CRN CONFERENCE 2007 REPORT

Managing Risks in Government, Business, and Society

14–16 June 2007, Brunnen, Switzerland

organized by
the Crisis and Risk Network (CRN)

CSS
ETH Zurich

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

This report is available on the Internet: www.crn.ethz.ch

Authors: Sergio Bonin
Elgin Brunner
Christoph Doktor
Beat Habegger
Manuel Suter

Postal address:

Center for Security Studies
ETH Zurich SEI
8092 Zürich
Switzerland
Tel. +41 44 632 40 25
Fax +41 44 632 19 41
www.crn.ethz.ch
crn@sipo.gess.ethz.ch

TABLE OF CONTENTS

1. SUMMARY OF SELECTED KEY ISSUES

Modern threats such as a global pandemic, the collapse of critical infrastructures, or terrorism are ubiquitous topics of public discussion. The ever-closer functional and geographic links in today's world lead to a wide array of risks and threats, and our closely interlinked, highly complex societies have become extremely vulnerable. We are exposed to a multitude of risks that can hinder the realization of social and private goals or even make them impossible. This means that fast, efficient, and effective strategic risk management is a key challenge for national governments, business enterprises, and international institutions.

What is the best way to deal with security policy risks the causes and consequences of which are unclear or can only be described in vague terms? How can risk analysts and decision-makers plan for an uncertain future in an insecure world? How can risks be identified promptly, assessed correctly, and mitigated effectively? – Around 55 experts from public administrations, security institutions, private corporations, and international organizations dealt with these questions at the 2007 Conference of the Crisis and Risk Network (CRN) on the topic of "Managing Risks in Government, Business, and Society", which took place in Brunnen from 14–16 June 2007.

What information is relevant?

To counter possible risks accurately, they must first of all be identified – a task that is more difficult than is apparent at first sight. In a world of information overload, the problem is often no longer one of accessing the data and facts, but of filtering out from them those that are really relevant, analyzing them correctly, and utilizing them purposefully. Several speakers were unanimous in stressing that one must know the sources from which information originates, how credible they are, and what cognitive biases and thinking pathologies the analysts display.

Turning insight into action

Many international organizations and national intelligence agencies have put in place early-warning systems in order to detect "weak signals" early on and to enable policy-makers to rapidly implement appropriate countermeasures. Several presentations showed that early warning is more than just comprehensive data collection: it essentially requires a broad network of experienced and open-minded analysts with well-developed imaginative and analytical skills. Beyond that, they should also possess communicative skills and a good knowledge of their audience in order to get their messages effectively across so that the insights of early warning can be translated into action.

Bridging the gap between analysts and decision-makers

Another topic was the frequently inadequate transfer of knowledge between analysts and decision-makers, mostly involving deficiencies in communication: analysts' messages are insufficiently tailored to the needs of their target group or are weighed down by technical jargon. On the other hand, decision-makers like to foster the stereotype of the expert obsessed with details, whose information, they say, is useless in practice, only to be entrapped by their own activism, preferring to bring in external expertise and ignoring what is often better advice from within their own organization. Therefore, improved risk communication

requires all participants to be fully transparent about their own assumptions on which they base their actions, to follow clear communication rules, and to establish a firmly anchored mutual learning process.

Underestimated consequences

Despite all precautions, some risks develop into crises or even major emergencies. One of the interesting observations made at the conference was that consequential damage often has a bigger impact than the damage caused directly by the event. For example, the insurance companies were quite well prepared for major catastrophes such as the terrorist attacks of 11 September 2001 or Hurricane Katrina in 2005. However, they had underestimated the enormous losses sustained by the insured firms as a result of the prolonged interruption of business. Increased attention must also be paid to the social and psychological consequences for victims of catastrophes (and their relatives). It was said that there will probably be an even more marked increase in the importance of second-, third-, or even fourth-order consequential damage in the future in closely interlinked, highly complex societies with their greater susceptibility to crises.

Restoring public trust

In breaking with old practices of secret deliberations between policy-makers and experts behind closed doors, a new model of shaping regulation is now emerging. It is based on more transparency, accountability, and the involvement of many stakeholders, intending to restore trust in public policymaking. But while more transparency generally leads to more trust, it also creates new challenges, such as selection biases, policy vacuums due to poor communication by regulators, or scientific pluralism instead of expert consensus. Experience shows that despite the new model of close public participation, trust in risk and risk management has not grown substantially. Consequently, more research, training, and education are needed, and media guidelines for more accurate information about science and risks should be developed.

2. MANAGING RISKS IN GOVERNMENT, BUSINESS, AND SOCIETY

Bengt Sundelius

(Swedish Emergency Management Agency)

Bengt Sundelius opened the conference with a short presentation that focused on the management of risks in government, businesses, and society. Pointing to the social contract between those who rule and those who are ruled, he presented the concept of societal security as an alternative to territorial security, which is traditionally seen as one of the main domains of the state. Societal security in this context is defined as the obligation of good government to imagine and prepare for the unthinkable and to allocate the necessary resources to minimize the impact of catastrophic events on individuals and society. It includes the comprehensive effort of all levels of government, public and private actors, and individuals to prevent, prepare for, respond to, and finally recover from events with catastrophic consequences. The security of society is currently affected by several trends such as trans-boundary and real-time flows, technological complexity, second- and third-tier consequences, and the predominance of the media. The real problem is not so much the event in itself, but the unpredictable and unknown cascading effects of the event and spill-over from one sector of the complex societal, political, and economical system to another. This context poses considerable challenges to leadership in crisis. Before and during the decision-making process, modern emergency and crisis management requires that an adequate situational diagnosis be carried out. Further challenges to crisis leadership include the framing of public perception in terms of meaning-making and the taking of responsibility. Finally, the decision-makers have to achieve closure and to start a learning process. For these purposes, cooperation between public and private sectors as well as work across national boundaries are indispensable.

3. PANELS

3.1 Panel I: Identifying information – the use of intelligence

Introduction

Data, facts, and many other forms and sources of information are at the heart of any risk management system. The constant accumulation of information allows analysts to elicit structured and explicit evidence of potential changes in an external environment. In this respect, the collection and processing of information is an essential precondition for spotting upcoming issues at an early stage. This information must be gathered, filtered, framed, analyzed, and put into the context of the relevant risk picture. This task is not made easier, but rather more complex in an information society. While it is evident that information on uncertain future events is by definition vague, imprecise, and incomplete, the information overload we are confronted with today makes it more difficult to identify and select the truly relevant information from the almost infinite amount of information available.

