CRN ROUNDTABLE REPORT

4TH ZURICH ROUNDTABLE ON CRISIS MANAGEMENT

Crisis Management in the Case of Critical Infrastructure Breakdowns

Zurich, 30 November 2007

organized by
the Crisis and Risk Network (CRN)

CRN
Supported by ISN

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

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

Author: Christoph Doktor

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 THE CRN ROUNDTABLES: BACKGROUND AND OBJECTIVES 2

2 OPENING AND INTRODUCTION TO THE 4TH CRN ROUNDTABLE 3

2.1 Welcome Address and CRN Overview 3

3 CRISIS MANAGEMENT IN THE CASE OF CRITICAL INFRASTRUCTURE BREAKDOWNS 4

3.1 Topic of the 4th CRN Roundtable 4

3.2 Introduction to the topic 4

3.3 Selected key questions for sessions I, II, and III 6

4 "CRITICAL INFRASTRUCTURES BREAKDOWNS": KEYNOTE ADDRESS BY PROFESSOR MARK DE BRUIJNE 7

5 CRITICAL INFRASTRUCTURES BREAKDOWNS: A VIEW FROM THE PUBLIC SECTOR 9

5.1 Preparations and Strategies of Crisis Management in the case of critical infrastructure breakdowns 9

5.2 Reports by CRN-Members and CRN "Affiliates" 12

6 ROUNDTABLE CONCLUSIONS 14

7 ROUNDTABLE PROGRAM AND PARTICIPANT LIST 15

7.1 Agenda of the day 15

7.2 List of Participants 16

1 THE CRN ROUNDTABLES: BACKGROUND AND OBJECTIVES

The 4th CRN Roundtable on Crisis Management, which took place on 30 November 2007 at ETH Zurich, continued the Roundtable series on Comprehensive Risk Analysis and Management of the Crisis and Risk Network (CRN). It was successfully launched in December 2005 as a new format of discussion and exchange within the CRN, an initiative for international dialog on national-level security risks and vulnerabilities. The first roundtable on the topic of national approaches to risk analysis was followed in May 2006 by a second roundtable on issues of risk communication and by a third roundtable on the topic how to detect emerging risks in November 2006.

The CRN today consists of several partner organizations in Switzerland and other European countries. It includes the Swiss Federal Office for Civil Protection, the Swedish Emergency Management Agency, the Norwegian Directorate for Civil Protection and Emergency Planning, the German Federal Office of Civil Protection and Disaster Assistance, the Danish Emergency Management Agency, and the Ministry of Interior and Kingdom Relations of the Netherlands. The CRN initiative is actively reaching out to new organizations in order to further expand its international circle of partners.

The CRN Roundtables are intended as a platform for bringing together a select group of experts exploring the character and dynamics of the contemporary risk environment. By establishing a collaborative relationship and exchange among likeminded experts, they foster the permanent international risk dialog and contribute to a better understanding of the complex challenges confronting the risk analysis community today. The CRN Roundtables take place once or twice a year.

The CRN initiative is academically and logistically supported by the CRN research team, which is part of the Center for Security Studies at ETH Zurich, a renowned academic institute in the field of international and national security policy, guaranteeing top-quality organizational and academic support for the CRN initiative. More information about the CRN (www.crn.ethz.ch) and the Center for Security Studies (www.css.ethz.ch) can be found on the internet.

2 OPENING AND INTRODUCTION TO THE 4TH CRN ROUNDTABLE

2.1 Welcome Address and CRN Overview

CRN coordinator *Myriam Dunn* welcomed the participants of the 4th CRN Roundtable on Crisis Management and wished them an interesting and inspiring day. She reminded them of the aims of the Roundtable series – exploring the characteristics and dynamics of the contemporary risk environment as well as the requirements on modern Crisis Management, establishing exchange between likeminded experts, fostering an international risk dialog, and enlarging the CRN initiative. She then provided background information about the CRN initiative, which greatly profits from its linkages to the Center for Security Studies at ETH Zurich in terms of content (wide research focus in international and security politics), human resources (fulltime senior researchers and doctoral candidates), and administrative support (organizing events and maintaining the CRN website). Dr. Dunn further introduced the members of the CRN research team. She also gave an overview on recent and forthcoming publications by team members as well as conferences in which the CRN team actively participated.

