Beat Habegger (ed.)

INTERNATIONAL HANDBOOK ON **RISK ANALYSIS AND MANAGEMENT**

PROFESSIONAL EXPERIENCES

Series Editors
Andreas Wenger, Victor Mauer, and Myriam Dunn Cavelty

Center for Security Studies, ETH Zurich

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

The **International Handbook on Risk Analysis and Management** is also available on the Internet in full text: www.crn.ethz.ch.

Beat Habegger (ed.)
Series Editors Andreas Wenger, Victor Mauer, and Myriam Dunn Cavelty
Center for Security Studies at ETH Zurich (Swiss Federal Institute of Technology)

Contact
Center for Security Studies
Seilergraben 45–49
ETH Zentrum / SEI
CH-8092 Zurich
Switzerland

Layout and Design Fabian Furter
Fonts Adobe Garamond Pro and The Sans (Cover)

ISBN 3-905696-18-5

INTERNATIONAL HANDBOOK ON **RISK ANALYSIS AND MANAGEMENT**

PROFESSIONAL EXPERIENCES

Edited by Beat Habegger

CSS
ETH Zurich

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

CONTENTS

Intelligence Services, Armed Forces, and Multilateral Institutions

Financial and Insurance Businesses

Annex

PREFACE

Following the disintegration of the Soviet Union, a variety of "new" and often non-military threats were moved onto the security political agendas of many countries. Even though the label "new" was not justified in most cases – social and economic inequalities, terrorism, or ethnic conflicts, to name just a few aspects of the "new" agendas, are certainly not creations of the post-Cold War world, though they might have increased in quantity and scale – many of these threats are distinctly different from Cold War security threats. The main difference is an unprecedented quality of uncertainty about them. Uncertainty surrounds the identity and goals of potential adversaries, their capabilities and motivations, the timeframe within which the threat is likely to arise, and the contingencies that might be imposed on the state. This uncertainty can be seen as consisting in the entire set of beliefs or doubts that stems from limited knowledge of the past and present (lack of knowledge) and the ability to predict future events, outcomes, and consequences (uncertainty due to variability).

Due to these characteristics, these security issues are usually no longer depicted as threats, but as "risks". Risks are indirect, unintended, uncertain, and are by definition situated in the future, since they only materialise when they are manifested as real events. In other words: the essence of risk is not that it is happening, but that it might happen. Likewise, security under the condition of uncertainty does not "happen" – rather

it becomes "produceable" through risk management. Risk management decisions in the security-policy domain can respond to some uncertainties by applying appropriate safety margins that take variation into account. Uncertainties can also be addressed by including resilience to potential crises through contingency planning. However, the implementation of effective risk management requires a thorough understanding of the character and dynamics of the new risks and vulnerabilities. Only if potentially hazardous developments are identified at an early stage can effective countermeasures be undertaken.

Confronted with such challenges, analysts and decision-makers are looking for reliable conceptual and methodological approaches to risk analysis and management. It is broadly acknowledged that only a systematic and continuous international dialog can prevent the constant "reinventing of the wheel" and allows a fruitful exchange of "best practices" among experts. It was on the basis of these premises that the "Crisis and Risk Network" (CRN; www.crn.ethz.ch) was launched in the year 2000 as a joint Swiss-Swedish initiative. CRN (the former Comprehensive Risk Analysis and Management Network) is run by the Center for Security Studies (CSS) at ETH Zurich in cooperation with the current CRN partner institutions and is an initiative for international dialog on security risks and vulnerabilities, risk analysis and management, emergency preparedness, and crisis management. Through the interchange of views, the CRN hopes to promote a better understanding of the complex challenges and opportunities confronting the risk community today and serves to establish a collaborative relationship and exchange among experts.

The "International Handbook on Risk Analysis and Management", the newest volume in the CSS Handbook Series, is a product of the CRN initiative and addresses the challenges identified above. The Handbook examines experiences and methods of risk analysis and management from various perspectives: it shows how officials in the public, security, and corporate sectors use a broad variety of techniques and methods for identifying and assessing risks according to their specific needs and it aims to make these approaches available to a wider network of peers and

the broader public. The Handbook thus supports various institutions in identifying risks and in assessing their possible consequences by providing an easily understandable and substantiated access to this topic. In this way, it intends to initiate a knowledge transfer among experts and to facilitate communication between risk analysts and decision makers.

The series editors would like to thank Dr. Beat Habegger, senior researcher at the Center for Security Studies (CSS) at ETH Zurich, for his efforts and high-quality contribution to this important topic. Additionally, the editors would like to thank all authors for generously sharing their professional experiences and knowledge with us. We also thank the following individuals for their assistance in the completion of this project: Christoph Bleiker, Christopher Findlay, Fabian Furter, and Susanne Schmid.

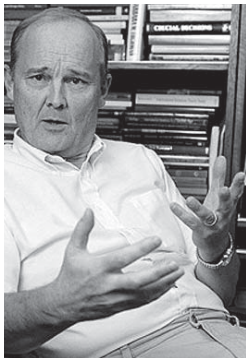
Zurich, January 2008

Prof. Dr. Andreas Wenger
Director, Center for Security Studies, ETH Zurich

Dr. Victor Mauer
Deputy Director, Head of Research, Center for Security Studies, ETH Zurich

Dr. Myriam Dunn Cavelty
CRN Coordinator, Center for Security Studies, ETH Zurich

FOREWORD



The management of risk and crisis is determined by timely leadership. A wise public or corporate leader assumes that he or she will eventually have deal with a major crisis. Thus, early investments in risk analysis capacity and in tools to help minimize the consequences of the unavoidable crises are cost-effective measures to ensure continued tenure as a leader. Although it is not guaranteed that such capacities will suffice against all contingencies, their absence would surely reduce the ability to provide leadership when it matters most.