The panel chair, Stefan Brem of the Federal Office for Civil Protection in Berne, introduced the topic and drew attention to methodological aspects of information gathering and identification. This important aspect of any risk management system was addressed specifically by the two panelists, Suzi Lyons and Nathalie Wlodarczyk.

Suzi Lyons

(World Health Organization, Department of Epidemic and Pandemic Alert and Response)

The presentation delivered by Suzi Lyons focused on epidemic intelligence in the WHO. She started her talk by presenting the "International Health Regulations" edited in 2005. The main aim of this first legal agreement on global health is to help to identify events that could threaten public health across international borders and to assess the risk that a given event will have international repercussions. Further goals are the provision of information to other state parties for preparedness and response as well as assistance to affected state parties to control the event. In the framework of an event management process, the Epidemic and Pandemic Alert and Response Department of the WHO uses formal and informal sources of information such as media, national ministries of health, WHO collaborating centers, and other international organizations and NGOs. This network of networks aims to provide global surveillance of infectious diseases. The event management process consists of several steps: it is concerned with information-gathering as well as with initial screening, event verification, risk assessment, and information-sharing. In order to support and facilitate an organization-wide event management process throughout the WHO, an Event Management System (EMS) informs and documents key decisions, but also accommodates and promotes IHR-specific activities and reporting. Regarding the quality of information, the EMS will be much more powerful in the future. Future priorities are to improve the positive predictive value of information sources and to maximize the use of new information and communication technologies (ICTs). Finally, strategic partnerships should be built to improve and diversify the ICTs used for global surveillance and response, and existing risk assessment tools should be adapted and developed.

Nathalie Wlodarczyk

(Exclusive Analysis)

Nathalie Wlodarczyk talked about strategic intelligence-gathering and analysis from the point of view of a private company. Exclusive Analysis is an intelligence company that forecasts violent and political risk. It offers products such as the Country Risk Evaluation and Assessment Model (CREAM) and the Weekly Global Risk Forecast and Intelligence Bulletins on subjects including energy, aviation, money-laundering, and marine/offshore issues, as well as regional editions. The intelligence infrastructure of Exclusive Analysis consists of different levels. At the level of intelligence-gathering, 1,200 specialist sources worldwide collect information using about 70 risk indicators such as the motivations, agendas, and capabilities of involved actors, and work together with 200 regional analysts who verify the information. In this context, the panelist pointed out, it is pivotal to find and manage the 'right sources'. Local knowledge, especially languages and personal relationships, but also external checks aim to assure the quality of intelligence. At the next level, an analysis team in a London-based Global Intelligence Center delivers specific forecasts and assessments based on information from that broad network of sources, but also from an analysis of about 15,000 media sources. At the highest level of the intelligence process, the assessments and forecasts are reviewed by executives and external experts. The final products, Nathalie Wlodarczyk argued, give governments, global firms, international organizations, and NGOs the possibility to engage in proactive strategic planning, maximizing opportunities and mitigating risk.

Comments and Discussion

The subsequent discussion revolved largely around the methodological aspects of information-gathering and identification. The main question addressed in the discussion concerned the reliability of the information, which means how to distinguish the important information from propaganda and rumors. Both panelists highlighted the decisive role of methodology: in the analysis, one must ask the 'right' questions. The questions have to be reviewed over and over again to improve and remake them, if necessary. Regarding the quality of information sources, the importance of establishing personal relationships with the sources was also highlighted, but specialists and experts are still required to verify the information.

3.2 Panel II: Planning ahead – the contribution of early-warning systems

Introduction

In consideration of the multitude of emerging risks and rapidly evolving threats, early-warning systems are indispensable elements of any strategic planning. Potentially dangerous developments must be identified as soon as possible in order to enable the policy-makers to assess and implement the appropriate countermeasures.

In contrast to traditional warning methodologies, which are based on predefined sets of indicators, the concept of early warning takes into account the "weak signals" – the barely perceptible evidence of future trends. However, detecting these weak signals is a very demanding task, and there is no "one-size-fits-all" solution for early-warning systems. Some weak signals may be detected by examining public sources, others by collecting new information or interpreting collected data in new ways. Regardless of how the weak signal has been detected, there will always be a need for further analyses, since weak signals are never explicit. An effective early-warning system should therefore include both data collection capacities and analytical capabilities.

The panel clearly reflected the fact that methods of early warning may differ considerably depending on the area in which they are applied. The panel chair, Myriam Dunn Cavelty, welcomed the panelists, who represented very different organizations, such as the OSCE (Erik Falkehed), the Health Threats Unit of the European Commission (Germain Thinus), the Department of War Studies at King's College (Daniel R. Morris), each of whom presented their own early-warning system. Meanwhile, the presentations made clear that apart from the differences, all early-warning systems depend on a broad network of well-placed partners, and on open-minded and experienced analysts.

Erik Falkehed

(OSCE Conflict Prevention Centre)

Erik Falkehed's presentation focused on early warning in the Conflict Prevention Centre (CPC) of the OSCE. Originally established to assist the Council of the OSCE in reducing the risk of conflict, the responsibilities of the CPC have changed and extended considerably. Today, the CPC is responsible for early warning in the field of conflict prevention and crisis management. This means that the CPC is not solely concerned with early warning in the area of traditional military conflicts, but also has to deal with risks like crime, disasters, or terror. In the context of an international organization, early warning in all these areas is crucial for any timely reaction, since the consensual decision-making process in multilateral bodies usually takes a lot of time.

In order to collect information about emerging threats, the CPC uses formal and informal channels. Due to the field operations of the OSCE, the CPC has a broad network of contacts at its disposal. Important sources of information include other institutions, delegations of the OSCE, as well as the representatives of the countries. These partners are often very well placed to get relevant information, because they are all closely in touch with the developments on the ground.

Through its contacts with various partners, the CPC pursues a very pragmatic approach of early warning. However, the information of these sources

tends to be ad-hoc and incomplete and needs to be analyzed carefully. In addition, these sources are of limited use for information about developments outside of the area of the OSCE. For these cases, the CPC has to find other sources.

Erik Falkehed concluded by mentioning that it is not enough to build up strong early-warning capacities – the warnings have also to be transformed in political action. Therefore, analysts must know the specificities of their audience (e.g. the sensitivities of member states in an international organization) and they must also be aware of the fact that the reaction time of policy-makers might be quite long.

