3RG REPORT

Focal Report 8: Risk Analysis Using the Internet for Public Risk Communication

Zurich, August 2013

CSS
ETH Zurich

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Contact:
Center for Security Studies (CSS)
ETH Zurich
Haldeneggsteig 4, IFW
CH-8092 Zurich
Switzerland
Tel.: +41-44-632 40 25

crn@sipo.gess.ethz.ch
www.css.ethz.ch

CONTENTS

Focal Reports: The Task

The analysis and evaluation of risks and threats relevant to the civil protection system is among the key responsibilities of the Swiss Federal Office for Civil Protection (FOCP). As part of a larger mandate, the FOCP has tasked the Center for Security Studies (CSS) at ETH Zurich with producing 'focal reports' (Fokusberichte) on risk and vulnerability analysis.

According to this mandate, the focal reports are compiled using the following method: First, a 'scan' of the environment is performed with the aim of searching actively for information that helps to expand and deepen the knowledge and understanding of the issue under scrutiny. This is a continuous process that uses the following sources:

- Internet Monitoring: New and/or relevant publications and documents with a focus on risk and vulnerability analysis are identified and collected.
- Science Monitoring: Relevant journals are identified and screened, and relevant articles evaluated.
- Government Monitoring: Policy documents with relevance to Switzerland from various countries and from international inter- and nongovernmental organizations are identified.

Second, the material thus collected is filtered, analyzed, and summarized in the focal reports.[1]

---

1   Previous focal reports by the Risk and Resilience Research Group can be downloaded from the CSS website at *http://www.who.int/csr/sars/country/en*.

1 INTRODUCTION

This focal report addresses key issues of public risk communication and the Internet. It identifies the main goals of risk communication generically and how they may be achieved using the Internet. In particular, it shows possible strategies of how key elements of traditional risk management can be adapted to the new information environment. It draws on two main sources: On the one hand, scholarly articles on risk communication, in general, and risk communication on the Internet in particular, have been identified and evaluated. On the other hand, Internet and government monitoring focusing on actual (Swiss and worldwide) public risk communication efforts that have used and/or are using the Internet have been identified.

The new information environment comes with opportunities as well as challenges. When information becomes popular and spreads widely and at great speed on the Internet, one speaks of information that has gone 'viral'. The adjective is relevant in three different ways:

- First, the word describes the high speed of the transmission of information from one person to the next.
- Second, 'viral' suggests difficulty of control: It is the image of information spreading on its own, as if the information was itself an organism capable of moving from recipient to recipient by itself.
- Third, the word 'viral' – although also used positively, as in "viral advertisement" – carries a possible negative connotation: Sickness and disease. Thus, false and untrue information or unsubstantiated rumors are also said to spread virally – and they may 'infect' many recipients in a very short time span.

As an example, as the first rumors about a dangerous, lethal disease originating from China began to spread in 2003 during the outbreak of SARS (severe acute respiratory syndrome), something like a worldwide hysteria ensued. This is not to belittle the fact that SARS has led to 916 deaths, officially.[2] But the news reports, rumors and fears that circulated about the disease have often been overblown and exaggerated, from E-Mails and online comments warning citizens of New York from visiting and eating in Chinatown, to countless reports on the imminence of a possible SARS-epidemic in the United States – while in reality, only eight people in the United States had contracted SARS, most of them abroad.[3] Thus, almost at the same time that the disease broke out in China, another epidemic spread virally: It was an "information epidemic", a term used by health and crisis communication analyst David J. Rothkopf which he shortened to the word "infodemic".[4] An infodemic makes a public health crisis harder to control and contain. Rothkopf defines the term infodemic as

> *A few facts, mixed with fear, speculation and rumor, amplified and relayed swiftly worldwide by modern information technologies [...]. [I]t is a phenomenon we have seen with greater frequency in recent years – not only in our reaction to SARS, for example, but also in our response to terrorism and even to relatively minor occurrences such as shark sightings.*

2 World Health Organization WHO (2003): Summary table of SARS cases by country, 1 November 2002 – 7 August 2003. Available at: *http://www.who.int/csr/sars/country/country2003_08_15.pdf* .

3 Eichelberger, Laura (2007): SARS and New York's Chinatown: The politics of risk and blame during an epidemic of fear. In: Social Science & Medicine, 65, 1284 – 1295, 1284 – 85.

4 Rothkopf, David J. (2003): When the Buzz Bites Back. In: The Washington Post, May 11, 2003, B01, available: *http://www.udel.edu/globalagenda/2004/student/readings/infodemic.html*.

In short, infodemics are what risk communication want as much as possible to avoid – or, if they are already happening, to contain. There are scholars who believe the Internet is, by its very nature, furthering infodemics.[5] It lies however not within the scope of this focal report to support or refute such claims. This focal report intends to take a pragmatic approach: Risk communication studies have shown as early as 2001 that people do turn to the Internet in order to find information about current risks.[6] The more connected societies become, the more citizens will also look for information about risks online. Infodemics do exist – one has therefore to analyze how they can best be countered and prevented. It is the belief of the authors that official risk communication can be successful on whatever channels it takes place – be that radio, TV or now also on the Internet. Of course, the Internet can further public skepticism: "All risk websites are potentially equal in Cyberspace, constrained only by the skill of the web designer".[7] The important word here is "potentially": The fact that information from dubious sources can be presented professionally and even convincingly must never prevent official and expert bodies to provide serious and thorough risk information on the web.

The basic rules for successful risk communication stay the same irrespective of the medium in which the communication takes place. This report therefore turns to an analysis of the basic nature of risk communication in Section 2. It focuses on the topic of public risk communication, lists its goals as well as the most common strategies employed to achieve these goals. Section 3 examines risk communication in the information age, exploring some of the main characteristics of the Internet that are relevant for public risk communication. In conclusion, the report shows how traditional risk management may be adapted to the new information environment – thus providing the basis for effective risk communication on the Internet.

5   Berube, David M.; Faber, Brenton; Scheufele, Dietram A.;
     Cummings, Christopher, L.; Gardner, Grant E.; Kelly, Martin N.;
     Martin, Michael S.; Temple, Nicolas M. (2010): Communicating
     Risk in the 21st Century. The Case of Nanotechnology. NNCO
     White Paper, February 2010, available: *http://rit.academia.
     edu/KellyNM/Papers/322606/White_Paper_Communicating_
     Risk_in_the_21st_Century*, 9.

6   Kittler, Anne F.; Hobbs, John; Volk, Lynn A.; Kreps, Gary L.; Bates,
     David W. (2004): The Internet as a Vehicle to Communicate
     Health Information During a Public Health Emergency: A Sur-
     vey Analysis Involving the Anthrax Scare of 2001. In: Journal of
     Medical Internet Research, 6, 1, e8, available: *http://www.ncbi.
     nlm.nih.gov/pmc/articles/PMC1550585*; see also: American Red
     Cross (2010): Social Media in Disasters and Emergencies, ARC
     survey July 2010, available: *http://www.redcross.org/www-
     files/Documents/pdf/other/SocialMediaSlideDeck.pdf*

7   Krimsky, Sheldon (2007): Risk communication in the internet
     age: The rise of disorganized skepticism. In: Environmental
     Hazards, 7, 157–164, 160.