3 CRISIS MANAGEMENT IN THE CASE OF CRITICAL INFRASTRUCTURE BREAKDOWNS

3.1 Topic of the 4th CRN Roundtable

The topic of the 4th CRN Roundtable was crisis management. The focus of the presentations as well as the discussions was on the question of the limits of traditional crisis management and new approaches to crisis preparation and crisis responses in the case of critical infrastructure breakdowns. Most experts in public administration and the research community agree that the increasing complexity and changing nature of crises demand new scenarios, preparations, and strategies for crisis management. Moreover, it is widely recognized that a modern conception of crisis management must be a holistic one that comprises planning, preparations, response, recovery, and finally assessment and implementation of lessons learned, particularly in the case of a breakdown of critical infrastructure.

3.2 Introduction to the topic

In the past few years, the threat picture has undergone noticeable change. The end of the East-West conflict and the increasing economic, political, and social integration in the course of globalization have broadened the spectrum of potential risks. Today, environmental and technological hazards as well as threats due to intentional human agency are frequently transnational and often near-impossible to define in geographical terms. Sub- and non-state actors as sources of security-policy challenges have gained importance. Situation analyses are characterized by increasing complexity and insecurity.

The demands made of crisis management have changed commensurately. Changes in crisis patterns necessitate far-reaching adaptation measures in terms of the institutions, processes, and actors involved in crisis management.

Defining new crises

All crises are characterized by certain elements that distinguish them from "normal" conditions. For example, there must be a danger to, or threat against, the social, political, or economic system that jeopardizes the underlying values of that system. Another hallmark of a crisis is a high degree of insecurity as far as its specific nature and its expected consequences are concerned. Finally, crises are always characterized by time pressure and the urgency of countermeasures. Often, decisions made at very short notice may entail serious consequences, such as high costs, material destruction, and/or the loss of human lives.

The particular novel aspects of modern crises can be characterized by three key trends. First of all, the causes of crises tend to be more complex and more difficult to identify. Traditional crisis categories such as natu-

ral or human-induced disasters, social conflicts, or external threats due to power politics are only of limited use in understanding modern crises. Secondly, a transnationalization of crises can be observed. In a global risk society, crises that are due to threats such as political violence or to disasters stemming from natural or technological causes often affect several states or societies at once. Third, some modern crises are more difficult to locate on a timeline than earlier ones. This development also implies that it becomes more difficult to determine the dynamics of crisis developments and the speed at which crises spread beyond the boundaries of policy fields and states. In case of critical infrastructure, incidents or breakdowns can lead to significant cascading effects across national or even international systems.

Rationale and conceptual approach

These changed framework conditions give rise to new challenges to crisis management. There is a strong requirement for reorganization within state crisis management organizations. Coordinated efforts must be made at all levels of national security structures. Important elements of an effective coordination strategy include the creation of common terminology, the establishment of expert groups and networks, and the definition of points of coordination and interfaces. Furthermore, it is necessary to establish close inter-state cooperation at the bilateral and multilateral levels as well as systematic cooperation with non-state actors. One long-term aim should be the establishment of public-private partnerships that involve not only collaboration in case of actual emergencies, but also joint planning and exercises. Finally, regarding the elements of critical infrastructures, special attention should be devoted to possibilities for early warning and prevention. In view of the difficulty of managing the dynamics of critical infrastructure breakdowns, a paradigm shift from reactive to proactive crisis management suggests itself.

3.3 Selected key questions for sessions I, II, and III

Session I
Critical infrastructure breakdowns: The limits of traditional crisis management and new approaches to crisis preparation and crisis responses

- What is critical infrastructure?
- What are the current challenges and emerging questions to crisis management in case of critical infrastructure breakdowns?
- What are the new approaches to crisis preparation and crisis responses regarding critical infrastructure breakdowns?