Germain Thinus

(European Commission, Health Threats Unit)

Germain Thinus talked about early warning in the health sector; in particular, he presented the early-warning and response tools of the EU Health Emergency Operation Facility (HEOF). These early-warning and alert systems serve to support member states in handling health-related crises; to improve the European Commission's awareness; and to facilitate co-operation and information-sharing.

In order to detect any signals that may be relevant for public health, many different sources of information have to be used. The primary contacts for the HEOF are the ministries of public health in all member states of the EU. Furthermore, it exchanges information with many other agencies such as the WHO, NATO, Europol, and the EMEA (European Medicines Agency). Besides the exchange with other agencies, the HEOF has also established a tool for "scanning the horizon", namely, the Medical Intelligence System (MedISys). This system is designed to collect information from various public sources, which include 1,000 news sites and 100 public health sites.

In the case of an incident, the responsible authorities of all member states must be informed as quickly as possible. Therefore, the HEOF has three different alert and early-warning systems at its disposal: The Early Warning and Response System (EWRS) for general communicable disease threats; the Rapid Alert System for Biological and Chemical Agents (RAS-BICHAT); and the Rapid Alert System for Chemical Incidents (RAS-CHEM). These alert systems are equipped with modern communication tools such as Short Message Service (SMS) and are linked to other rapid-alert systems of the EU Commission.

In the context of public health, many different sources of threats have to be considered, and the threats must be tackled very quickly in order to prevent diseases from spreading rapidly. Thus, several early-warning systems are established within the network of public health agencies of the EU, and the communication channels to the policy-makers are very direct.

Daniel R. Morris

(King's College, Department of War Studies)

Daniel R. Morris's presentation provided insights into the Strategic Early Warning System for organized and serious crime (SEWS) of the Criminal Intelligence Service of Canada (CISC), which he co-developed in 2004. He began by outlining the importance of early warning in the domain of law enforcement. As organized crime is transnational, clandestine, networked, adaptive, and connected, it is difficult to identify

stable indicators that can be used to monitor trends. In the constantly changing context of organized crime, there are always unknown factors that need to be identified in order to enable accurate response strategies. The early-warning system of the CISC was developed with the help of experts, and the methodology was constantly refined. Now it is conceptualized as a bottom-up, analyst-driven approach that consists of three different processes. It begins with threat perception including environmental scan and scenario-building. Then it moves to threat evaluation and monitoring. The collected data must be placed in a strategic context and changes of the threat level should be reflected. Finally, the process of early warning results in the threat assessment and warning. The findings have to be formulated in a concise and accessible format for decision-makers.

By developing the early-warning system, the CISC learned that early warning is a distinctive type of analysis and requires more than a comprehensive collection of data. It demands imaginative skills for the scenario-building process; analytical skills to assess new findings; and communication skills to transform the findings in understandable and coherent warnings for the policy-makers.

Comments and Discussion

In the discussion, all three panelists again stressed the importance of communication. The warnings must be heard by the policy-makers. Depending on the audience and the context, this might be difficult to achieve. Therefore, personalized contacts with decision-makers are especially useful.

The question of how to tackle the unknown factors was subsequently raised. The panelists admitted that there is no easy solution for this problem; however, by sharing information with other organizations and by implementing structures that allow the analysts to think out of the box, it is possible to detect weak signals at an early stage.

3.3 Panel III: Transferring knowledge – explaining risks to decision-makers

Introduction

A key challenge for risk management is to convince decision-makers of the relevance of upcoming risks and threats in order to implement adequate countermeasures. Several institutional, cultural, or psychological factors may prevent an optimal exchange of knowledge between analysts and policy-makers, thus leading to unrealistic expectations, misunderstanding, or recriminations. Decision-makers may not be satisfied with the statements about emerging threats, possible scenarios, or proposed countermeasures as delivered by the experts; analysts, on the other hand, may accuse policy-makers of not taking their analyses and warnings into account, of not taking actions or taking the wrong ones, and of shifting the blame to them in the event of a crisis. A better understanding of the respective specific positions and needs is a key element for improving the transfer of knowledge with regard to an optimal risk management. The panel chair, Christopher Bunting of the International Risk Governance Council in Geneva, opened the panel by pointing out these challenges to the task of informing policy-makes with expert knowledge.

Gareth W. Shepherd

(World Economic Forum, Global Risk Network)

Gareth W. Shepherd from the World Economic Forum's (WEF) Global Risk Network in Geneva, which addresses non-business risks that affect business, focused on the inherent challenges of explaining risks to decision-makers and on the challenges of getting risks on the agenda of the WEF gathering in Davos. It is important to note that business executives make incentives-based decisions, they tend to be over-confident as concerns risks, and they are often unaware of risks. Moreover, as risks are highly interconnected, the extreme complexity of interdependencies is often neglected. This context poses serious challenges to the effective communication of risks. In order to mitigate the global risks within such an environment, it is necessary to address issues of business continuity and the potential for analogies between government agencies and individual firms in concrete terms in the learning process. Furthermore, the massive interdependencies can only be addressed by collective efforts, and the networking of communities is indispensable. Unfortunately, the least likely risks are often the ones most frequently discussed.

Martin J. Eppler

(University of Lugano, Chair of Information and Communication Management)

Martin J. Eppler, Chair of Information and Communication Management at the University of Lugano, argued in his presentation that it is the collaborative knowledge visualization of risk analysts and decision-makers that makes risk communication most effective, due to their engagement in a joint rationalization process. He pointed out and elaborated on the numerous barriers that frequently impede the effective transfer of risk-related knowledge from experts to decision-makers. The problem patterns in risk communication are grouped along five key issues stemming from suboptimal behavior of both sides, experts and decision-makers, and their respective roles. While the analysts are highly specialized, focused on details, and tend to be risk-averse, the policy execu-

tives need to be generalists, action-oriented, and tend to be opportunity-seeking. On the one hand, experts in general and risk analysts in particular are often ineffective in presenting their risk analysis to political executives because they either get lost in technical jargon or ambiguous terminology, or overload their communicable analysis with details, or do not sufficiently show the practical implications of their findings; in short, risk analysis is often not adequately tailored to the cognitive needs of decision-makers. A second problem stemming from the analysts' side is the potential bias of expertise. Sometimes, the problem arises of experts succumbing to the temptation of trying to 'tune' their audience. They then go beyond their field of expertise in the analysis, providing biased expertise. On the other hand, there are also problem patterns that stem from the decision-makers, such as the 'political' distortion of expert analysis leading to a misuse of expertise or the so-called premature closure of an issue, which occurs when a decision-maker no longer considers the evolution of an issue due to his or her earlier established stance on it. Moreover, policy executives are susceptible to what is called the prophet syndrome, i.e., searching for authoritative expertise from outside while disregarding essential internal knowledge. At certain moments, the outright inability to ask the right and relevant questions or the inconsistent weighting of expert analysis contributes to the neglect of risk expertise. Thirdly, there are also problems of risk communication commonly caused by experts and executive actors, such as the general lack of a common ground or the invocation of reciprocal stereotypes between both analysts and decision-makers, but also the lack of mutual and institutionalized feedback, all of which lead to mismatched communication.