2   GOALS AND CHALLENGES OF RISK COMMUNICATION

Before we discuss how the Internet affects the public communication of risk (Section 3), it is necessary to clarify the concept of risk communication and to sketch out some major trends in risk communication research and practice. Although humans have always communicated about dangers, public risk communication has only quite recently been recognized as a distinct and pivotal task that concerns both private and public organizations.[8] The concept of risk communication as it is commonly understood today became popular in the wake of the rise of technical risk assessments in the second half of the twentieth century.[9] Such risk assessments were supposed to calculate the hazards associated with new technological developments in an objective manner and thereby to counter uninformed and sometimes panicky public sentiments towards technological progress. In this way, operators of nuclear plants, owners of chemical companies and other managers of potentially harmful technological innovations illustrated the controllability of these technologies by applying the classic risk formula developed in the insurance industry. This formula suggests that risk can be defined as the product of the probability of a harmful event and the magnitude of its consequences. Following this approach, it is the purpose of professional risk communicators to educate non-experts on the probability and effects of specific hazardous events with the goal, as Hadden stated, "to persuade laymen of the validity of their risk assessments or risk decisions".[10] The provision of objective risk metrics to the public is expected to increase risk literacy, reduce panic and

panic-fuelled reactions, and finally legitimize those institutions handling the risks.[11]

Today, quantitative risk assessments are widespread in various contexts relating to human and social safety, ranging from epidemiology, to natural hazards, and the management of international terrorism. At the same time, the traditional view that risk communication should *inform* the public about expert risk assessments in an objective and understandable fashion is increasingly criticized as being unsuitable to address the complexities and uncertainties of our time. State actors simply lack the knowledge, the computational capabilities as well as the societal reach to mount the task of risk governance by themselves alone. Therefore, more and more voices promote the utilization of stakeholders and citizens as a resource for risk governance processes, instead of dismissing them as passive recipients of top-down information.[12] Moreover, as research in the fields of psychology, communication science, sociology and other disciplines has shown, there are several limitations to such a purely technical understanding of risk with respect to the public acceptance of risks.[13] At least three fundamental conditions of successful public risk communication militate against the use of technical approaches to risk communication (see Box 1).

---

8   Plough, Alonzo; Krimsky, Sheldon (1987): The emergence of risk communication studies: Social and political context. In: Science, Technology, & Human Values, 12, 3/4, 4–10.

9   Bernstein, Peter L. (1996): Against the Gods. The Remarkable Story of Risk. Wiley: New York.

10   Hadden, Susan G. (1989): Institutional barriers to risk communication. In: Risk Analysis, 9, 301–308, 301.

11   Plough; Krimsky (1987).

12   See e.g. International Risk Governance Council (2009): Risk Governance Deficits. An analysis and illustration of the most common deficits in risk governance. IRGC Report, available: *http://www.irgc.org/IMG/pdf/IRGC_rgd_web_final.pdf*, 19ff.

13   Fischhoff, Baruch (1995): Risk Perception and Risk Communication Unplugged. Twenty Years of Process. In: Risk Analysis, 15, 2, 137–145; Gurabardhi, Zamira; Gutteling, Jan M. & Kuttschreuter, Margot (2004): 'The Development of Risk Communication. An Empirical Analysis of the Literature in the Field', Science Communication, 25, 4, 323–349.

⬥ **People do not judge risks quantitatively:** Numbers do not speak for themselves. Rather, they can be understood as metaphors.[14] Therefore, quantitative risk information has to be interpreted. To use an example, the information that the risk to die in a car accident in the United States is around 1 to 7'000 does not tell us whether to go to work by car or by train. People use risk comparisons, historical analogies, narratives and heuristics to process risk information.[15] These interpretative processes are influenced by personal experiences, cultural norms and other factors that can potentially make the public more risk-averse than experts in some instances, while at the same time disregarding other risks that experts regard as critical.

⬥ **People do not like to be 'enlightened' about risks:** A too technical, top-down approach to risk communication that does not address the needs and fears of the recipients is seldom successful. If people get the feeling that they are merely passive objects of prefabricated, probably even manipulative risk messages, they are likely to reject the message.[16] In recent decades, citizens of liberal societies increasingly expect to be treated as stakeholders in social affairs that affect their lives, and subsequently press for their rights to partici-

pate in political decision-making processes or at least to voice their opinion in public risk discourses. This trend can be expected to continue in the foreseeable future.[17]

⬥ **Without credibility and trust, risk communication does not work:** How people respond to risk messages heavily depends on the amount of credibility and trust assigned to the risk messenger. However, trust and credibility cannot be prescribed or purchased, and Renn warns, "the slightest mistake by the risk management agency can be sufficient to destroy the delicate balance of trust".[18] Building trust is thus a sensitive long-term process that requires an organization to engage constantly in an honest and preferably transparent matter with its stakeholders.

Box 1: Three key challenges for risk communication
⬥ People do not judge risks quantitatively
⬥ People do not like to be 'enlightened' about risks
⬥ Without credibility and trust, risk communication does not work

---

Policy-makers as well as researchers in the field of risk communication have discussed the challenges of technical risk communication extensively in recent years and attempted to draw the right lessons from failures of risk communication.[19] These learning processes have highlighted various ways to overcome these challenges and make risk communication more effective. Many of the suggested solutions to

---

14   Fischer, Frank (2003): Reframing public policy, Oxford University Press: Oxford, 171f.

15   Douglas, Mary; Wildavsky, Aaron B. (1983): Risk and culture. University of California Press: Berkeley; Renn, Ortwin (1992): Concepts of risks: A classification. In: Krimsky, Sheldon; Golding, Dominic (eds.): Social Theories of risk, Praeger: Westport, 53 – 82.; Slovic, Paul (2000): The perception of risk. Earthscan: London.).

16   Millstone, Erik; van Zwanenberg, Patrick; Bauer, Martin; Dora, Carlos; Dowler, Elizabeth; Draper, Alizon; Dressel, Kerstin; Gasperoni, Giancarlo; Green, Judith; Koivusalo, Meri; Ollila, Eeva (2006) 'Improving communication strategies and engaging with public concerns', in: Dora, Carlos (ed.): Health, Hazards and Public Debate. Lessons for risk communication from the BSE/CJD saga. WHO, available: *http://www.euro.who.int/ en/what-we-publish/abstracts/health,-hazards-and-public-debate.-lessons-for-risk-communication-from-the-bsecjd-saga*, 264 – 281; Leiss, William (1996): Three phases in the risk communication practice. In: Annals of the American Academy of Political and Social Science, 545, 5, 85 – 94.

17   Renn, Ortwin (2008): Risk Governance: Coping with Uncertainty in a Complex World, Earthscan: London, 283.

18   Renn (2008), 228.

19   See e.g. U.S. National Research Council (1996): Understanding Risk. Informing Decisions in a Democratic Society. Committee on Risk Characterization, National Research Council, available: *http://www.nap.edu/catalog/5138.html*; Dora, Carlos (ed.) (2006): Health, Hazards and Public Debate. Lessons for risk communication from the BSE/CJD saga. WHO, available: *http://www.euro.who.int/en/what-we-publish/abstracts/ health,-hazards-and-public-debate.-lessons-for-risk-communication-from-the-bsecjd-saga*.

the challenges of risk communication can be subsumed (and addressed) by answering the following three principle questions.

⬧ **How can we listen more closely?** The first principle question relates to the monitoring of the organizational environment. Today, there is broad agreement that risk communication is a two-way process. As an example, the World Health Organization defines risk communication as "an interactive exchange of information and opinions concerning risk among risk assessors, risk managers, consumers and other interested parties (…)".[20] However, when communicating with laypersons, experts often tend to miss what their audience needs and wants. While thinking they are providing all the 'relevant' information the public needs, experts often fail to recognize the information the public actually demands. It is therefore essential for organizational risk communicators to firstly be aware of who their target audience is, and secondly, what kind of information that audience is interested in. In particular, this implies paying thorough attention to the public perceptions of and acceptance of specific risks. As Covello and Sandman emphasize, "if people feel or perceive that they are not being heard, they cannot be expected to listen".[21] In practice, this means monitoring on-going discourses in the organizational environment as well as investing more directly in a steady dialogue with relevant stakeholders and the general public in order to be able to adapt organizational communication in a prospective fashion.

⬧ **How can we find a tailored response?** The second overarching question is how to deliver the right message to the right audience. While some fundamentals of risk communication, such as promptness, sincerity, clarity and empathy should characterise the communication irrespective of the audience, other features of risk communication must be tailored to the specific audience, or even to its subgroups.[22] Recent research shows risk communication is most effective when it is tailored to and actionable for the individual recipient of risk information.[23] Tailored risk communication can be used to provide specific information to specific audiences. These audiences can then employ this information to avoid or mitigate the risks they are specifically vulnerable to. Moreover, successful tailoring can contribute to establishing and upholding a constant risk dialogue between the organization and the public at risk. Among those aspects that can be tailored are: the choice of the media of risk messages, which should accommodate the audience as far as possible; the choice of the risk communicator within the organization; and the tone of the message, which should be understandable, but not in any way patronizing.[24]

⬧ How can we share the stakes? The third issue is probably the most challenging. Today, there is broad agreement that the management of complex risks in liberal societies cannot be achieved by the public sector alone. Rather, it requires the

20 FOA/WHO (2011): Codex Alimentarius Commission. Procedural manual. 20th edition, available: *ftp://ftp.fao.org/codex/Publications/ProcManuals/Manual_20e.pdf*, 112.