Session II and III
Managing emergencies and crises caused by critical infrastructure breakdowns: A view from the public sector

- What are your organization's conceptions and strategies of crisis management in case of critical infrastructure breakdowns?
- How does your organization deal with the "new nature" of the crisis?
- Is your organization appropriately equipped for dealing with critical infrastructure breakdowns at the operational level?
- Is cooperation with other departments/security actors assured to manage the possible cascading effects of critical infrastructure breakdowns?
- How do you bring lessons learned to the attention of decision-makers in order to implement them in the further conceptions and strategies?

4 "CRITICAL INFRASTRUCTURES BREAKDOWNS": KEYNOTE ADDRESS BY PROFESSOR MARK DE BRUIJNE

The 4th CRN Roundtable was opened with a keynote address delivered by *Mark de Bruijne*, assistant professor at the Faculty of Technology, Policy and Management at the Delft University of Technology. The presentation, with the title "Critical infrastructure breakdowns: The limits of traditional crisis management and new approaches to crisis preparation and crisis responses", consisted of findings from the author's research in critical infrastructure industries that are relevant to crisis management professionals.

Prof. de Bruijne started his presentation by defining the notion of 'critical infrastructures' (CIs). While there is no universally agreed definition of the term for policy purposes, critical infrastructures are commonly defined as including all elements of infrastructure where a disruption of service provision might cause potentially large-scale societal disruptions. They include large-scale technical systems or grids, but also services such as food supplies, health care, law enforcement, etc.

Critical infrastructures, as Prof. de Bruijne emphasized, usually provide extraordinarily reliable performance. However, recent developments pose a challenge for crisis management. On the one hand, as the societal dependence on critical infrastructures grows, there is demand for higher levels of reliability given the increasingly complex interdependence of CIs as well as the rapid technological innovation in the field of CIs; on the other hand, deregulation and liberalization leads to organizational fragmentation in the design and management of critical infrastructures. As a result of these developments, critical infrastructures have become technically more complex and interconnected than ever, and at the same time have reached unprecedented levels of organizational and institutional fragmentation.

The problem for crisis management is how to deal with this paradoxical situation. Prof. de Bruijne suggested refocusing attention on organizational aspects of crisis management and critical infrastructure protection. Institutional fragmentation increasingly forces operators in critical infrastructures to deal with surprises. The emphasis in the management of institutionally fragmented critical infrastructures is shifting from long-term planning to real-time management, from anticipatory analysis to improvisation and experience, and finally from formal com-

Mark de Bruijne is an Assistant Professor in the School of Technology, Policy and Management, Delft University of Technology, the Netherlands. His research focuses on issues of reliability, the management of critical infrastructure industries, and the consequences of institutional fragmentation that results from developments such as privatization, liberalization, and outsourcing. His articles on this subject have appeared in journals like Journal of Contingencies and Crisis Management and the Journal of Public Administration Research. His recent work explores the consequences of institutional fragmentation for the reliability of service provision in critical infrastructures.

He can be reached at:
m.l.c.debruijne@tbm.tudelft.nl

munication to informal communication and coordination.

But the shift towards real-time management has negative consequences. In addition to other issues, the traditional operations and procedures of crisis management need to be changed, and major inefficiencies and a lack of professionalism also constitute serious challenges.

In addition, crisis management is affected by the fact that the risks and financial consequences of failure in private critical infrastructure are so large that national governments have a vital interest in supporting prevention and crisis response. At the same time, the fact that many of the critical infrastructures are in private hands raises the question of who 'owns' the problem of ensuring safety and security. Currently, as Prof. de Bruijne pointed out, the crisis management concepts in Critical Infrastructure Protection focus too much on top-down prevention. The implications for government roles in crisis management regarding critical infrastructure breakdowns should be rethought.

After the presentation, the participants had the opportunity to ask questions and to make critical remarks. In addition to the broader question of which infrastructure is really critical and should be maintained, the question of boundaries between public policy and private sector and of responsibility in the cases of crisis was addressed in particular, and in connection with this issue, the capability of governments to assure the reliability of critical infrastructures was discussed. In this context, the importance of private-public partnerships (PPPs) was stressed. It was stated that PPPs should be seen as a contribution to societal resilience and that it is necessary to integrate the private sector into the whole process of crisis management. In this regard, the government can foster an adequate framework for communication, preparation, and training. But the question of how to create a framework where all private and public participants involved know what to do still remains a challenge.