In order to overcome these various problems in risk communication, Prof. Eppler suggested four measures: the creation of rules and standards, the creation of a common ground, the establishment of an iterative process of communication, and the intention to secure and use the lessons of previous experience. To illustrate such a process of joint sense-making of experts and decision-makers, he briefly presented a so-called risk-ruler software tool, a dynamic database that helps evaluate the total risk impact factor.

Comments and Discussion

In the discussion several key issues where raised again. The importance of not setting artificial deadlines in crisis communication was stressed as well as the need to be aware of and avoid cognitive biases. Moreover, traceability as a key element to adequate risk assessment and communication was highlighted. Transparency is helpful in order to assure that, first, an assessment is not altered, or if it is, these changes are visible in transmission; and second, traceability ensures that a memory exists of the process of risk assessment. Further it was pointed out that dealing with risks inherently means also dealing with uncertainty. Nevertheless, there is a tendency to avoid the articulation of uncertainties. While Mr. Eppler insisted on the importance for analysts to indicate the level of (un)certainty of their assessment, Mr. Shepherd stressed the importance for analysts to weight their assessments towards the consequences in order to be heard. The pricing of risks in terms of financial costs but also in terms of potential casual-

ties does, according to Mr. Shepherd, help decision-makers to implement the recommendations issued by analysts. Therefore, Mr. Eppler insisted, it is imperative for experts to present their findings such that they are memorized, by e.g. recurring to anecdotes and metaphors. From a risk-management point of view, both crisis and risk communication should attempt to bring the knowledge and the implementation together. Important herein is, as the panel chair Christopher Bunting carved out in his concluding remarks, that there are political agenda-setting processes taking place with regard to low-probability risks that need to be taken into consideration.

3.4 Panel IV: Emergency planning and response – coping with crisis situations

Introduction

Even if risks are identified in a timely manner, their evolution is tracked effectively, and adequate preventive countermeasures are taken, there is no absolute guarantee that they will never manifest themselves. Even the best risk management cannot prevent disastrous events altogether. There is always the possibility that a potential risk will turn into a real threat, and ultimately lead to a crisis. Effective emergency planning is therefore the logical further development of a meaningful risk management system. It is indispensable for any clear-sighted institution to develop operational contingency plans and effective emergency response plans in order to adequately prepare itself for crisis situations. The panel chair Marco Lombardi introduced two presentations by Edward P. Borodzicz, professor of Risk and Crisis Management at the University of Portsmouth, and by Mr. Simon Turney, emergency planning adviser and consultant, South Yorkshire.

Edward P. Borodzicz

(University of Portsmouth Business School)

Edward Borodzicz presented "Project Argus", an applied knowledge transfer and training simulation project to look at security and resilience in complex and crowded areas and at measures that can be taken to make the local community, businesses, and infrastructure more resilient against various catastrophic incidents, particularly a terrorist attack.

Traditional approaches to emergency response follow a top-down process where the emergency services, once they have arrived at the scene, tell the affected people what to do and how to behave. However, given the fact that the emergency services need some time to get to the scene of an incident and bearing in mind that the effects may turn out to be worse than a terrorist attack itself, Project Argus investigated and trained the feasibility of building resilience in crowded areas by raising the awareness and preparedness of people living and working in such crowded places. The aim of building resilience among local stakeholders as envisaged by Project Argus is to facilitate their capabilities for:

- The provision of immediate first aid to victims (first phase: e.g., injuries, food, water, clothes);
- Limiting the effects of a disaster especially in the first hours after an incident (second phase: "buddying"; e.g., contact staff, consumers, other businesses); and to
- Ensure business continuity (third phase: e.g., to prevent bankruptcy in small businesses).

In Phase 1 of Project Argus, the simulation tool was developed and tested in two locations in Portsmouth and Liverpool in 2006. The exercise ran for one morning as an interactive role-play simulation. The attendees grouped together in small mixed groups in order to get to know each other and to solve virtual problems to be expected from a terrorist attack, as well as to meet with emergency services and local emergency planning officers (EPOs). In Phase 2, the project is being expanded into a national training tool to improve resilience in 250 crowded locations in the UK. Learning points of Project Argus include the following:

- Get to know and help each other (business buddies) as well as the EPOs;
- Identifying the specific skills of local businesses and individuals relevant for a crisis situation;
- Media training to help local businesses avert damage to their own business after an incident (e.g., sustain trust in a local business area so that consumers return); and an
- Improved risk communication, so that people understand possible risks, become aware of them, and are accordingly more resilient.

The simulations were designed and run by Portsmouth University for the UK's National Counter Terrorism Security Office (NaCTSO) with a special focus on terrorist incidents. However, Project Argus provides generic training that is applicable to other types of disasters.

Simon Turney

(Emergency Planning Lobbyist and Consultant)

In the second presentation of Panel IV, Simon Turney talked about the consequences of inadequate disaster management, i.e., post-disaster incidents or "Second Disasters" with respect to the inadequate behavior of emergency responders, whose response is often too "technical", desensitized, and inhuman. People can and do cope with the aftermaths of death and destruction in the most appalling disasters. They can be resilient and rebuild their lives after a disaster with their experiences melded into their new realities. What angers people beyond measure, and corrodes and embitters their new realities, is callous disregard for their plight by the organizations tasked to rescue, succor, and support them in their time of need. Citizens often become mere objects for the responding authorities, are lied to and disrespected, and sometimes the victims are even blamed by the media and public bodies.

"Second disasters" occur when disaster responders treat disaster victims with contempt and ignorance. Disasters are by nature times of high intensity, so memories are sharp, detailed, and long-lasting. These second disasters create residues of resentment and anger that can endure beyond the generation affected by the initial disaster.