21 Covello, Vincent T.; Sandman, Peter M. (2001): Risk communication: Evolution and Revolution. In: Anthony Wolbarst (ed.): Solutions to an Environment in Peril, John Hopkins University Press, 164−178, 174.

22 Callaghan, James D. (1989): Reaching Target Audiences with Risk Information. In: Covello, Vincent T.; McCallum, David B.; Pavlova, Maria T. (eds.): Effective Risk Communication. The Role and Responsibility of Government and Nongovernment Organizations, Plenum Press: New York, 137−142.

23 See e.g. Wood, Michele M.; Mileti, Dennis S.; Kano, Megumi; Kelley, Melissa M.; Regan, Rotrease; Bourque, Linda B. (2012): Communicating Actionable Risk for Terrorism and Other Hazards. In: Risk Analysis, 32, 4, 601−615.

24 Covello, Vincent T. (2003): Best Practices in Public Health Risk and Crisis Communication. In: Journal of Health Communication, 8, 5−8.

involvement of various social actors to ensure societal resilience.[25] Social groups such as environmental initiatives, customer organizations or citizens' groups are mostly encapsulated as 'the stakeholders', which are admitted a legitimate interest in organizational decision-making processes. In this context, it is important to note that the inclusion of stakeholders in risk decision-making is not at all unproblematic, particularly in respect to the efficiency and accountability of political decisions.[26] On the other hand, the involvement of stakeholders can increase the democratic legitimacy as well as the quality of risk decision-making.[27] Following a study by the US National Research Council, deliberative procedures can have positive effects at all stages of the risk decision process, in particular by "improving problem formulation, providing more knowledge, determining appropriate uses for controversial analytic techniques, clarifying views, and making decisions more acceptable".[28] In an equal tone, a meta-analysis of 239 case studies of stakeholder involvement concludes that "there may be many ways to produce decisions of high technical quality, but there are relatively few methods that do so while also educating the public, eliciting public values, resolving conflict, and building trust in agencies, as many stakeholder processes do".[29] Yet, if organizations decide to follow such a stakeholder approach, this has major implications for

the organizational communication of risks. First of all, in order to achieve ownership, stakeholders should not only be invited into risk decision-making processes after all important decisions are taken, but rather as early as possible.[30] Moreover, selective provision of information to stakeholders will most likely not foster stakeholder trust in the risk communicators. Even though the inclusion of stakeholders is often limited for practical and legal reasons in practise, professional risk managers should aim to identify fields in which more transparency is feasible to meet legitimate demands for public involvement as well as for democratic accountability and control. Admittedly, as in other policy domains, public interest in risk information and organizational interest in non-disclosure of some risk information form a natural relationship of tension. This tension should be acknowledged and when necessary made the subject of open debates.

Box 2: Three Key Questions for Risk Communication
- How can we listen more closely to our audience in order to understand their beliefs and fears, and match their information and communication needs?
- How can we find tailored responses to our audience's needs that are suitable in the choice of content, medium and tone as well as enhance self-efficiency?
- How can we employ risk communication to share the stakes in risk governance among our partners and foster their involvement?

Obviously, the answers to these guiding questions differ. The answers depend on the type of risk that has to be managed and communicated, the organizational and political configuration that is in place

---

25   Crisis and Risk Network (2011): Focal Report 6: Risk Analysis. Resilience – Trends in Policy and Research.

26   Löfstedt (2003), 425.

27   McComas, Katherine A. (2009): Linking Public Participation and Decision Making through Risk Communication. In: Heath, Robert L.; O'Hair, H. Dan (eds.): Handbook of Risk and Crisis Communication, Routledge: London, 364–385, 367ff.

28   National Research Council (1996): Understanding Risk. Informing Decisions in a Democratic Society. Committee on Risk Characterization, National Research Council, available: *http://www.nap.edu/catalog/5138.html*, 79.

29   Beierle, Thomas C. (2002): The Quality of Stakeholder-Based Decisions. In: Risk Analysis, 22, 4, 739–749, 748.

30   Sellnow, Timothy L.; Ulmer, Robert R.; Seeger, Matthew, W.; Littlefield, Robert S. (2008): Effective Risk Communication. A message-centered approach. Springer: New York.

to govern a risk, and on the stakeholders that have a stake in a risk. Despite the diversity of risks and the approaches needed in terms of communication, there is not a single type of risk, be it natural, social or technical, which has not been affected by the rise of new information and communication technologies. Therefore, in Section 3 we address the question of how the above mentioned challenges can be met in a communication environment in which the Internet and other information and communication technologies play an increasingly important role.

3   RISK COMMUNICATION IN THE INFORMATION AGE

The revolution of interpersonal communication that came with the spread of new communication technologies has affected almost all facets of today's societies. Among these, the Internet has fundamentally changed the way personal opinions are turned into social movements, but also how political institutions are legitimized or delegitimized. Although the Internet is cherished around the globe for making communication easy, cheap and (probably) more democratic, its reputation concerning risk communication is variable. As an example, while social media play an important role in many crisis communication strategies,[31] their application to risk communication has remained rather limited to date. Social media, blogs, wikis and other websites are often suspected of being the breeding grounds for rumours, hoaxes, disinformation and public panic. This sentiment is argued on the logic that since anyone with internet access can distribute unverified content online, exaggerated or manipulated information can easily spread to a potentially global audience. Indeed, in many cases the most extreme messages on the Internet are those that receive the most attention, weakening traditional control mechanisms in public communication. Sceptics of new communication technologies warn that "(...) while traditional media (newspapers, radio) seem to both attenuate and amplify risk perceptions, digital media, including electronic technologies (blogs, podcasts, wikis, etc.) generally tend to amplify risk perceptions".[32]

However, such a negative portrayal of the role new ICTs play in risk communication appears to capture only half of the picture, since it *ignores the positive role* new media can play in risk communication. In the following, we reflect on the guiding questions discussed in Section 2 in order to illustrate some potentially positive applications of online media for risk communication, and to capture some of the most pressing challenges of contemporary risk communication. First, we discuss how the Internet can be employed by organizational risk communicators to learn about risk perceptions and risk acceptance among relevant stakeholders, and identify issues that organizational risk communication should address ("How can we listen more closely?"). Secondly, we discuss different ways to use new communication technologies to design an organizational communication approach that is tailored to the specific needs of particular target groups ("How can we find a tailored response?"). Finally, we discuss the possibility of establishing mutual trust, shared responsibility and cooperation between organizations and their environments with the help of ICT ("How can we share the stakes?").

3.1   Listening to the web

Although monitoring the organizational environment is important for public and private organizations, it is pivotal for organizations that are responsible for the management of potential hazards, and that are at the same time publicly accountable. For risk management organizations understanding public risk perceptions and risk acceptance is an central precondition for organizational legitimacy. This understanding can only be achieved by thorough monitoring of the organizational environment. As Shari Veil and her co-authors emphasize, "listening to and understanding a public through monitoring public opinion about risk is essential in the development of

---

31   CSS (2012): Conceptualizing the Crisis Mapping Phenomenon: Insights on behavior and the coordination of agents and information in complex crisis. Focal Report 7. Center for Security Studies (CSS), ETH Zürich, available: *http://www.css. ethz.ch/publications/risk_resilience_reports*.

32   Berube et al. (2010), 9.

a relationship".[33] Many organizations integrate their monitoring activities into broader processes of issue management that generally aim to identify and tackle critical trends in the organizational environment at an early stage.[34]

The two main traditional tools for organizations to monitor trends on the societal level are the constant monitoring of (mostly print and TV) media and public opinion surveys. While media monitoring has the advantage that it is comparatively cheap and fast,

---

Box 3: Monitoring issues debated in social media

Social media monitoring services such as Radian6 provide easy to use tools for the analysis of online communication of risk issues. For example, in a study on climate change discourses, Adrian Chan compares the dynamics in communication of climate change issues in mainstream media, blogs and twitter conversations. Yet, services like Radian6 not only allow following trends in online communication flows, but moreover to gain insights into demographic characteristics of social media users, their geographical location and even into relationships between users, which can used for example to identify the most relevant groups in the organizational environment. In another application, the American Red Cross uses Radian6 in its recently created Social Media Digital Operations Center to integrate social media into its relief management efforts.

