CRN REPORT

SUMMARY OF THE INTERNATIONAL HANDBOOK ON RISK ANALYSIS AND MANAGEMENT

Background, results, recommendations

Zurich, February 2008

Crisis and Risk Network (CRN)
Center for Security Studies (CSS), ETH Zürich

CRN
Supported by ISN

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Author: Beat Habegger

© 2008 Center for Security Studies (CSS), ETH Zurich

Contact:

Center for Security Studies
Seilergraben 45-49
ETH Zürich
CH-8092 Zürich
Switzerland

Tel.: +41-44-632 40 25

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

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the Center for Security Studies.

The CRN Reports represent the views and interpretations of the authors, unless otherwise stated.

Summary of the

International Handbook on Risk Analysis and Management: Background, Results, Recommendations

1. Rationale

Analysts and decision-makers in public administrations, armed forces, international organizations, and business corporations have discovered risk as a preferred tool for analyzing and managing future trends and developments. Risk is at the center of many of today's debates in public policy and corporate governance as it embodies the uncertainty about how the future will unfold in an interconnected, complex, and uncertain international environment. The early identification, adequate assessment, and appropriate mitigation of risks have become decisive requirements for effective and successful policy-making across sectoral and territorial divides.

2. Aim

The aim of the handbook is to provide insights into the threat perception, risk valuation, and mitigation efforts of risk practitioners in a broad range of professional contexts. It shows what challenges experts in civil defense organizations, intelligence services, or financial and insurance businesses face in dealing with risks and how they support decision-makers in thinking about, planning for, and coping with the future. The collected contributions provide evidence of a great deal of experience and profound knowledge within and across professional communities and the volume offers a starting point for more research, stimulating reflections, and profound discussions about risks and threats today and tomorrow.

3. Contents

The handbook starts with an introductory chapter by Beat Habegger that briefly sketches the risk concept, characterizes the essential features of today's risk landscape, explores the design of an ideal risk management process, and introduces the handbook's framework and contents. It is followed by the three main parts, each covering a specific professional context:

- In the first part, professionals serving in civil defense agencies, all of them partner organizations of the Crisis and Risk Network (CRN), outline their approaches to risk management. It includes articles from Giulio Gullotta (German Federal Office of Civil Protection and Disaster Assistance), Sara Myrdal (Swedish Emergency Management Agency), and Stefan Brem and François Maridor (Swiss Federal Office for Civil Protection).
- In the second part, authors from security-related institutions such as intelligence services, armed forces, and multilateral institutions present their views. It includes articles from Matthias Klopfstein (Swiss Federal Office for Police), Daniel R. Morris (King's College London) and Gregory Baudin-O'Hayon (Criminal Intelligence Service Canada), Roland Kaestner (German Bundeswehr Academy), and Erik Falkehed (OSCE Conflict Prevention Center).

- The third part contains contributions by risk experts from the financial and insurance business community, including articles by Bruno Käslin (Institute for Insurance Economics of the University of St. Gallen), Marco Lier (Swiss Reinsurance Company), and René P. Buholzer and Manuel Rybach (Credit Suisse).

The handbook ends with a concluding chapter by Beat Habegger, a brief glossary of methods of risk analysis, and the list of contributors.

4. Selected results

The following paragraphs draw on contributions to the handbook and briefly highlight selected problems, challenges, and practices of risk analysis and management. They are not particular to a specific institution or policy context, but explore common concerns beyond the boundaries of specific professional communities.

A changing international environment

A rapidly changing international environment forces institutions and analysts to adequately adapt to altered circumstances. Four interlinked elements are constitutive of today's risk landscape. First, the international linkages and connections between states, international institutions, multinational corporations, civil society, and individuals have created more interdependencies than ever before in world history; second, these interdependencies combined with intense interactions between many independent actors or events create high levels of complexity; third, increased complexity leads to a higher degree of uncertainty; and fourth, these three interlinked elements are collectively affected by an accelerated dynamic of change. In the domain of security policy, the diffuse threats and hardly predictable forms and evolutions of security challenges after the Cold War implied that the concept of risk is a well-suited tool to explain the state and dynamic of a radically transformed security landscape. It is thus not surprising that the civil defense organizations of Germany, Sweden, and Switzerland have all profoundly changed over the last decade. Similarly, this adjustment process and the associated debate about emerging risks and public policy issues also occurred in other areas, ranging from armed forces to financial businesses.