Simon Turney mentioned several examples of misbehavior by emergency responders, such as the 1966 Aberfan coal mine disaster, the 1989 Hillsborough football stadium disaster, the 1996 Dunblane Primary School massacre, and others. With reference to these catastrophes, he denounced the behavior and partial guilt of police forces, other emergency responders and corporations, as well as the sometimes shocking and disrespectful treatment of victims and relatives, all of which had long-lasting effects on people's minds until today. He fostered the following practical steps to avoid such a second disaster:

- Expect the second disaster and look for early signs;
- Train and tell disaster responders how they can and cannot behave;
- Keep all the evidence of a disaster and the subsequent emergency management, however uncomfortable;

- Remember that corporate amnesia endeavors to immunize today's managers from yesterday's blunders;
- Maintain integrity as first responder/victim;
- Build respect into the fabric of all training;
- Move observers in early, including cameras; and
- People generally behave well, whereas organizations tend to behave appallingly.

Comments and Discussion

The subsequent Q&A session on Panel IV centered on the expectations of citizens with respect to emergency management strategies and the training and attitude of first responders, especially of police forces. It was stated that people want to help in crisis situations and that they should be honestly empowered to do so, not least because it is their community that is affected and because it gives them a feeling of satisfaction to do so. As regards the police forces, it was stated that the desensitization of certain units is programmatic, leading to inhuman behavior. On a tactical level, participants discussed the problem that some incidents, such as the Hillsborough football disaster, were dealt with as a matter of maintaining public order instead of a public safety issue by the police, turning many victims into wrongdoers.

4. KEYNOTE ADDRESS RISK COMMUNICATION IN THE 21ST CENTURY

Introduction

Risk comunication stretches across all relevant phases of an effective risk management system. Its goal is to ensure an intentional (not accidental) transfer of information designed to respond to public concerns or public needs related to real or perceived hazards. The concrete approach varies according to the audience that the message is targeted at (the general public, the media, organized interests, other governmental agencies, private corporations), the specific moment in time at which communication is attempted (crisis situation, before or even after a hazardous event), or the different objectives it may pursue (acquiring, promoting, and sustaining public trust and credibility; controlling the flow of information; or evaluating and optimizing risk communication after a crisis). The keynote speaker, Ragnar Loefstedt, professor of Risk Management and director of King's Center of Risk Management at King's College London, tackled these issues, arguing that risk communication in Europe has undergone profound changes over the past 20 years. He briefly outlined the changes that have occurred over time in order to discuss some of the resulting teething problems that now need to be addressed.

Ragnar Loefstedt

(King's College, King's Centre for Risk Management)

Prof. Loefstedt started his talk by first giving a brief theoretical overview over risk perception, management and communication. Several differentiations help to conceptually seize risk and its communication. It is important whether a particular risk stems from natural hazards or from technological hazards for the public evaluation of it. The acceptance of voluntary risks such as those potentially stemming from the use of mobile phones is higher than the one stemming from involuntary risks such as the deployment of a mobile phone antenna. Furthermore, people are more worried about unfamiliar risks like SARS than about more familiar ones like catching a flue. The potentially controlled risk of driving a car is perceived lower than the uncontrolled one of taking an airplane. Also risks involving children cause more worries than those that do not and women are more risk sensitive than men.

There are several different principles of risk communication. The top-down approach to risk communication does, according to Prof. Loefstedt, not work. As an example he invoked the policy executive responsible during the mad cow crisis in the United Kingdom whom's daughter was publicly eating a hamburger. The fear did not decrease. The dialogue approach to risk communication attempts to empower the community while the bottom-up approach to risk communication traces the way from an issue related problem, to become a local one and finally a national one. Moreover, a narrative approach to communicate risks is highly important since people do not like abstract numbers when stakes rise to become tangible concerns of their lives. Also, one should be aware of the tendency of what is called the social amplification of risks which does for example set in after an airplane accident. Also, trust is often key to public risk perception. A high level of public trust does often combine with a low level of publicly perceived risk and vice versa.

Prof. Loefstedt argued that risk communication suffers from a lack of trust in society due to failing policy-makers having lead to a decline in trust across

entire Europe. This decline in public trust is also linked to a number of scandals in risk communication such as in the case of the mad cow and the associated Creutzfeldt-Jakob disease where any relation was first denied. Of course, afterwards people thought that they were lied at. This led to a change in the making of regulation from the old so-called consensus model according to which deliberation between policy makers and industry representatives took place behind closed doors and according to which scientists had an important role to play insofar as they were outlining the pros and cons of regulatory actions for the elites, to a new model which is now based on greater transparency, more accountability, the involvement of the public and the stakeholders, and according to which science plays less of a role, as scientific results are increasingly questioned and scientists seen as just another stakeholder.

A number of teething problems arise from this change: the call for greater public and stakeholder participation often leads to a selection bias problem. That is to say that the persons interested in participating in exercises are not representative of the aggregate of the public. This does not increase public trust, of course. A second problem associated with regulatory model change is that the involvement of stakeholders can lead to a decrease in public trust due to the separate agendas stakeholders may pursue. Moreover, the increase of transparency is surely a positive impetus for trust but can nonetheless lead to some problems such as the creation of policy vacuums since policy-makers and regulators are unfortunately often poor communicators. Also does transparency forge scientific pluralism where before there was consensus. This too does not increase public trust. Hence, notwithstanding the new model, increasing the power of the public and in particularly of the stakeholders, public trust in policy related to risk, its management, and its communication has not grown substantially. Due to the increasingly aggressive media the above mentioned problems are even aggravated. So, what should be done? Answering to this question, Prof. Loefstedt pointed out four concrete measures. First he argued, more risk communication workshops should be done in particular in collaboration with the new EU-memberstates. Second, more research should be conducted on both the deliberation process including the participation therein and on how to address the problems stemming from transparency. Third, an EU academy of sciences should be established in order to address risk issues on the level of evaluating whether and which risks are real and which ones are artificially produced. This academy should become an authoritative entity. And fourth, media communication guidelines should be developed so that the media does accurately communicate science, (un)certainty, and risk.

Comments and Discussion

The short discussion after the keynote address centered on the very last and provocative point made by Prof. Leofstedt. Discussion evolved around the freedom of the press on the one hand and the social responsibility the media systems have to assume on the other hand. Unfortunately some media are not ready to absorb this social responsibility since they are purely market driven. Another media related problem stems from the new technologies potentially making of every citizen a 'journalist'.