Chan, Adrian (2008): Radian6 and climate change: views of mainstream, blog, and twitter conversations. In: Gravity7. Social Interaction Design by Adrian Chan. Blog May 1, 2008, available: *http://www.gravity7.com/blog/media/2008/05/radian6-and-climate-change-views-of.html#ixzz1wLLLNvRQ*.

American Red Cross (2012): The American Red Cross and Dell Launch First-Of-Its-Kind Social Media Digital Operations Center for Humanitarian Relief, ARC Press Release, available: *http://www.redcross.org/news/press-release/The-American-Red-Cross-and-Dell-Launch-First-Of-Its-Kind-Social-Media-Digital-Operations-Center-for-Humanitarian-Relief*.

---

33 Veil, Shari R.; Buehner, Tara; Palenchar, Michael J. (2011): A Work-In-Process Literature Review: Incorporating Social Media in Risk and Crisis Communication. In: Journal of Contingencies and Crisis Management, 19, 2, 110 – 122, 111.

34 Ansoff, H. Igor (1980): Strategic issue management. In: Strategic Management Journal, 1, 131 – 148.

its major drawback is that it does not measure attitudes and opinions directly at the societal level, but instead captures societal trends only as they are filtered through media outlets.[35] By contrast, public opinion surveys can capture opinions, attitudes and behaviours more directly through first-hand data collection. However, methodologically sound surveys are extraordinarily cost-intensive (both in terms of human and financial resources) and require long periods of preparation, which makes them a rather inflexible tool for monitoring the organizational environment. In this context, monitoring risk issues using the Internet provides an interesting alternative (or at least also a complementary mechanism) to traditional monitoring techniques. Online monitoring allows large amounts of data to be processed at relatively low cost in a timely way – in some instances even in real-time.[36] For example, social media data can be used to monitor the geographic spread of communicable diseases by using social media communication concerning the diseases as a proxy.[37] Box 3 illustrates how large scale user-generated data related to risk issues can be monitored and fed into risk management cycles.

Internet monitoring is not limited to quantitative techniques. Risk managers can also profit from monitoring public risk discourses as they develop in the forums of the websites of environmental initiatives or consumer protection organizations. It goes without saying that the expressions of concern, endangerment and fear that can be found in the Internet may often appear unreasoned or exaggerated from the perspective of a professional risk manager. However, it is important to keep in mind that speculation about uncertain information is natural.[38] Therefore, public concerns should not be ignored or appeased, instead they should be valued as important indicators of public risk perceptions and risk acceptance. Moreover, when the risk communicator closely follows the beliefs, attitudes, and online correspondence, they can counter rumours, incorrect or manipulative information, spread and amplified through the Internet, with knowledgeable, comprehensive and honest organizational communication.[39] In practice, online media monitoring and organizational communication are often closely interlinked.[40]

3.2 Tailoring communication online

For many years the Internet has been identified by businesses, companies and non-profit organizations, as well as many government departments and agencies as a powerful medium to implement tailored communication strategies for specific groups. This organizational popularity is mirrored by the popularity of the Internet as a place where the public obtains their information. In addition, the Internet permits real-time risk communication, which is particularly

---

35   It is important to note here that print and TV media are today often also monitored using online services such as LexisNexis, Google News or Voxalead.

36   Heath, Robert L. (2000): New communication technologies: An issues management point of view. In: Public Relations Review, 24, 3, 273–288. For a practical application of real time social media analysis in disaster prevention, see: Abel, Fabian; Hauff, Claudia; Houben, Geert-Jan; Stronkman, Richard; Tao, Ke (2012): Semantics + Filtering + Search = Twitcident. Exploring Information in Social Web Streams. In Proceedings of International Conference on Hypertext and Social Media, Milwaukee, USA, available: *http://fabianabel.de/papers/2012-wis-hypertext-twitcident.pdf*.
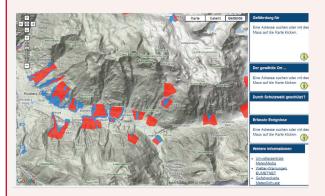
37   Brownstein, John S.; Freifeld, Clark C.; Madoff, Lawrence C. (2009): Influenza A (H1N1) Virus, 2009 — Online Monitoring. In: New England Journal of Medicine, 360, 2153–2157.

38   Sandman, Peter M.; Lanard, Jody (2003): It Is Never Too Soon to Speculate. Column September 17, 2003, available: *http://www.psandman.com/col/speculat.htm*.

39   Chung, Ik Jae (2011): Social Amplification of Risk in the Internet Environment. In: Risk Analysis, 31, 12, 1883–1896.

40   Paris, Céline; Wan, Stephen (2011): Listening to the Community. Social Media Monitoring Tasks for Improving Government Services. CHI Conference on Human Factors in Computing Systems 2011, May 7–12, 2011, Vancouver, BC, Canada, available: *http://dl.acm.org/citation.cfm?id=1979878*.

Box 4: Tailoring alpine risk communication to specific audiences

In Switzerland, the website of the Amt für Wald und Naturgefahren Graubünden uses an intuitive geographical user interface (comparable with Google Maps) to inform the users about alpine risks in specific geographical locations. Emphasis is put here on precision and usability.
http://naturgefahren.ebp.ch

A different approach to the communication of avalanche risks takes the website check-your-risk.de by the German Alpine Association (DAV). This service aims specifically to educate adolescents about avalanche risks, an age when many skiers and snowboarders start to freeride on their own. Therefore the website supplements basic information about the risks of freeriding with appealing videos of professional snowboarders and skiers in action, videos of actual avalanche incidents as well as daily updated avalanche risk reports.
www.check-your-risk.de

The third example, the website www.biberberti.com by the Austrian Federal Ministry of Agriculture, Forestry, Environment and Water Management, explains alpine risks to school kids and illustrates how online risk communication can be an opportunity to communicate with target audiences in a tone and language which is both understandable and credible.
http://www.biberberti.com/DE/themen.php

crucial when a crisis is imminent or underway.[41] Finally, due to the segmented organization of social groups on the Internet, relevant social groups can be targeted with high precision. As Strecher and his co-authors show, interactive media can be used to tailor risk communication "to users' social and cultural milieu, socio-demographic characteristics, relevant life events, literacy level, concept recognition abilities and preferences, risk perceptions (...)".[42]

Successful communication strategies should be designed for specific audiences in respect to their content, format and tone. In order to implement a tailored risk communication strategy, organizations dealing with risks first need to identify their target groups. Building on target group identification processes, organizations can best design a risk communication strategy.[43] After having clarified who the strategy is targeted at, the next step is to identify the communication techniques and services that are already used by the target group and which can be exploited for the organizational risk communication efforts. For example, since smartphones are particularly widespread among young people, organizations can create their own smartphone software (so-called 'apps') to reach their audiences. For example, the U.S. Federal Emergency Management Agency (FEMA) has created apps for the popular iPhone and Android systems that allow hazard-affected individuals to register for government assistance for instance with their smartphone in circumstance when other communication channels are often not available during, or immedi-

ately after hazard activity, even though there is also a risk that this service is down due to power outage (after a severe storm, earthquake or technical failure).[44]

A second question relates to the content of online risk communication. While in some cases, being up-to-date and comprehensive are important features, in other instances an emphasis on usability, clarity and soundness is more appropriate. Using the example of alpine risks, the three websites in Box 4 exemplify how different online risk communication strategies can be designed, depending on the goal of the communication strategy.

A final opportunity of online risk communication relates to the self-efficacy of risk messages. As Matthew Seeger and his co-authors warn, "(w)hen people perceive a risk is severe but that there is little or nothing they can do to avoid it, they are likely to engage in defensive avoidance behavior such as denial or evasion of the issue".[45] In this context, online communication techniques allow tailoring risk messages to very specific sub-groups of the audience, so that each sub-group receives those risk messages that it can use to adapt its behavior to a risk.