5 CRITICAL INFRASTRUCTURES BREAKDOWNS: A VIEW FROM THE PUBLIC SECTOR

5.1 Preparations and Strategies of Crisis Management in the case of critical infrastructure breakdowns

The afternoon session was opened by Giulio Gullotta of the German Federal Office of Civil Protection and Disaster Assistance. He spoke about the German approach to preparation and strategies of crisis management in case of critical infrastructure breakdowns and described the lessons learned from the power outage due to a blizzard in Münsterland in November 2005, which lasted several days and affected several hundreds of thousands of citizens.

Mr. Gullotta defined critical infrastructures as facilities and organizations of major importance to the community whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order, or other dramatic consequences. He made clear that so far, no infrastructure breakdown of national concern has taken place in Germany. Because of this lack of incidents, a kind of 'vulnerability paradox' could be seen: people and government are no longer used to, and therefore not prepared for, supply shortages. The lack of self-sufficiency in Germany is a society-wide phenomenon, which can be observed even in the German armed forces.

The German approach to crisis management in case of critical infrastructure breakdowns, as briefly described by Mr. Gullotta, mainly consist of the following parts: first, a review of the situation is undertaken, followed by an assessment of vulnerability and criticality, and finally, the adequate measures should be taken. In the framework of the German approach, PPPs and combined joint exercises are integrated into the whole process of crisis management.

The essential findings regarding the German experiences in the area of crisis management mainly concern training and preparation. First, politicians are not used to making decisions in a state of uncertainty. During a crisis, there is no time for "final findings". Therefore, politicians have to be trained to take responsibility for their decisions. Cooperation during a crisis relies on the pre-crisis relationship of actors involved. The crisis managers have to know their counterparts and their capabilities as well as their needs. The responsible decision makers must be known before the crisis arises in order to cooperate effectively during a crisis. Government agencies and even departments in Germany are no longer used to focused cooperation. In the German model, experts from private enterprise – e.g., power supply companies – are integrated into the crisis cabinet or crisis management groups. But while the public sector is well prepared for crisis management, the private sector is primarily concerned with business crises. Critical infrastructure breakdown never has been and is still not a common topic of concern for businesses in Germany.

Second, self-sufficiency regarding power, water, food, and IT technology, including redundancies and remedies, is an important part of crisis preparation. Integration of external experts and provision of information to the public has to be planned for. Therefore, the crisis management staff has to be given guidance by the responsible politicians together with representatives of the respective critical infrastructure providers. Information before crisis includes knowledge about risks and recommendations for measures to reduce them, but also recommendations for preparation if a disaster occurs. Joint public and private information initiatives are most the promising approaches. During a crisis, there is no time for recommendations. Orders or instructions should be prepared concerning content and wording. Preparations must include plans for reaching and communicating with the citizens (power outage = no radio).

Mr. Gullotta concluded by stressing that one must remember that during a crisis, anything that can go wrong will go wrong, and at the worst possible moment (Finagle's Law of Dynamic Negatives). That's why only simple things work. Finally, after the crisis, the experiences made should be analyzed in order to improve the existing strategies and concepts, because the aftermath of a crisis is the run-up to the next crisis. In the German public administration, there are regular meetings with representatives from CI to share experiences.

The second speaker in this session was Arnold Dupuy of Analytic Services, Inc. (ANSER). He spoke about Crisis Management and Resilience using the example of the US energy sector during and after Hurricane Katrina in August 2005.

Mr. Dupuy started his presentation by framing the issue and delivering some information about the US energy industry. The Gulf Coast is the heart of the country's energy industry, producing 25 per cent of the US crude oil production and 40 per cent of the US natural gas production. The Midwest and Northeast of the US are heavily dependent on Gulf Coast energy products. Given the importance of the energy industry, the private and public energy sectors have enacted proactive and cooperative measures to reduce the sector's vulnerability, which proved to be successful and made the energy sector's response to the Hurricane Katrina one of the few success stories of this natural disaster experience.