The need for internationalization

Closely connected to the changing environment is the increasing internationalization of policy-making that forces all actors to abandon an exclusively national perspective. Nowadays, strengths, weaknesses, opportunities, and threats have to be considered in view of international trends and developments. It is evident that the emergence of systemic risks, which are often global in origin and have transboundary impact, demand more international cooperation and better coordination among all actors involved, within and across territorial boundaries, in order to effectively counter arising threats.

A common central premise of risk management

It is interesting to note that the central premise of risk management remains the same throughout all articles: it is the need for an early detection of upcoming issues and their adequate assessment in order to ensure that decision-makers can act upon them in a timely and appropriate manner. Accordingly, risk management always embodies two basic rationales: in a reactive sense,

it intends to prevent surprises from happening that may negatively affect envisaged (institutional) objectives; in a proactive sense, it aims to keep and enhance room for strategic maneuvers to better realize envisaged objectives.

Beyond this overall objective, the different contributions also point to a number of aspects that are more specific to the three key phases of an ideal risk management process – risk identification, assessment, and mitigation.

Risk identification depends on vulnerability assessments

The first phase of a risk management process is to observe the risk landscape in a broad manner, to draw a holistic picture of the threat situation, and to plan and implement the appropriate countermeasures. An interesting result is that institutions perceive risks differently, not necessarily because they face different risks, but due to varying vulnerability assessments. Evidently, not all risks are relevant to all institutions or to the same degree. Whether and to what extent a particular risk is actually relevant depends on how an institution estimates being affected by it, which in turn depends on the institution's objectives: civil defense organizations strive to protect the population from incidents that negatively influence safety or welfare, intelligence agencies aim to protect state and society from aggressions by criminal networks, and companies serve their shareholders by protecting the firm's integrity and economic strength. They all frame their protection goals differently and recognize other risks as being relevant, although they are faced with the same overall risk spectrum.

Risk assessment separates public and private actors

Risk assessment includes the structuring, evaluation, and prioritization of risks. In terms of risk prioritization, it is interesting to note that insurance companies specifically focus on risks with a high potential of cumulative claims that may lead to ruinous damages. It might be easier for private than for public actors to clearly set priorities because their institutional objectives are more narrowly framed, stakeholders' expectations more specific, and those who profit from risk mitigation are those who have to pay for it. In public policy, instead, there are usually more involved stakeholders, all having specific expectations and insisting on covering "their" risks: while citizens request mitigation measures for the risks by which they feel threatened, bureaucrats emphasize the significance of the risks they personally deal with, and both justify their claims by referring to an often vaguely defined public duty.

Risk mitigation may lead to unintended effects

Risk mitigation refers to preventive (prevention of occurrence of an adverse event) or precautionary measures (alleviating the damage in the case of occurrence) that mitigate identified and prioritized potential threats. An intriguing result is that public policy actors often resort to issuing new laws or regulations, while private actors, which obviously do not have the respective capacities, are affected by such governmental interventions. One of the key rationales of corporate risk management is to monitor governmentally induced regulatory changes to counter potential negative effects and to create a regulatory framework that is conducive to business success. The somewhat paradoxical result is eventually that public risk mitigation may lead to risks against which private institutions shield with their own risk management. This fact underlines that risk

mitigation may not have the intended effect or may even unfold unexpected consequences – including the opposite of those desired – in areas or sectors that were not targeted by the measures.