3.3 Openness and responsiveness on the Internet

In recent years, risk decision-making in many countries has experienced a sharp increase of stakeholder engagement and public participation. Free information and communication are at the heart of these developments, as Matthew Seeger and his co-authors note: "Essentially, stakeholders claim a freedom of in-

---

41 See e.g. Sriramesh, Krishnamurthy; Wattegama, Chanuka; Abo, Frederick John (2007): The role of ICTs in risk communication in Asia Pacific, in: Librero, Felix; Arinto, Patricia B. (eds.): Digital Review of Asia Pacific, Sage/IDRC, available: *http://web.idrc.ca/en/ev-127030-201-1-DO_TOPIC.html*.

42 Strecher, Victor J.; Greenwood, Todd; Wang, Catharine; Dumont, Dana (1999): Interactive Multimedia and Risk Communication. In: Journal of the National Cancer Institute Monographs, 25, 134–139, 135.

43 CSS (2009b): Risk Analysis. Risk Communication in the Public Sector, Focal Report 3. Center for Security Studies (CSS), ETH Zürich.

44 FEMA (2012): The FEMA App for Google Adroid Systems, available: *https://play.google.com/store/apps/details?id=gov.fema.mobile.android*.

45 Seeger, Matthew W.; Sellnow, Timothy L; Ulmer, Robert R. (2003): Communication and Organizational Crisis, Praeger: Westport, 210f.

formation based on the right to know about potential harms associated with products, services, manufacturing facilities, technology, transportation, and many other organizationally constituted processes and outcomes".[46] These claims have been proliferated to a considerable degree by the fast spread of online communication technologies which have given new opportunities for information-gathering, coordination

and public communication also to low-resourced societal groups. As Sheldon Krimsky observes, the Internet particularly helps stakeholder groups to get their messages out, because "it levels the playing field to a public that does not understand the hierarchy of expertise (meritocracy). Importantly, the poorest public interest group can have an Internet site that is as elaborate as that of a multi-billion dollar corporation".[47]

Box 5: Establishing a risk dialogue through social media

An increasing number of governmental institutions use own social media websites to communicate with the public about risk issues. As an example, the Bastrop County office of Emergency Management has created an account on Facebook to communicate continuously their risk assessments for natural hazards such as thunderstorms, but also to inform the public about the office's publication and upcoming events such as extreme weather preparedness trainings. The major advantage of using Facebook for such purposes is that this way young citizens can be easily reached which often do not read local newspapers. Moreover, services like Facebook allow for question-and-answer reciprocity (Veil et al. 2011: 113). Such feedback loops can be effective in encountering rumours and public misperceptions.

A second type of social media that has gained social influence at a high speed in recent years and that can also be used for organizational risk communication are microblogging services such as Twitter. As an example, the U.S. Center for Disease Control and Prevention uses Twitter to disseminate health risk information and provide behavioural advice. Microblogging services are particularly effective to reach large audiences without time delays and keep them updated on subsequent developments. Through reposting functions risk messages also can reach users that do not follow the sources of message themselves.

source: *http://www.facebook.com/pages/Bastrop-County-Office-of-Emergency-Management/193202960708177*

---

46   Seeger et al. (2003),70.

47   Krimsky (2007), 160.

Nevertheless, risk managers should not simply regard the Internet as a threat to established knowledge-based power positions. Likewise, for organizations responsible for risk management, the Internet offers many opportunities to strengthen the relationship with the organizational environment. For instance, organizations can use the Internet to employ reputation-building efforts, which may be a pivotal precondition for trust-based risk communication.[48] Here, online platforms that enable dialogic forms of communication with stakeholders and interested citizens are important (see for example Box 5). The goal here is not primarily to foster public trust in individual representatives of the organization, but rather trust in the institution that is responsible for the risk management process, which is the more relevant form of trust in respect to public risk-acceptance.[49]

Online media are promising for these new forms of communication and decision-making due to their openness, their accessibility for many people, as well as the speed with which such platforms can be set up or altered. Another advantage is that online communication channels can be structured according to the context-specific needs. For example, when debating controversial risk issues, conflicts often can be moderated and also mitigated if debates are broken down into smaller sub-debates, each dealing with a particular aspect of an issue.[50] In this case, online forums appear useful, since they can easily be organized into issue-specific dialogues. Finally, the Internet can be employed to assess success as well as challenges in communication efforts with stakeholders and the general public.

Summing up, the Internet can be employed in various ways to improve transparency and responsiveness in public risk communication. Still, the opportunities that new ICT's bring for risk communication so far have not been exploited to the fullest. While the Internet is often used to enhance transparency and to establish continuous communication with the public, deliberative and participatory processes in risk decision-making using the Internet are still in their infancy.[51] This reflects the larger picture of organizational online communication where the Internet is used to disclose information to the public, but the opportunities for interactive communication are not yet exhausted.[52] In order to engage in a more dialogic approach to public communication, most public and private organizations involved in risk governance would still need to first invest in the additional technical and human resources that are necessary for responsive communication in social networks and other new media. But arguably even more important, these organizations would need to rethink their relationships with their organizational environment and particularly accept the fact that today's information contexts do no longer allow them to control public communication processes as it had been possible in the pre-internet age.

---

48 See e.g. Briones, Rowena; L., Kuch, Beth; Liu, Brooke F.; Jin, Yan (2011): Keeping up with the digital age: How the American Red Cross uses social media to build relationships. In: Public Relations Review, 37, 1, 37–43.

49 Sjöberg, Lennart (2008): Antagonism, trust and perceived risk. In: Risk Management, 10, 32–55.

50 Hance, Billie Jo; Chess, Caron; Sandman, Peter M. (1987): Improving Dialogue with Communities: A Risk Communication Manual for Government. In: Covello, Vincent T.; McCallum, David B.; Pavlova, Maria T. (eds.) Effective Risk Communication. The Role and Responsibility of Government and Nongovernment Organizations. Plenum Press: New York, 191–296, 241.

51 McComas (2009), 369f.

52 Waters, Richard D., Burnett, Emily, Lamm, Anna; Lucas, Jessica (2009): Engaging Stakeholders through Social Networking: How Nonprofit Organizations are Using Facebook. In: Public Relations Review, 35, 102–106.

4   CONCLUSIONS AND IMPLICATIONS FOR SWITZERLAND

4.1   General conclusions: Adapting risk management to the information environment

In the previous section, we have shown how variable and often contrary the role of social media, blogs and other online media in risk communication can be. However, many organizations tend to look at new information and communication technologies only from a single perspective – either as a source of potential trouble or as an additional channel to spread organization-specific information. In order to capture the multiple and often ambivalent roles new information technologies can play, organizations could benefit from a more holistic approach, accepting online media as a permanent feature of the organizational environment that influences risk management at every step of the process. Risk management is mostly described as a cyclic process that consists of four consecutive steps which basically are: identifying risks, assessing risks, addressing risks, monitoring impact/learning.[53] Based on our analysis of the impact of ICT on risk communication in the preceding sections, we argue that online risk communication can be understood as a second cyclic process that is at the heart of the risk management process (see figure 1).

- **Identifying risks:** The public can be a valuable resource in risk identification processes.[54] Public risk perceptions and societal risk discourses are important additives to expert judgments and can help to identify adverse events long before they materialize. To this end, risk managers can monitor issues debated in online media such as micro blogs and social networks.

- **Assessing risks:** Even more than risk identification, risk assessment is a task that cannot be resolved by experts alone, since risks need to be weighed and valued on the societal level as well. As Ortwin Renn emphasizes, "[t]he most controversial aspect of handling risks refers to process of delineating and justifying a judgment about the tolerability or acceptability of a given risk".[55] Internet-based technologies offer various ways to establish public dialogues that take into account social risk perceptions as well as risk acceptance. The benefits of dialogical and participative risk assessment on the internet are far from being exhausted, and it should be expected that this aspect of online risk communication will steadily grow in importance into the future.

- **Addressing risks:** Every policy strategy that aims to prevent or mitigate risks includes a communication dimension. Although online media will not replace traditional media like television and newspaper in the foreseeable future, the internet will most likely gain importance as a medium for the dissemination of risk information. Due to the provision of networking, feedbacks and user-generated content in many online technologies, the growing importance of online communication opens new opportunities to strengthen dialogic communication over risk issues between organizations responsible for risk management.