5. WORKSHOPS

5.1 Breakout group I: Terrorism

Variously described as actors engaging in "asymmetric warfare" or "sub-conventional warfare", as "sub-state actors", or simply as "terrorists", political violence movements have disrupted and destabilized democratic countries and other forms of states at all times. They have increasingly become one of the major focuses of international security since the end of the Cold War and have been perceived as such by a large global public since September 2001. While the debate on a common definition of terrorism is unlikely ever to cease entirely, there is agreement on three characteristics of terrorism: the goal of spreading fear, the political motivation, and the fact that actions are perpetrated by sub-national/clandestine actors. Due to the inherent uncertainty of the potential terrorist threat and its simultaneous urgency in terms of societal psychology, governmental counterterrorism policies succumb to the same logic as those of risk government. Contemporary political violence movements have developed along innovative lines combining highly flexible, decentralized organizational forms, advanced logistics, and operational experience with increased mobility of actors and the use of information and communication technology, and thus challenge the state on an ever-changing terrain. With this context in mind, the breakout group discussed the conceptual challenges of fighting political extremism by applying insights to early warning and crisis management.

First, the discussion addressed the specific challenges in implementing an effective information-gathering and early-warning system related to political violence movements. Multiple points were raised, such as the importance of imaginative threat perception in order to increase the potential for gathering relevant information. The fundamental difference between the attempt to prevent a terrorist incident stemming from an already known and existing group and one stemming from a potential new movement was pointed out. Moreover, the issue of how to (re-) organize complexity relative to information-gathering and to information analysis was raised.

The second major set of questions addressed was centered on the nature of key precautionary measures in order to prepare for a crisis situation stemming from a terrorist incident. First the group discussed whether crisis management related to terrorist incidents is fundamentally different from accident crisis management, and if so, to what extent. Then the issue of communication during a crisis was raised. It is very important to communicate immediately in the event of a crisis, even if not all information is available. Spokespeople should state clearly what is known and what is not. Last but not least, matters of resilience were addressed. Societal resilience is better in cases where people have experienced crisis. Officials and experts must therefore consider ways to enhance the resilience of their societies if the latter have not experienced crisis situations in the recent past. What is also required is an awareness that vulnerabilities have increased immensely in contemporary societies.

5.2 Breakout group II: Pandemic diseases

According to the World Health Organization (WHO), the world has now moved closer to a pandemic than at any time since 1968, and all the prerequisites for the start of a pandemic have been met with the emergence of the H5N1 influenza subtype, except for the evolution of an efficient human-to-human transmission. An outbreak could have disastrous implications. Based on the experience of past pandemics, the WHO estimates that even under optimistic assumptions, between 2 and 7 million people would die worldwide as a result of an H5N1 influenza pandemic, and tens of millions would require medical attention. In the worst case, the human death toll could rise to more than 50 million. Besides the fact that there is hardly a national public health system that would be capable of handling the grave medical consequences of a catastrophic influenza pandemic, the impact on society in general would be devastating. Even in unaffected countries, fear, panic, and chaos would spread. Large parts of the workforce might be absent from work for months, while domestic and foreign trade, travel, and transportation would be reduced or halted, and a wide range of essential commodities, such as food, fuels, and medicines would be in short supply. In other words, an outbreak would cause huge economic loss. Since an influenza pandemic cannot be avoided altogether, all that remains is to lessen its impact through preparatory measures. The most important of these are the development and stockpiling of strain-specific vaccines, and, as a second line of defense, the storage of antiviral drugs.

Three key issues were discussed in the workshop on pandemic diseases, namely early warning, risk and crisis communication, and precautionary or response measures. As regards early warning, the panel agreed that a lot has happened in this respect since the SARS epidemic of 2002/2003 and that the technology for early warning relating to a pandemic disease is in place. However, various imminent problems and issues remain:

- Early warning of what? Today, many actors expect and prepare for a H5N1 influenza pandemic, but there is a possibility that the virus might mutate further or that another influenza subtype or even an emerging disease, such as SARS, could take on pandemic proportions. Depending on the exact nature of a pandemic, other countermeasures are needed.
- A problem is the inability or unwillingness of non-transparent societies to communicate openly on disease outbreaks. An understanding is needed in these countries that open communication is required internally and externally and that information has to flow rapidly, where it usually does not. In addition, laboratories and other necessary capacities are often not available in developing countries.
- How is the information derived from early-warning systems to be processed? For instance, information on SARS quickly became available, but initially, nobody knew what to do with it and how this particular problem had to be understood and dealt with.

The issue of risk/crisis communication vis-à-vis society and decision-makers also poses some serious problems:

- What is the decision trigger? Is this point reached when a disease outbreak becomes apparent, or should it be based on a situational and rather "abstract" risk assessment? Decision-makers must understand that it is not necessarily bird flu that may become pandemic.
- How and when do you inform the population without risking fear and panic? An unknown threat induces an instinctive reaction, and it was agreed in the panel that authorities generally underestimate the worries of the population. In contrast, the media in industrialized societies are now increasingly becoming silent on the issue although it is still imminent – no media coverage, no issue.
- The provision of multiple or contradictory messages by varying authorities is a problem. For instance, some officials may emphasize the continuing smooth operation of society with all its sectors, while public health institutions tell people to stay at home in order to prevent new infections.

As regards precautionary/response measures, the following points were discussed in the panel:

- Many countries have dealt with the problem of a pandemic as a mere health issue. However, it is becoming increasingly clear that, if hit hard, society becomes affected as a whole. A pandemic has the potential for a "super crisis" requiring the mobilization of the whole society.
- The limits of what people are ready to accept during peacetime would soon be reached, but such issues have to be preplanned and dealt with. It may become necessary to impose movement restrictions and close borders; infected people have to be forced to stay in hospital; others need to be forced to go to work (e.g., nurses); etc. Such infringements on basic human rights may be in the public interest and necessary for the sake of early containment, but require a legal basis and serious preplanning of all the associated problems that may arise.
- On top of that, the stocks of vaccines and antiviral drugs (assuming that the right ones have been developed and obtained for a specific pandemic disease) are insufficient in many countries, requiring a selective distribution within a population. How do you distribute them and explain that the selection of recipients?
- If such issues are handled and communicated badly, the outbreak of civil unrest is likely. People might start to act on their own; large parts of the workforce might be absent; infrastructure problems could arise; food and water supplies may run out; people could start to loot grocery stores or transports of antiviral drugs; riots could break out; etc.