In order to analyze the reasons for the energy sector's success, Mr. Dupuy centered on the case study of Entergy, a local energy provider in the US, examining in great detail the preparations, the course of events, and mitigation strategies during the Hurricane Katrina disaster.

The lessons learned show that the Critical Infrastructure Resilience (CIR) that was already built into the energy sector before the Katrina disaster was one of the most important factors. It included a combination of realistic training and rehearsals, good Standard Operating Procedures (SOPs), and investment capital. Mr. Dupuy pointed to the three Rs of energy networks, adding up to what he calls the R-Factor: reliability, robustness, and resilience as pivotal elements of successful crisis management during the hurricane. In addition, he

highlighted the role of cooperation in resilience between local, state, and federal, but also public and private actors in terms of lessons learned.

In his conclusion, Mr. Dupuy emphasized that Hurricane Katrina brought the concept of resilience to the forefront. A key to CIR is the ability to push decision-making down to the lowest levels. This requires quality people and a system that reinforces initiative and does not punish risk or mistakes. But he also mentioned that even the best-planned SOPs cannot foresee every eventuality because conditions will always be unique.

In the discussion, several key issues of both presentations were raised again. The importance of cooperation between different departments and private actors was stressed as well as the need to establish trust and some kind of institutional memory through cooperation with competent and creative people and experts at all levels of the crisis management process. In this regard, planning and exercises are also crucial because they bring together the involved actors and help them to understand the different approaches of the public and private sectors. Moreover, information-sharing was highlighted as a key element of purposeful and effective crisis preparation and management. Some kind of common language and common knowledge between experts should be established and developed. Finally, the necessity of good communication was emphasized, and in this regard, the creation of rules and standards was suggested.

5.2 Reports by CRN-Members and CRN "Affiliates"

The CRN Roundtables are intended as a platform for bringing together experts from various countries and professional communities in order to share their knowledge and experiences. With this goal in mind, several participants gave a short report on the topic under consideration and provided their colleagues with valuable input and thought-provoking insights.

The first speaker was Shainila Pradhan of the British Civil Contingencies Secretariat. She reported on the flooding in England in summer 2007 and the lessons and implications of this event for the Critical National Infrastructure. She started by presenting the main points of the British Central Government Concept of Operations. In addition to the preparation and continuity of crisis management measures and functions, integration of key stakeholders, and cooperation between them, one of the most important principles of the UK Central Response is subsidiarity. Crisis management is based on a bottom-up approach, which delegates decision-making to local key responders. Police and other local responders play a crucial role, and are only guided by government departments where necessary.

During the 2007 summer floods, Mrs. Pradhan reported, nearly 50,000 homes and 8,000 businesses were severely affected. The floods presented a significant challenge to essential services because of many people lost their homes and consumers were cut off from water and electricity. In particular, the distribution of water is worth mentioning because military assistance was needed. The main lessons identified from this exceptional weather event are the necessity of reinforcing business continuity planning as well as the need to involve more private organizations. An independent review is underway to identify lessons for the future, most likely including recommendations on Critical National Infrastructure protection, flood risk, and closer inter-agency collaboration.

François Maridor of the Swiss Federal Office for Civil Protection started with a brief overview of the Critical Infrastructure Protection (CIP) activities of Switzerland. He mentioned that the Swiss CIP program is quite young, having been officially launched in 2005 by the Swiss Federal Council. However, that does not mean that nothing was done before. A lot of efforts have actually been made, especially in the domain of the protection of Critical Information Infrastructures (CII) and the security of nuclear facilities as well as water dams. In a federal state like Switzerland, there is a strong need for cooperation at the federal level, as well as at the cantonal and communal levels and between all these levels, Mr. Maridor stated. There is also a need to establish collaboration with Switzerland's neighboring states. The 'CIP Scenarios' working group at the Swiss Federal Office for Civil Protection uses scenarios to identify the gaps in Swiss CIP. The aim is to collect and deepen already existing scenarios with the collaboration of experts from federal administrative bodies, and with the participation of the private sector and of the academic sector, in order to gain a set of matching scenarios which aims to enable the

identification of harmonized measures and the design of a coherent CIP Strategy by 2012.