---

53   See e.g. UK Resilience (2008): Communicating Risks. Report by the Cabinet Office, available: *http://www.cabinetoffice.gov.uk/sites/default/files/resources/communicating-risk-guidance.pdf*, 25.

54   Seeger, Matthew W. (2006): Best Practices in Crisis Communication: An Expert Panel Process. In: Journal of Applied Communication, 34, 3, 232 – 244, 238.

---

55   Renn (2008), 149.

◆ **Monitoring impact/ learning:** The internet is well-suited to assess the success of organizational risk communication. Online debates in chat rooms, online fora and social networks, can be monitored in order to identify and understand public uncertainties, misperceptions, attitudes, values and beliefs. Using a flexible medium like the Internet could ensure misunderstandings can be corrected quickly and directly. As such, the inclusion of bottom-up feedback can be used to improve risk management as well as risk communication strategies.

Figure 1: Integration of online risk communication into risk management cycle

4.2 Implications for Switzerland

Various Swiss agencies have been using the Internet for risk communication processes for quite some time. While it is impossible to list all the efforts here, there are a few examples worth mentioning at this point:

◆ *http://www.planat.ch*: Switzerland's "National Platform for Natural Hazards" PLANAT is an extra-parliamentary expert commission. The Federal Office for Civil Protection (FOCP) is one of the key contributors to the commission's internet platform, which was founded by the Federal Council in 1997. The commission's goals include the contribution to a paradigm shift from pure protection against hazards to the management of risks. Its homepage serves as a comprehensive information resource about all kinds of possible natural hazards in Switzerland and illustrates strategies for the management of these hazards. It includes tailored information for different stakeholders such as homeowners, authorities and partner organizations in the realm of disaster management. There is also a dedicated section entitled 'risk dialogue', offering official risk information by Swiss government agencies, explaining the responsibilities of different actors in the case of natural hazards, and showcasing 'good examples' of official risk communication efforts in the area of national hazards. Planat.ch is not set up for immediate active communication with the public (there is no forum, no presence on social networks or microblogging sites) – it serves purely as a database, offering up-to-date risk information for concerned and interested parties.

◆ *http://naturgefahren.ch*: This website is the official natural hazard warning page of the Swiss government. It shows current warnings, information about all kinds of natural hazards and their occurrence, instructions for cases of emergency, as well as a section on hazard prevention strategies. It is the government's duty to warn the public of natural hazards, and the site naturgefahren.ch is the information page of all official expert agencies handling natural hazards that work closely together at all times (Swiss Meteorological Institute MeteoSwiss, Federal Office for the Environ-

ment, Institute for Snow and Avalanche Research WSL/SLF, Swiss Seismological Service (SED), Swiss Federal Office for Civil Protection (FOCP) as well as the Federal Chancellery). As such, the page serves as the Internet news and information outlet concerning current and past warnings and thus it is an important part of the government's national hazard information strategy. The site is purely an information platform – it does not offer any dialogue functions and is not present on social networks or micro-blogging sites.

◆ *http://pandemia.ch*: The information site of the Federal Office of Public Health (FOPH) about pandemic influenza. During the outbreak of the H1N1 virus in 2009/2010, the FOPH was engaged in risk communication on all available channels (Radio, TV, newspapers, information in public places, pharmacies and doctors' offices, and also the Internet). The site can be regarded as a prime example of professional traditional risk communication: There are various explanatory sections about influenza pandemics, in general, and H1N1 in particular. All the government's efforts and strategies to prevent the pandemic influenza are listed and explained in detail, in easily understandable language. Possible questions from concerned citizens are taken into account (for instance, "Why prepare?" is a section explaining why some prevention efforts are necessary, and the section "individual hygiene efforts", as well as a downloadable document entitled "this is how we can protect ourselves" shows all the steps needed to counter the spread of influenza). Furthermore, the site also has a section for health professionals, providing documents of a more scientific nature. Lastly, the site also offers a collection of all public information campaigns (Youtube-videos of TV-spots featuring Swiss celebrities that were shown during the outbreak of H1N1). Again, what the site does not offer is a forum section, and it is not pre-

sent on the social networks and micro-blogging sites such as Twitter.

◆ *http://www.ensi.ch*: The Swiss Federal Nuclear Safety Inspectorate (ENSI) is in some ways the odd one out on this list. It is not part of the Swiss Federal Office of Energy, but an independent body constituted under public law. This may explain its risk communication strategy, which differs from all the others mentioned above. While the *website* does not differ much from those of Swiss government agencies (there is a huge information library about ENSI's actions, nuclear safety in Switzerland and current and past projects and happenings), ENSI is also present on the micro-blogging site *Twitter* and on *Facebook*. Here, ENSI does not only communicate current events and news updates from its website – it can and sometimes does also engage in direct conversation with concerned citizens.

A recent example shows the effectiveness of Twitter as an instant risk communication device. On February 12 2012, only a few days after the emergency shutdown (reactor scram) on February 8 2012[56], the Swiss government's press office sent out the same E-Mail warning about the reactor shutdown again – there was a technical problem which lead to the re-sending of the E-Mail[57]. The news quickly made the rounds on the micro-blogging site Twitter. Various people, among them Swiss journalists, wrote about yet another reactor shutdown at Mühleberg. Because of its presence on Twitter, ENSI was able to immediately

---

56   ENSI (2012): Reaktorschnellabschaltung im Kernkraftwerk Mühleberg, press release February 8, available: *http://www.ensi.ch/de/2012/02/08/reaktorschnellabschaltung-im-kernkraftwerk-muhleberg*.

57   ENSI (2012b): E-Mail-Panne beim NSB: Kein neues Ereignis im Kernkraftwerk Mühleberg, press release February 13, available: *http://www.ensi.ch/de/2012/02/13/kein-neues-ereignis-im-kernkraftwerk-muhleberg*.

counter the false information[58] (*"E-Mail Panne: Kein neues Ereignis im Kernkraftwerk Mühleberg"*). ENSI's 'tweet' about the wrong E-Mail also contained a link to ENSI's homepage, where the story of the wrong E-Mail was explained in more detail. Even a tweet from a concerned Swiss political journalist to ENSI (*"Ihr jagt einem ja ganz schön den Schrecken ein"*) was immediately answered by the nuclear safety inspectorate: *"Die technische Verantwortung für den E-Mail-Versand des News Service Bund liegt bei der Bundeskanzlei, nicht beim ENSI"*.[59]

This is a prime example for risk communication on the Internet. An example that shows both aspects of communication on the Internet mentioned in this report – the bad as well as the good. In the first case, accidentally communicated misinformation from an official source spread on Twitter and elsewhere within minutes. The Internet clearly helped spread this misinformation from an otherwise reliable source at great speed. However, on the same social network (Twitter), the experts from ENSI were also immediately capable of correcting and explaining the misinformation, even engaging in direct conversation with one particular journalist. This is therefore an example of the power of risk communication on the Internet to correct misinformation very quickly: The flow of messages about the alleged second shutdown died down quickly, while ENSI's correction spread through Twitter's 'retweet' function. On the next day, there were no articles in the press containing the wrong information originally passed on. Thus ENSI's risk communication successfully prevented a possible 'infodemic'.

As the above examples show, the Internet is already widely used by Swiss government departments for risk communication. However, with the exception of the Swiss Federal Nuclear Inspectorate ENSI (an independent body under public law), which engages in two-way-communications and also listens to stakeholders online as shown above, the online risk communication efforts by Swiss government bodies are in general still one-way in nature (pre-defined information without the possibility of direct conversation/feedback by stakeholders).

Therefore, we suggest that Swiss government agencies consider enhancing their public risk communication strategies with greater web-enabled engagement. The following questions could be considered by every agency engaged in public risk communication:
- Do we want our risk communication to incorporate feedback and input from stakeholders?
- How could we achieve a better two-way-communication with citizen participation?
- In what areas and departments could such a contribution make sense and actually enhance the quality and effects of official risk communication efforts?

The present report cannot answer these questions. They should be evaluated by the departments. Also, general guidelines concerning the use of social media and micro-blogging sites such as Twitter should be discussed and developed on an intra-departmental level. As of now, Swiss government agencies are not present on social networks or on Twitter. If managed appropriately, these communication media could enhance risk communication between government and citizens via the Internet.