5.3 Breakout group III: Critical (information) infrastructure protection

Critical Information Infrastructure Protection (CIIP) is perceived as a key part of national security in numerous countries today. A critical infrastructure is commonly defined as an infrastructure or asset the incapacitation or destruction of which would have a debilitating impact on the national security and the economic and social welfare of a nation. As most of these infrastructures are built upon or monitored and controlled by vulnerable ICT systems, the "cyber"-infrastructure has become the new focal point of protection policies. States face various challenges in the field of CIIP, since technical, economic, organizational, law-enforcement, and security-policy aspects have to be taken into account. Adding to the challenge is the fact that many critical information infrastructures are owned and operated by the private sector. Thus, governments must find new ways of interaction and cooperation with actors that have not traditionally been part of the security arena.

The participants applied some of the insights gained in the panel sessions on the issue of Critical Infrastructure Protection (CIP). It was outlined that there are many potential threats to critical information infrastructures (e.g. technical failures, natural hazards, human error, or malicious attacks) and that infrastructures are highly interdependent. These challenges for governmental risk management are aggravated by the fact that many infrastructures are operated by private companies. In order to build up early-warning systems in the domain of CIP, it is therefore essential to establish information-sharing between different infrastructure sectors, as well as between the private actors and the government.

Many countries have already established basic early-warning capacities in the domain of CIP, but these usually only deal with known threats. As CIP is often perceived as a mainly technical task, social-political and economical impacts are sometimes neglected. Referring to Dave Snowden's Cynefin framework, which delineates four relationships between cause and effect (simple, complicated, complex, and chaotic), it was stressed that there are not enough tools to tackle complex and chaotic questions in the domain of CIP.

6. CONFERENCE PROGRAM AND PARTICIPANTS LIST

6.1 Agenda

OPENING NIGHT: THURSDAY, 14 JUNE

19:00 Opening Reception
Hotel "Waldstätterhof", Brunnen

19:45 Welcome (Center for Security Studies)
Move to Tables

20:00 Dinner

DAY 1: FRIDAY, 15 JUNE

08:30 CRN Welcome Address and Outline of Seminar Concept

08:45 Managing risks in government, business, and society
Bengt Sundelius
Swedish Emergency Management Agency, Stockholm

09: 15 Panel Session I: Identifying information – the use of intelligence
Panel Chair: Stefan Brem, Federal Office for Civil Protection, Bern
Suzi Lyons, World Health Organization, Department of Epidemic and Pandemic Alert and Response, Geneva
Nathalie Wlodarczyk, Exclusive Analysis, London

10:30 Coffee

11:00 Panel Session II: Planning ahead – the contribution of early-warning systems
Panel Chair: Myriam Dunn Cavelty, Crisis and Risk Network, Zurich
Erik Falkehed, OSCE Conflict Prevention Center, Vienna
Daniel R. Morris,, King's College, Department of War Studies, London
Germain Thinus, European Commission, Health Threats Unit, Luxembourg

12:30 Lunch

14:00 Panel Session III: Transferring knowledge – explaining risks to decision-makers
Panel Chair: Christopher Bunting, International Risk Governance Council IRGC, Geneva
Gareth W. Shepherd, World Economic Forum, Global Risk Network, Geneva
Martin J. Eppler, University of Lugano, Chair of Information and Communication Management, Lugano

15:15 Coffee

15:45 Panel Session IV: Emergency planning and response – coping with crisis situations

Panel Chair: Marco Lombardi, Catholic University of the Sacred Heart, Milan

Edward Borodzicz, University of Portsmouth, Business School, Portsmouth

Simon Turney, Emergency Planning Consultant (formerly Director of Emergency Planning), South Yorkshire

17:00 Wrap-up

17:30 Adjourn

19:00 Dinner

DAY 2: SATURDAY, 16 JUNE

08:30 Summary and Reflections on Day 1 (Panel Sessions I-IV)

09:00 Keynote Address: Risk Communication in the 21st Century

Ragnar E. Loefstedt, King's College, King's Centre for Risk Management, London

10:00 Coffee

10:30 Workshops

Breakout groups on terrorism, pandemic diseases, and critical (information) infrastructure protection

11:45 Reporting on Workshops

12:15 Wrap-up and Closing Remarks

12:45 Lunch

14:00 Excursion: Mount Rigi (optional)

6.2 List of participants

Balmer Jürg (juerg.balmer@babs.admin.ch)	Federal Office for Civil Protection (BABS), Bern, Switzerland
Bergan Tone D. (tone.bergan@dsb.no)	Directorate for Civil Protection and Emergency Planning (DSB), Norway
Bonin Sergio (bonin@sipo.gess.ethz.ch)	Crisis and Risk Network, Center for Security Studies, Zurich, Switzerland
Borodzicz Edward (Edward.Borodzicz@port.ac.uk)	University of Portsmouth Business School, Risk and Crisis Management, Portsmouth, UK
Brem Stefan (stefan.brem@babs.admin.ch)	Federal Office for Civil Protection (BABS), Risk Analysis and Research Coordination, Bern, Switzerland
Brunner Elgin (brunner@sipo.gess.ethz.ch)	Crisis and Risk Network, Center for Security Studies, Zurich, Switzerland
Bunting Christopher (christopher.bunting@irgc.org)	International Risk Governance Council (IRGC), Geneva, Switzerland
Burkhalter Fred (fred.burkhalter@bwl.admin.ch)	Federal Office for National Economic Supply (BWL), Bern, Switzerland
Dawes Terry (terry.dawes@commissum.ch)	Business Continuity Institute BCI Switzerland, Zurich, Switzerland
Doktor Christoph (doktor@sipo.gess.ethz.ch)	Crisis and Risk Network, Center for Security Studies, Zurich, Switzerland
Dunn Cavelty Myriam (dunn@sipo.gess.ethz.ch)	Crisis and Risk Network, Center for Security Studies, Zurich, Switzerland
Eppler Martin J. (martin.eppler@gmail.com)	University of Lugano, Chair of Information and Communication Management, Lugano, Switzerland
Falkehed Erik (Erik.Falkehed@osce.org)	OSCE Conflict Prevention Center, Vienna, Austria
Geveke Henk (henk.geveke@minbzk.nl)	Ministry of the Interior and Kingdom Relations (BZK), Netherlands
Gullotta Giulio (Giulio.Gullotta@bbk.bund.de)	Federal Office of Civil Protection and Disaster Assistance (BBK), Germany
Habegger Beat (habegger@sipo.gess.ethz.ch)	Crisis and Risk Network, Center for Security Studies, Zurich, Switzerland
Henriksen Stein (stein.henriksen@nsm.stat.no)	Norwegian National Security Authority (NSM), Norway
Jeanty Bernard (bernard.jeanty@dsp.admin.ch)	Directorate for Security Policy (DSP), Bern, Switzerland
Karlsen Marianne (Marianne.Karlsen@dsb.no)	Directorate for Civil Protection and Emergency Planning (DSB), Norway
Käslin Bruno (bruno.kaeslin@unisg.ch)	University of St.Gallen, Institute of Insurance Economics (IVW-HSG), Switzerland
Kessler Rainer (rainer.kessler@ch.ey.com)	Ernst & Young, Technology and Security Risk Services, Switzerland