The third speaker was Harry McNeil of the Swedish Emergency Management Agency. In his short statement, he pointed out the fact that there is no real crisis awareness in Sweden. Due to structural problems, it is difficult to coordinate the planning, cooperation, and crisis management measures in the case of critical infrastructure breakdowns. In addition, a common terminology regarding CIP does not really exist, but is needed. Private-public partnerships are an important part of every modern strategy for effective CIP and crisis management. However, in order to create trust, clear purposes are necessary, and the mutual benefits for actors involved must be shown, Mr. McNeil concluded.

The last speaker was Williët Brouwer of the Dutch Ministry of Interior and Kingdom Relations. At the beginning of her presentation, Mrs. Brouwer addressed the issue of a gap in expectancies between what the critical infrastructure providers expect from the government and what the government expects from critical infrastructure providers in times of crisis. The interests of the national government primarily center on continuity. In order to assure such continuity, the critical infrastructure providers are expected to be prepared for crises, which means taking interdependencies with other sectors in account and knowing their crisis partners (both public and private), but also informing the government. The expectations of CI providers are different. In crisis situations, they mainly expect the government to protect and support them, and to give them priority access to emergency facilities. In addition, they also need to be supplied with information, clear expectations about service levels, and last, but not least, a coherent government policy. In emphasizing these differences, Mrs. Brouwer outlined the basic principles of the Dutch CIP conception, which regards the owners of CI as being primarily responsible for the continuity of their product, processes, and service. The national government, for its part, supports the owners of CI in taking responsibility and has an overall responsibility to make sure the subject-matter is getting the attention it needs. Moreover, the national government takes protective and repressive measures when necessary, while the local government is responsible for public safety and security. According to these principles, the current activities to strengthen the Dutch crisis response are aimed at making the responsibilities and expectations explicit and identifying interdependencies.

6 ROUNDTABLE CONCLUSIONS

The 4th CRN Roundtable on Crisis Management was a continuation of the Roundtable series on Comprehensive Risk Analysis and Management of the Crisis and Risk Network (CRN). Participants shared their knowledge and experiences with regard to crisis management scenarios, preparations, and strategies in the case of critical infrastructure breakdowns. The focus of the presentations as well as of the discussions was on the question of the limits of traditional crisis management and new approaches to crisis preparation and crisis responses. Several questions were debated intensively:

- How should the responsible parties deal with the growing societal dependence on critical infrastructures in view of the increasingly complex interdependence of CIs and rapid technological innovation in various fields of CI on the one hand, and the organizational and institutional fragmentation in the design and management of critical infrastructures on the other hand?
- Who 'owns' the problem of ensuring safety and security, given the fact that many of the critical infrastructures are in private hands?
- How should the boundaries be defined between public policy and the private sector, and how should responsibility be allocated in cases of crisis?
- How can the diverging mutual expectations of private providers and governments in the field of critical infrastructure be resolved?

The participants came to the conclusion that the crisis management concepts in CIP often focus too much on top-down prevention. More subsidiarity and self-sufficiency are needed. In this context, the importance of private-public partnerships (PPPs) was stressed once again. It was stated that PPPs should be seen as a part of societal resilience and that it is necessary to integrate the private sector into the whole process of crisis management. The governments can foster an adequate framework for communication, preparation, and training. In this regard, cooperation between different departments and private actors is crucial, because it brings together the involved actors and helps them to understand the different ways in which the public and private sectors work. In addition, the importance of establishing trust and some kind of institutional memory through cooperation with competent and creative people and experts at all levels of crisis management process was stressed, and it was emphasized that a common language and common knowledge between experts should be developed. Finally, the necessity of good communication as well as information-sharing was emphasized, and in this regard, the creation of rules and standards was suggested.