The ready risk discourse that the Internet and social media permit should not be ignored by government departments: Risk communication needs to take place where the stakeholders and public are. While

---

58 ENSI (2012c): E-Mail-Panne: Kein neues Ereignis im Kernkraftwerk Mühleberg, Twitter message, available: *https://twitter.com/ENSI_CH/status/169050981064118272*.

59 ENSI (2012d): Die technische Verantwortung für den E-Mail-Versand des News Service Bund liegt bei der Bundeskanzlei, nicht beim ENSI, Twitter message, available: *https://twitter.com/ENSI_CH/status/169063382597644289*.

some members of society still require risk information from traditional sources, the growing pervasiveness of the Internet and social networking particularly, highlights the need for risk communicators to understand and utilize all modes of communication. If stakeholders do not find the information they are looking for on official websites and in (social) media channels, they are likely to turn to other sources[60] – and potentially receive and pass on misinformation. Of course, clear guidelines concerning the rules and best practice of official risk communication on the Internet and social networking sites must be established.[61] While the Internet offers a fast, low priced and effective way of communicating with partners, stakeholders and the public in a dynamic way, information disseminated in this way must be well prepared in advance, both technically and on an organizational level, for example by employing diverse risk scenarios to train staff for the challenges of risk communication in today's highly dynamic information environment.

60 Stephens, Keri K.; Malone, Patty C. (2009): If Organizations Won't Give us Information . . .: The Use of Multiple New Media in Crisis Technical Translation and Dialogue. In: Journal of Public Relations Research, 21, 2, 229 – 239.

61 Veil et al. (2011), 112.

5   BIBLIOGRAPHY

Abel, Fabian; Hauff, Claudia; Houben, Geert-Jan; Stronkman, Richard; Tao, Ke (2012): Semantics + Filtering + Search = Twitcident. Exploring Information in Social Web Streams. In: Proceedings of International Conference on Hypertext and Social Media, Milwaukee, USA, available: *http://fabianabel.de/papers/2012-wis-hypertext-twitcident.pdf*.

American Red Cross (2012): The American Red Cross and Dell Launch First-Of-Its-Kind Social Media Digital Operations Center for Humanitarian Relief, ARC Press Release, available: *http://www.redcross.org/news/press-release/The-American-Red-Cross-and-Dell-Launch-First-Of-Its-Kind-Social-Media-Digital-Operations-Center-for-Humanitarian-Relief*.

American Red Cross (2010): Social Media in Disasters and Emergencies, ARC survey July 2010, available: *http://www.redcross.org/www-files/Documents/pdf/other/SocialMediaSlideDeck.pdf*.

Amt für Wald und Naturgefahren Graubünden (2012): Check your Risk. Naturgefahrenkarten Graubünden, available: *http://naturgefahren.ebp.ch*.

Ansoff, H. Igor (1980): Strategic issue management. In: Strategic Management Journal, 1, 131–148.

Bastrop County Office of Emergency Management (2012): BCOEM Facebook page, available: *http://www.facebook.com/pages/Bastrop-County-Office-of-Emergency-Management/193202960708177*.

Beierle, Thomas C. (2002): The Quality of Stakeholder-Based Decisions. In: Risk Analysis, 22, 4, 739–749.

Bernstein, Peter L. (1996): Against the Gods. The Remarkable Story of Risk. Wiley: New York.

Berube, David M.; Faber, Brenton; Scheufele, Dietram A.; Cummings, Christopher, L.; Gardner, Grant E.; Kelly, Martin N.; Martin, Michael S.; Temple, Nicolas M. (2010): Communicating Risk in the 21st Century. The Case of Nanotechnology. NNCO White Paper, February 2010, available: *http://rit.academia.edu/KellyNM/Papers/322606/White_Paper_Communicating_Risk_in_the_21st_Century*.

Briones, Rowena; L., Kuch, Beth; Liu, Brooke F.; Jin, Yan (2011): Keeping up with the digital age: How the American Red Cross uses social media to build relationships. In: Public Relations Review, 37, 1, 37–43.

Brownstein, John S.; Freifeld, Clark C.; Madoff, Lawrence C. (2009): Influenza A (H1N1) Virus, 2009 — Online Monitoring. In: New England Journal of Medicine, 360, 2153–2157.

Callaghan, James D. (1989): Reaching Target Audiences with Risk Information. In: Covello, Vincent T.; McCallum, David B.; Pavlova, Maria T. (eds.): Effective Risk Communication. The Role and Responsibility of Government and Nongovernment Organizations, Plenum Press: New York, 137–142.

Cassell, Michael M.; Jackson, Christine; Cheuvront, Brian (1998): Health Communication on the Internet: An Effective Channel for Health Behavior Change? In: Journal of Health Communication. International Perspectives, 3, 1, 71–79.

Chan, Adrian (2008): Radian6 and climate change: views of mainstream, blog, and twitter conversations. In: Gravity7. Social Interaction Design by Adrian Chan. Blog May 1, 2008, available: *http://www.gravity7.com/blog/media/2008/05/radian6-and-climate-change-views-of.html#ixzz1wLLLNvRQ*.

Chung, Ik Jae (2011): Social Amplification of Risk in the Internet Environment. In: Risk Analysis, 31, 12, 1883–1896.

Covello, Vincent T.; Sandman, Peter M. (2001): Risk communication: Evolution and Revolution. In: Anthony Wolbarst (ed.): Solutions to an Environment in Peril, John Hopkins University Press: Baltimore, 164–178.

Covello, Vincent T. (2003): Best Practices in Public Health Risk and Crisis Communication. In: Journal of Health Communication, 8, 5–8.

CSS (2012 forthcoming): Conceptualizing the Crisis Mapping Phenomenon: Insights on behavior and the coordination of agents and information in complex crisis. CRN Focal Report 7. Center for Security Studies (CSS), ETH Zürich. available: *http://www.css.ethz.ch/publications/risk_resilience_reports*.

CSS (2009): Examining Resilience. A concept to improve societal security and technical safety, CRN Factsheet. Center for Security Studies (CSS), ETH Zürich, available: *http://www.css.ethz.ch/publications/pdfs/Factsheet-Examining-Resilience.pdf*.

CSS (2009b): Risk Analysis. Risk Communication in the Public Sector, CRN Focal Report 3. Center for Security Studies (CSS), ETH Zürich, available: *http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=110683&lng=en*.

CSS (Oktober 2009). Risikokommunikation: Nutzen für die Sicherheitspolitik. Analysen zur Sicherheitspolitik, 62, Center for Security Studies (CSS), ETH Zürich, available: *http://www.css.ethz.ch/publications/pdfs/CSS-Analysen-62.pdf*.

Deutscher Alpenverein (2012): Check your risk. German Alpine Association (DAV), available: *http://www.check-your-risk.de*.

Dora, Carlos (ed.) (2006): Health, Hazards and Public Debate. Lessons for risk communication from the BSE/CJD saga. WHO, available: *http://www.euro.who.int/en/what-we-publish/abstracts/health,-hazards-and-public-debate.-lessons-for-risk-communication-from-the-bsecjd-saga*.

Douglas, Mary; Wildavsky, Aaron B. (1983): Risk and culture. University of California Press: Berkeley.

Eichelberger, Laura (2007): SARS and New York's Chinatown: The politics of risk and blame during an epidemic of fear. In: Social Science & Medicine, 65, 1284–1295.

ENSI (2012): Reaktorschnellabschaltung im Kernkraftwerk Mühleberg, press release February 8, available: *http://www.ensi.ch/de/2012/02/08/reaktorschnellabschaltung-im-kernkraftwerk-muhleberg*.

ENSI (2012b): E-Mail-Panne beim NSB: Kein neues Ereignis im Kernkraftwerk Mühleberg, press release February 13, available: *http://www.ensi.ch/de/2012/02/13/kein-neues-ereignis-im-kernkraftwerk-muhleberg*.

ENSI (2012c): E-Mail-Panne: Kein neues Ereignis im Kernkraftwerk Mühleberg, Twitter message, available: *https://twitter.com/ENSI_CH/status/169050981064118272*.

ENSI (2012d): Die technische Verantwortung für den E-Mail-Versand des News Service Bund liegt bei der Bundeskanzlei, nicht beim ENSI, Twitter message, available: *https://twitter.com/ENSI_CH/status/169063382597644289*.