Klopfstein Matthias (matthias.klopfstein@fedpol.admin.ch)	Federal Office of Police, Service for Analysis and Prevention, Bern, Switzerland
Knudsen Øistein (Oistein.Knudsen@dsb.no)	Directorate for Civil Protection and Emergency Planning (DSB), Norway
Lanitis Johanna (johanna.lanitis@weforum.org)	World Economic Forum, Global Risk Network, Geneva, Switzerland
Lehmann Peter (peter.lehmann@deza.admin.ch)	Swiss Agency for Development and Cooperation (SDC), Bern, Switzerland
Loefstedt Ragnar E. (ragnar.lofstedt@kcl.ac.uk)	King's College, King's Centre for Risk Management, London, UK
Lombardi Marco (marco.lombardi@unicatt.it)	Catholic University of Sacred Heart, Milan, Italy
Lundberg Jan (jan.lundberg@krisberedskapsmyndigheten.se)	Swedish Emergency Management Agency (SEMA), Sweden
Lyons Suzi (lyonssu@who.int)	World Health Organization, Department of Epidemic and Pandemic Alert and Response, Geneva, Switzerland
Mauer Victor (mauer@sipo.gess.ethz.ch)	Center for Security Studies, Zurich, Switzerland
Moholt Ingunn (ingunn.moholt@dsb.no)	Directorate for Civil Protection and Emergency Planning (DSB), Norway
Morris Daniel R. (daniel.3.morris@kcl.ac.uk)	Department of War Studies, King's College, London, UK
Mueller Nicolas (Nicolas.Mueller@vtg.admin.ch)	Swiss Armed Forces, Bern, Switzerland
Myrdal Sara (sara.myrdal@kbm-sema.se)	Swedish Emergency Management Agency (SEMA), Sweden
Niederhäuser Paul (paul.niederhaeuser@cremo.ch)	Cremo SA, Fribourg, Switzerland
Peduzzi Fabio (Fabio.Peduzzi@stab-sia.admin.ch)	Staff of the Federal Council's Security Committee, Bern, Switzerland
Ruegger Frederick (frederick.ruegger@ch.thalesgroup.com)	Thalesgroup Switzerland
Rybach Manuel (manuel.rybach@credit-suisse.com)	Credit Suisse, Public Policy, Zurich, Switzerland
Schmid Susanne (schmid@sipo.gess.ethz.ch)	Crisis and Risk Network, Center for Security Studies, Zurich, Switzerland
Schmidt Przemylslaw (schmidt@sipo.gess.ethz.ch)	Center for Security Studies, Zurich, Switzerland
Shepherd Gareth W. (Gareth.Shepherd@gmail.com)	World Economic Forum, Global Risk Network, Geneva, Switzerland
Squires Chloé (chloe.squires@cabinet-office.x.gsi.gov.uk)	Cabinet Office, Civil Contingencies Secretariat, Resilience Capabilities & Risks, London, UK

Sundelius Bengt (bengt.sundelius@krisberedskapsmyndigheten.se)	Swedish Emergency Management Agency (SEMA), Sweden
Suter Manuel (suter@sipo.gess.ethz.ch)	Crisis and Risk Network, Center for Security Studies, Zurich, Switzerland
Thinus Germain (Germain.Thinus@ec.europa.eu)	European Commission, Health Threats Unit, Luxembourg
Turney Simon (simon@qdconsult.co.uk)	Emergency Planning Lobbyist and Consultant, South Yorkshire, UK
Valterio Françoise (Francoise.Valterio@stab-sia.admin.ch)	Staff of the Federal Council's Security Committee Bern, Switzerland
van Dam Anja (anja.dam@minbzk.nl)	Ministry of the Interior and Kingdom Relations (BZK), Netherlands
Weymann Martin (Martin_Weymann@swissre.com)	Swiss Reinsurance Company, Sustainability & Emerging Risk Management, Zurich, Switzerland
Wlodarczyk Nathalie (Nathalie.Wlodarczyk@exclusive-analysis.com)	Exclusive Analysis, London, UK
Zellweger Kaspar (zellwek7@hei.unige.ch)	Graduate Institute of International Studies (HEI), Geneva, Switzerland
Zimmermann Doron (doron.zimmermann@soliswiss.ch)	Soliswiss, Political Risk Advisors, Bern, Switzerland

CSS
ETH Zurich

The Center for Security Studies of the ETH Zurich (Swiss Federal Institute of Technology) was founded in 1986 and specializes in the fields of international relations and security policy. The Center for Security Studies is a member of the Center for Comparative and International Studies (CIS), which is a joint initiative between the ETH Zurich and the University of Zurich that specializes in the fields of comparative politics and international relations.

The Crisis and Risk Network (CRN) is an Internet and workshop initiative for international dialog on national-level security risks and vulnerabilities, critical infrastructure protection (CIP) and emergency preparedness. Originally launched as a Swiss-Swedish Initiative, the partner network today consists of partners from six countries: the Federal Office for Civil Protection and Disaster Assistance (BBK), Germany; the Danish Emergency Management Agency (DEMA), Denmark; the Directorate for Civil Protection and Emergency Planning (DSB), Norway; the Federal Office for Civil Protection (FOCP) at the Swiss Federal Department of Defense, Civil Protection and Sports, Switzerland; the Federal Office for National Economic Supply (NES) at the Federal Department of Economic Affairs, Switzerland; the Ministry of Interior and Kingdom Relations, Netherlands; and the Swedish Emergency Management Agency (SEMA), Sweden.

As a complementary service to the International Relations and Security Network (ISN), the CRN is coordinated and developed by the Center for Security Studies at the Swiss Federal Institute of Technology (ETH) Zurich, Switzerland. (www.crn.ethz.ch)