5. General policy recommendations

The collected contributions refer to a variety of facets of risk analysis and management. While some address very particular issues and problems, some common strands of practices and challenges can also be identified. In this respect, risk serves as a conceptual tool that connects issues and institutions hitherto perceived as being far distant from one another. With regard to the further development of risk analysis and management, the following general recommendations may contribute to even better tailored and more effective strategic solutions.

Develop a nuanced understanding of risk and the risk landscape

It is crucial to develop a nuanced understanding of the risk landscape and the risk management process as such. Analysts should understand the essential elements of the risk concept and develop a comprehensive picture of the risks that are potentially relevant to their institution. They should also be aware of the complexity and accelerated dynamic of an often volatile, fluctuating, and diffuse risk landscape. Finally, they should recognize that risk analysis and management involves a long-term commitment and requires a clear definition of values and objectives, a meaningful evaluation and prioritization of identified risks, and a lucid appreciation of the resources needed for mitigating them.

Learn to think in alternative futures

Dealing with risks means dealing with a variety of "possible futures". Concretely, analysts and decision-makers alike must learn to think in alternatives, or more precisely, in alternative futures. Risk experts are not assigned to predict *the* future, because no one can know it and it is misleading to pretend to. Their job rather is to imagine many futures in order to deal with uncertainty by presenting alternative scenarios. They should confront decision-makers with the reality of complexity and uncertainty, while aiming at reducing both to a degree that allows formulating meaningful policy choices.

Conceive uncertainty as a matter of degree

Uncertainty should not be perceived in a binary way that assumes the world as either certain and its future course open to precise prediction, or as uncertain and therefore completely unpredictable. Both views are wrong and dangerous: underestimating uncertainty leads to strategies that do not defend against probable threats, while assuming unpredictability leads decision-makers to abandon analytical rigor and to forego a systematic risk management. Risk analysts should aim at overcoming the binary view of "certain" versus "uncertain": a complete lack of knowledge is a rare state; even in the most uncertain environments, is it possible to detect some information, and usually, it is possible to identify a host of hitherto unknown factors if the right analyses are performed. A sophisticated understanding of different levels of uncertainty may help analysts and decision-makers to choose the appropriate strategic responses and to adequately tailor their methodological tools to particular needs.

"Zero risk" is neither feasible nor desirable

A certain amount of "residual risk" always remains. Usually, it is impossible to eliminate a particular risk completely. Such an approach would not only require "total control" of future developments; it might be equally unfeasible in view of limited resources and the need for an efficient balancing of costs and benefits of all (public) policy measures. Furthermore, it may even be undesirable because risks often incorporate an (undetected) opportunity because risk is at the heart of the innovation process and those who want to capture benefits are forced to take risks. In the real world, not in an artificial or ideal-state environment, the objective of risk mitigation is thus not to completely eliminate every single risk, but to aim for an adequate and justifiable degree of residual risk.

Develop and use international networks of risk experts

The sharing of knowledge within and across professional communities should be facilitated and encouraged. When future challenges become global and their impact transboundary, there is a growing need to engage one another across countries and to connect public administrations, international institutions, private companies, universities and think tanks, civil society organizations, and the broader public. Insurance companies, for instance, already heavily resort to external experts or consultants in order to purchase specialized knowledge – a trend that will certainly spill over to the public sector and create more demand for access to risk expertise outside government. In order to facilitate such a knowledge-sharing process, risk analysts should engage in the establishment of various forms of platforms for the exchange of ideas and best practices in risk management.

Cultivate an open risk dialog with the public

Although risk perception largely depends on individually held values, worldviews, goals, and interests, risk identification and assessment require some form of collective judgment to initiate risk mitigation. In a public policy context, this task cannot be left to the elites in the inner circles of government if public trust in political leadership and democratic institutions is not to be undermined. It is thus vital to engage all involved stakeholders, to establish the appropriate communication channels, and to inform the broader public in a timely and regular manner about risk assessments and planned mitigation measures. A systematic and patient risk dialog that generates public awareness and understanding of the complexity of the risk landscape is crucially needed.

February 2008
Center for Security Studies (CSS), ETH Zürich

CSS
An ETH Center

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.

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)