Fischer, Frank (2003): Reframing public policy, Oxford University Press: Oxford.

Fischhoff, Baruch (1995): Risk Perception and Risk Communication Unplugged. Twenty Years of Process. In: Risk Analysis, 15, 2, 137–145.

FEMA (2012): The FEMA App for Google Adroid Systems, available: *https://play.google.com/store/apps/details?id=gov.fema.mobile.android*.

FOA/WHO (2011): Codex Alimentarius Commission. Procedual manual. 20th edition, available: *ftp://ftp.fao.org/codex/Publications/ProcManuals/Manual_20e.pdf*.

Greenberg, Michael; Haas, Charles; Cox, Anthony Jr.; Lowrie, Karen; McComas, Katherine; North, Warner (2012): Ten Most Important Accomplishments in Risk Analysis, 1980–2010. In: Risk Analysis 32, 5, 771–781.

Hadden, Susan G. (1989): Institutional barriers to risk communication. In: Risk Analysis, 9, 301–308.

Hance, Billie Jo; Chess, Caron; Sandman, Peter M. (1987): Improving Dialogue with Communities: A Risk Communication Manual for Government. In: Covello, Vincent T.; McCallum, David B.; Pavlova, Maria T. (eds.) Effective Risk Communication. The Role and Responsibility of Government and Nongovernment Organizations. Plenum Press: New York, 191–296.

Heath, Robert L. (2000): New communication technologies: An issues management point of view. In: Public Relations Review, 24, 3, 273–288.

International Risk Governance Council (2009): Risk Governance Deficits. An analysis and illustration of the most common deficits in risk governance. IRGC Report, available: *http://www.irgc.org/IMG/pdf/IRGC_rgd_web_final.pdf*.

Kittler, Anne F.; Hobbs, John; Volk, Lynn A.; Kreps, Gary L.; Bates, David W. (2004): The Internet as a Vehicle to Communicate Health Information During a Public Health Emergency: A Survey Analysis Involving the Anthrax Scare of 2001. In: Journal of Medical Internet Research, 6, 1, e8, available: *http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1550585*.

Krimsky, Sheldon (2007): Risk communication in the internet age: The rise of disorganized skepticism. In: Environmental Hazards, 7, 157–164.

Leiss, William (1996): Three phases in the risk communication practice. In: Annals of the American Academy of Political and Social Science, 545, 5, 85–94.

Löfstedt, Ragnar (2003): Risk communication. Pitfalls and promises. In: European Review, 11, 417–435.

McComas, Katherine A. (2009): Linking Public Participation and Decision Making through Risk Communication. In: Heath, Robert L.; O'Hair, H. Dan (eds.): Handbook of Risk and Crisis Communication, Routledge: London, 364–385.

Millstone, Erik; van Zwanenberg, Patrick; Bauer, Martin; Dora, Carlos; Dowler, Elizabeth; Draper, Alizon; Dressel, Kerstin; Gasperoni, Giancarlo; Green, Judith; Koivusalo, Meri; Ollila, Eeva (2006) 'Improving communication strategies and engaging with public concerns', in: Dora, Carlos (ed.): Health, Hazards and Public Debate. Lessons for risk communication from the BSE/CJD saga. WHO, available: *http://www.euro.who.int/ en/what-we-publish/abstracts/health,-hazards-and-public-debate.-lessons-for-risk-communica-tion-from-the-bsecjd-saga*, 264–281.

Österreichisches Bundesministerium für Land- und Forstwirtschaft, Umwelt und Wasserwirtschaft (2012): Biber Berti und seine Freunde, available: *http://www.biberberti.com/DE/themen.php*.

Paris, Céline; Wan, Stephen (2011): Listening to the Community. Social Media Monitoring Tasks for Improving Government Services. CHI Conference on Human Factors in Computing Systems 2011, May 7–12, 2011, Vancouver, BC, Canada, available: *http://dl.acm.org/citation.cfm?id=1979878*.

Plough, Alonzo; Krimsky, Sheldon. (1987): The emergence of risk communication studies: Social and political context. In: Science, Technology, & Human Values, 12, 3/4, 4–10.

Renn, Ortwin (2008): Risk Governance: Coping with Uncertainty in a Complex World, Earthscan: London.

Renn, Ortwin (1992): Concepts of risks: A classification. In: Krimsky, Sheldon; Golding, Dominic (eds.): Social Theories of risk, Praeger: Westport, 53–82.

Rothkopf, David J. (2003): When the Buzz Bites Back. In: The Washington Post, May 11, 2003, B01, available: *http://www.udel.edu/globalagenda/2004/ student/readings/infodemic.html.*

Sandman, Peter M.; Lanard, Jody (2003): It Is Never Too Soon to Speculate. Column September 17, 2003, available: *http://www.psandman.com/col/spe-culat.htm*.

Seeger, Matthew W. (2006): Best Practices in Crisis Communication: An Expert Panel Process. In: Journal of Applied Communication, 34, 3, 232–244.

Seeger, Matthew W.; Sellnow, Timothy L; Ulmer, Robert R. (2003): Communication and Organizational Crisis, Praeger: Westport.

Sellnow, Timothy L.; Ulmer, Robert R.; Seeger, Matthew, W.; Littlefield, Robert S. (2008): Effective Risk Communication. A message-centered approach. Springer: New York.

Slovic, Paul (2000): The perception of risk. Earthscan: London.

Sjöberg, Lennart (2008): Antagonism, trust and perceived risk. In: Risk Management, 10, 32–55.

Sriramesh, Krishnamurthy; Wattegama, Chanuka; Abo, Frederick John (2007): The role of ICTs in risk communication in Asia Pacific, in: Librero, Felix; Arinto, Patricia B. (eds.): Digital Review of Asia Pacific, Sage/IDRC, available: *http://web.idrc.ca/ en/ev-127030-201-1-DO_TOPIC.html*.

Stephens, Keri K.; Malone, Patty C. (2009): If Organizations Won't Give us Information . . .: The Use of Multiple New Media in Crisis Technical Translation and Dialogue. In: Journal of Public Relations Research, 21, 2, 229–239.

Strecher, Victor J.; Greenwood, Todd; Wang, Catharine; Dumont, Dana (1999): Interactive Multimedia and Risk Communication. In: Journal of the National Cancer Institute Monographs, 25, 134–139.

UK Resilience (2008): Communicating Risks. Report by the Cabinet Office, available: *http://www.cabinetoffice.gov.uk/sites/default/files/resources/communicating-risk-guidance.pdf*.

U.S. Centers for Disease Control and Prevention (2012): Social Media at CDC, available: *http://www.cdc.gov/SocialMedia/Tools/Twitter.html*.

U.S. National Research Council (1996): Understanding Risk. Informing Decisions in a Democratic Society. Committee on Risk Characterization, National Research Council, available: *http://www.nap.edu/catalog/5138.html*.

Veil, Shari R.; Buehner, Tara; Palenchar, Michael J. (2011): A Work-In-Process Literature Review: Incorporating Social Media in Risk and Crisis Communication. In: Journal of Contingencies and Crisis Management, 19, 2, 110–122.

Waters, Richard D., Burnett, Emily, Lamm, Anna; Lucas, Jessica (2009): Engaging Stakeholders through Social Networking: How Nonprofit Organizations are Using Facebook. In: Public Relations Review, 35, 102–106.

World Health Organization WHO (2003): Summary table of SARS cases by country, 1 November 2002 – 7 August 2003, available: *http://www.who.int/csr/sars/country/country2003_08_15.pdf*.

Wood, Michele M.; Mileti, Dennis S.; Kano, Megumi; Kelley, Melissa M.; Regan, Rotrease; Bourque, Linda B. (2012): Communicating Actionable Risk for Terrorism and Other Hazards. In: Risk Analysis, 32, 4, 601–615.

Wright, Donald K.; Hinson, Michelle D. (2009): Examining How Public Relations Practitioners Actually are Using Social Media. In: Public Relations Journal, 3, 3, 2–32.

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** specializes in research, teaching, and information services in the fields of international relations and security policy. The CSS also acts as a consultant to various political bodies and the general public. The Center is engaged in research projects with a number of Swiss and international partners, focusing on new risks, European and transatlantic security, strategy and doctrine, state failure and state building, and Swiss foreign and security policy.