts like Ralph Langner to believe that the nuclear facilities in Iran were Stuxnet's intended target [3].

3.2 Lessons Learned from the Stuxnet Incident

The coverage of Stuxnet in western main-stream media was rather a distant view than fueling fears of a possible threat and the public perception of risk therefore remained relatively modest. Yet, this incident demonstrates that strategic cyber attacks are indeed possible and realistic and could happen on the territory of any arbitrary country and therefore, new systems related to critical infrastructure should be designed to take risks arising from cyber attacks into account right from the start.

3.2.1 Effects of Stuxnet on the Security Policy of a UK Water Company

Faily et al. describe in [12] how to balance security versus usability by employing requirements engineering in the case of a UK water company which purifies dirt water and feeds it back to the hydrologic cycle. Lacking real world penetration of the infrastructure, there are several ways to evaluate security reaction strategies. In order to yield an evaluation which is as close as possible to a real world scenario, Faily et al. chose to carry out the study as an Action Research intervention. "Action Research is an iterative research approach involving the planning of an intervention, carrying it out, analyzing the results of the intervention, and reflecting on the lessons learned; these lessons contribute to the re-design of the social action, and the planning of a new intervention."[12]
The methodology breaks down to 5 points

1. Diagnosis: Identifying key factors in the design of the intervention

2. Plan actions: Adapting or planning a process the fits the intervention's objectives

3. Execute actions: Take the actions as planned in the previous step

4. Evaluate: Evaluate the results

5. Identify actions worthy of propagation to become topics of further research

In the diagnosis phase, Faily et al. managed to pinpoint several factors that can cause serious security risks and most likely appear not only in the UK water company (from here on referred to as ACME) they investigated but also in other areas of critical infrastructure.

- Like probably many other companies, ACME put trust in the security through obscurity principle. By not releasing any specifics about their proprietary systems, some manufacturers and their clients trick themselves into believing this would protect their product from attacks. Stuxnet has successfully implanted itself in the proprietary Windows operating system as well in a proprietary controlling system by Siemens and therefore demonstrated what many experts have been preaching all along, that the security through obscurity method is not reliable.

- Critical systems within infrastructure entities like power plants are usually physically disconnected from the outside world. This is effective against intruders from the Internet, however, attackers could abuse virtually any electronic device nowadays (USB devices, mobile phones) that is capable of interacting with computers inside the security perimeter to smuggle in malware.

- Before the Stuxnet incident, ACME had never taken into consideration that they could be a potential target for a cyber attack and therefore would have been relatively unprepared to a real strike. Accordingly, the consequences of a cyber strike had never been thought of in detail.

The measures proposed to the water company as a result of the study focus mainly on tackling the points presented above. Restricting access of external contractors to computers, prohibiting the use of USB devices inside of the facility and working out possible attack scenarios are on the list of suggestions.

3.2.2 General Lessons and their Application

Stuxnet demonstrated how limited technical security measures can be and that any system is vulnerable if the attacker is resourceful and sophisticated enough. It is impossible to account for all unavoidable variables like third-party software that could contain unknown security holes or carelessness of staff while handling computer systems or external devices. Therefore, the public perception of risk following a potentially successful cyber attack and its possibly fatal and harmful consequences like riots should find consideration in the system already in design and implementation.
It is evident in Ik Jae Chung's [7] that poor information policy can cause social ripple effects as described in the social amplification of risk framework (chapter 2.4). Anticipating whether a particular event will cause ripple effects is hardly possible. It depends on a number of factors like group dynamics and individuals (in [7] a woman who went on several hunger strikes) that are not predictable. However, recalling the psychological, anthropological and interdisciplinary approaches introduced in previous chapters, a couple of simple measures could help contain the damage

- Evidence of precautionary arrangements, even if they were not enough to prevent an incident, can take the wind out of activits' sails and prevent anger from rippling and spreading
- As stated in chapter 2.1, people use heuristics based on their memory of preceding, similar incidents to estimate the risk of an event. Learning from previous incidents and being able to credibly convince the public that earlier problems have been taken seriously is a powerful argument.
- Working out general reaction plans to possible attack scenarios
- Avoiding the security through obscurity principle
- Anticipating the consequences of possible attacks
- Communicating openly and consulting independent experts

Having elaborated a lot on general rules, the question remaining is how to put them into concrete terms.
An Example: Imagine a case where a company responsible for critial infrastructure finds out that they have been infected by the Stuxnet worm. Since this paper focuses on risk perception management, most of the technical aspects regarding the removal of the worm will be left aside and the application of the Social Amplification of Risk framework to this case will pose the focus.
How can a company react in the scenario described above?
Figure 2 includes several elements like "Personal Experience", "Individual Sense" or "Informal Social Networks" which are developed by each individual differently and over a long term and thus hardly allow for any form of control from the outside. Also, "Group and Individual Responses" are heavily complex and dynamic processes that it is difficult to excert directed influence on. They are relevant at a stage where opinion-forming is already completed.
The stages our example company should focus on are "Social Stations of Amplification" and in particular "Individual Stations of Amplification". The former stage directly includes "Public Relations" departments of companies and the latter stage can be approached utilizing insights from the chapters 2.1 and 2.2.
Concretely, a possible reaction, organized by the elements of the Social Amplification of Risk framework, might look as follows:

Social Stations of Amplification

- Information Offices (PR)
  - Company's way to shape people's emotions about the company through the use of Public Relations tools like advertisement
  - Rather a long term instrument than suitable for an immediate response to an incident
  - Should be used to associate the company with positive values like trustworthiness and openness
- News and Media
  - Can react quickly and exert strong influence on peoples' opinions
  - Handling of media determines the way they report about incidents which in turn is taken on by most people
  - A closed information policy can affect media coverage very negatively (see Fukushima Daiichi incident [2]), for our Stuxnet example this means keeping the media up-to-date about progress regarding working on a solution with the vendors (Siemens)
  - ⇒ be open about possible consequences and risks with the big players in media but careful regarding possibly resulting mass panics
  - ⇒ work closely together with selected, responsible media institutions
  - have independent experts confirm statements for more credibility, experts like Ralph Langer were intrigued by the degree of sophistication of Stuxnet

Individual Stations of Amplification

- All items in this group are connected to heuristics as described in 2.1
- Key insights and possible steps to take:
  - Memory of previous instances that are similar to the current incident strongly influences peoples' opinions
  - Point out differences to previous instances and present the incident as diverse to prevent people from easily putting it into predefined risk categories. There has arguably never been a worm as sophisticated as Stuxnet before
  - Illustrate possible risks with examples to avoid "misconception of chance"

– Work with positive examples to influence "biases due to imaginability", for example point out that the worst case in the Stuxnet example would be shutting down the motors and replacing them with different models from different vendors

– Since peoples' perception of risk is prone to "adjustment and anchoring", be very thorough and careful with your very first reporting of the incident since it will serve as an anchor for everything that follows

Despite taking measures affecting the public perception of risk, people might also be able to actively contribute to preventing cyber attacks. Raising awarness about dangers in cyberspace leaves users more conscious regarding the technical risks and even though the chances are miniscule, it may lead some versed users to actually detect anomalies on their systems or at least make the masses keep their virus scanners up-to-date. Although Stuxnet was only active on computers with very specific properties, it spread via a multitude of normal PCs. Normal users did not play an active role in this cyber attack, yet, they still were cogs in the machinary that made the Stuxnet incident possible.

4. CONCLUSION

Reactions to events can intensify and cause a new series of events, possibly with higher impacts than the incident they originated from. This is an important take-away message from the theory of the social amplification of risk framework.

Strategies based on psychological, cultural and interdisciplinary attempts at predicting and analyzing human perception could contribute right from the planning stage to the design of new systems in a way that addresses and recognizes the public perception of risk.

Exemplified by the arguably growing threat of cyber attacks on critical infrastructure, this work showed incidents of cyberwar and their consequences on political views as well as measures taken to prevent them in the future. The speed that drives development and change in the technical world presents an excellent opportunity to react to cyber risks when planning new systems and to learn lessons in respect to communication and handling of the public.

With some countries rumored to specifically hire hackers to put together military cyber forces, the future will certainly bring similar incidents as Stuxnet and it will be interesting to see the state of preparations for and the reactions to those threats.

5. REFERENCES

[1] Augsbuger Allgemeine, Increased Number of Iodine Pills and Geiger Counter Sales. `http://www.augsburger-allgemeine.de/panorama/Jodtabletten-und-Geigerzaehler-sind-begehrt-uebertriebene-Vorsorge-id14280346.html`.

[2] Fukushima Daiichi. `http://world-nuclear.org/info/Safety-and-Security/Safety-of-Plants/Fukushima-Accident-2011/#.Ud_dS4YbwWM`.

[3] Origin of Stuxnet. `http://www.csmonitor.com/World/terrorism-security/2010/1001/Clues-emerge-about-genesis-of-Stuxnet-worm`.

[4] R. Bendrath. The cyberwar debate: Perception and politics in us critical infrastructure protection. *Information & Security: An International Journal*, 7:80–103, 2001.

[5] Å. Boholm. Risk perception and social anthropology: Critique of cultural theory. *Ethnos*, 61(1-2):64–84, 1996.

[6] N. C. Bronfman, L. A. Cifuentes, M. L. DeKay, and H. H. Willis. Explanatory power of the psychometric paradigm: Aggregate and disaggregate analyses. *Santiago, Chile: Pontificia Universidad Catolica de Chile*, 2004.

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

[8] V. T. Covello and J. Mumpower. Risk analysis and risk management: An historical perspective. *Risk analysis*, 5(2):103–120, 1985.

[9] C. Czosseck and K. Geers. A brief examination of media coverage of cyberattacks (2007-present). *The Virtual Battlefield: Perspectives on Cyber Warfare*, 3:182, 2009.

[10] M. Douglas. *Risk and Blame: Essays in Cultural Theory*. Routledge, 2002.

[11] M. Douglas and A. Wildavsky. *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*. Univ of California Press, 1983.

[12] S. Faily and I. Flechais. User-centered information security policy development in a post-stuxnet world. In *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*, pages 716–721. IEEE, 2011.

[13] B. Fischhoff, P. Slovic, S. Lichtenstein, S. Read, and B. Combs. How safe is safe enough? a psychometric study of attitudes towards technological risks and benefits. *Policy sciences*, 9(2):127–152, 1978.

[14] R. Gregory and R. Mendelsohn. Perceived risk, dread, and benefits. *Risk Analysis*, 13(3):259–264, 1993.

[15] C. M. Jenkin. Risk perception and terrorism: Applying the psychometric paradigm. *Homeland Security Affairs*, 2(2):1–14, 2006.

[16] R. E. Kasperson, O. Renn, P. Slovic, H. S. Brown, J. Emel, R. Goble, J. X. Kasperson, and S. Ratick. The social amplification of risk: A conceptual framework. *Risk analysis*, 8(2):177–187, 1988.

[17] R. Langner. Stuxnet: Dissecting a cyberwarfare weapon. *Security & Privacy, IEEE*, 9(3):49–51, 2011.

[18] P. Slovic. Perception of risk. *Science*, 236(4799):280–285, 1987.

[19] A. Tversky and D. Kahneman. *Judgment under Uncertainty: Heuristics and Biases*. Springer, 1975.