7 ROUNDTABLE PROGRAM AND PARTICIPANT LIST

7.1 Agenda of the day

09:00	**Arrival of participants / Coffee & Tea**
09:30 – 10:00	**Welcome and latest CRN-Developments** *Myriam Dunn, CRN (Switzerland)*
10:00 – 11:30	**Session I – Keynote Address** ▪ Critical infrastructure breakdowns: *Mark de Bruijne*, Delft University of Technology - Faculty of Technology, Policy and Management ▪ Questions & Answers, Discussion
11:45 – 13:15	**Lunch Break** Dozentenfoyer, ETH Zentrum Hauptgebäude
13:30 – 15:00	**Session II – Critical infrastructure breakdowns: A view from the public sector** ▪ Preparations and Strategies of Crisis Management in the case of critical infrastructure breakdowns. *Giulio Gullotta (BBK, Germany* *Arnold Dupuy (Analytic Services, Inc., USA)* ▪ Questions & Answers, Discussion
15:00 – 15:430	**Coffee break**
15:30 – 17:00	**Session III** ▪ Reports by CRN-Members and CRN "Affiliates" *1. Shainila Pradhan (GB)* *2. François Maridor (Switzerland)* *3. Harry McNeil (Sweden)* *4. Williët Brouwer (Netherlands)*
17:00 – 17:15	**Conclusions / Final Remarks**

7.2 List of Participants

Name	E-Mail	Affiliation
Bonin, Sergio	bonin@sipo.gess.ethz.ch	Center for Security Studies, Switzerland
Brem, Stefan	stebrem@gmail.com	Federal Office for Civil Protection, Switzerland
Brouwer, Williët	williët.brouwer@minbzk.nl	Ministry of Interior and Kingdom Relations, Netherlands
Bruijne, Marc de	M.L.C.deBruijne@tudelft.nl	Delft University of Technology, Netherlands
Burkhalter, Fred	fred.burkhalter@bwl.admin.ch	Federal Office for National Economic Supply, Switzerland
Closson, Stacy	closson@sipo.gess.ethz.ch	Center for Security Studies, Switzerland
Dam, Anja van	anja.dam@minbzk.nl	Ministry of Interior and Kingdom Relations, Netherlands
Doktor, Christoph	doktor@sipo.gess.ethz.ch	Center for Security Studies, Switzerland
Dunn, Myriam	dunn@sipo.gess.ethz.ch	Center for Security Studies, Switzerland
Dupuy, Arnold	arnold.dupuy@anser.org	Analytic Services, Inc., USA
Forstner, Michael	michael.forstner@zurich.com	Zurich Global Corporate / Risk Engineering, Switzerland
Giroux, Jennifer	giroux@sipo.gess.ethz.ch	Center for Security Studies, Switzerland
Gullotta, Giulio	giulio.gullotta@bbk.bund.de	Federal Office for Civil Protection and Disaster Assistance, Germany
Habegger, Beat	habegger@sipo.gess.ethz.ch	Center for Security Studies, Switzerland
Klopfstein, Matthias	matthias.klopfstein@fedpol.admin.ch	Federal Office of Police, Service for Analysis and Prevention, Switzerland
Koelle, Rainer	rainer.koelle@eurocontrol.int	EUROCONTROL Brussels, Belgium
Maridor, François	francois.maridor@babs.admin.ch	Federal Office for Civil Protection, Switzerland
McNeil, Harry	harry.mcneil@kbm-sema.se	Swedish Emergency Management Agency, Sweden
Müller, Nicolas	nicolas.mueller@bk.admin.ch	Head of Strategic Leadership Training, Switzerland
Pradhan, Shainila	shainila.pradhan@cabinet-office.x.gsi.gov.uk	Civil Contingencies Secretariat, United Kingdom
Suter, Manuel	suter@sipo.gess.ethz.ch	Center for Security Studies, Switzerland

CSS
ETH Zurich

The 4th Zurich Roundtable took place on 30 November 2007 at ETH Zurich. It continued the Roundtable series of the Crisis and Risk Network (CRN), a Swiss-Swedish internet and workshop initiative for international dialog on national-level security risks and vulnerabilities.

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)