When risks materialize, executives are held accountable not only for their actions or lack of action when dealing with the acute phases of response and recovery. They will also be judged subsequently as to whether or not their prevention and preparedness measures have been adequate. The necessary capacities for risk and crisis management must be in place well before an acute incident occurs. Precautions against risks that affect the political sphere and preparations for crisis management at the top level will frequently be opposed by sector experts as a waste of valuable resources that are needed elsewhere in the organization or in society at large. Commitment at the top level of the organization is required to ensure that such measures are given priority among many competing claims for time and other scarce resources.

There are numerous examples of cases from many nations where leaders have lost their high positions or their public legitimacy because

of their failure to secure the necessary risk and crisis management tools ahead of time. In the end, risks always entail a price to be paid. It is costly to invest in risk management, but often an even heavier price must be paid for consequence management. In hindsight, after a major crisis or catastrophe, failures in early warning are noted and blame is apportioned to individuals or to specific causes. The willingness is usually very high to deal quickly with the consequences and to try to restore confidence.

Reform is the stepchild of crisis, as the historical record shows. There is an inherent risk that leaders in these post-crisis situations will take a reactive stance, even though they may think they are being pro-active. Drawing on the most recent consequential event, a new mental reference point will be found for future risk analysis and for crisis management tools. Their subsequent efforts, then, are not forward-looking, with open eyes and minds, but in reality backwards-looking. One hopes to avoid a repetition of the most recent negative experience. Adapting to the past rather than learning for the future becomes the basis for the risk analysis.

Low-frequency events with catastrophic consequences are particularly challenging for the methodology and organization of risk management. Leaders and their staffs must be able to keep both eyes and minds open without falling into the mental trap of scanning the horizon for endless negative possibilities. Lack of good management, failure of imagination, and inadequate investment in research and training contribute to the occurrence of avoidable catastrophic events. An event that may be presented by the media as a sudden flash of lightning from the clear blue sky is often the result of a longer, but undetected process of transformation. A creeping crisis develops over time. A chain of small, but detectable anomalies or changes leads up to a fatal collapse or catastrophic event. An example is metal fatigue, which has caused numerous catastrophes in the transport industry.

Societal security is not about building a risk-free society, but about adequate management of risks and crises. A catastrophe avoided, a crisis well managed, will increase public confidence in leadership and contribute to future credibility. Risk and crisis management are built on

research-based knowledge and on experience-based insights. Education and training must draw on both sets of understanding in synergy.

This important handbook serves the capacity-building purpose of bridging the gap between the world of informed scholarship and the intense sphere of risk assessment and crisis management experiences. Hopefully, the book will help strengthen the link between advances in knowledge, knowledge-based training, and improved practices for high-stakes decision-making and action by public and private leaders.

Prof. Dr. Bengt Sundelius

Chief Scientist
Swedish Emergency Management Agency

INTRODUCTION

RISK ANALYSIS AND MANAGEMENT IN A DYNAMIC RISK LANDSCAPE

Beat Habegger

The notion of risk embodies uncertainty about how the future will unfold in an increasingly complex, dynamic, and fast-changing world. Its broad dissemination in politics and business implies that it "unlocks some of the most basic characteristics of the world in which we now live".[1] Risk has gained new ground in the public and scientific debate with sociologist Ulrich Beck's seminal book on the "risk society".[2] He recognized in the 1980s that the accelerated technological change and its consequences for work, economic production, and consumption lead to risks that increasingly defy political control and governance. Modern technological advancements, for instance in the field of bio- or nanotechnology, not only promise great hope for social progress, but also evoke great fears of unknown threats.

It is exactly this twofold nature of risks – the potential threat and the opportunity linked to it – that makes them so challenging to manage.

1 Giddens, Anthony, *Runaway World: How Globalization is Reshaping Our Lives* (New York: Routledge, 2001), p. 39.

2 Beck, Ulrich, *Risikogesellschaft: Auf dem Weg in eine andere Moderne* (Frankfurt: Suhrkamp, 1986).

Eliminating risks completely is neither feasible nor desirable for at least three reasons: there is no absolute control as such for human beings in dealing with the future; the (financial) resources available for prevention and precaution are always limited; and taking risks is at the heart of the innovation process and a necessary condition for economic growth and social progress. The challenge of prudently and successfully steering the course of risks between opportunity and threat has brought risk analysis and management – which some consider "the singular most important analytical tool of the modern world"[3] – to the core of public policy and corporate governance in recent times.

The aim of this "International Handbook on Risk Analysis and Management" is to provide insights into the threat perception, risk valuation, and mitigation efforts of risk practitioners in a broad range of professional contexts. It contains contributions by experts from civil defense organizations, intelligence services, armed forces, and the financial and insurance businesses. Despite the great diversity in their analyses, their varying perspectives on risks, and their differing issues and concerns, a common strand is apparent throughout the book: the key objective of risk analysis and management is always to find ways and approaches to detect upcoming issues in a timely manner, to assess future threats adequately, and to design and implement successful mitigation policies. With this central premise of risk management in mind, this introduction has been divided into four sections: section 1 briefly sketches the risk concept, section 2 characterizes the essential features of today's risk landscape, section 3 explores the design of an ideal process of risk analysis and management, and section 4 introduces the framework and content of the following articles.

3 Jarvis, Darryl S.L. and Martin Griffiths, 'Risk and International Relations: A New Research Agenda', *Global Society*, 21/1 (2007), pp. 1–4, at p. 1.

1 The meaning of risk

"Risk" is an almost ubiquitous term. It has many terminological and conceptual connotations, and it is used in very diverse organizational, disciplinary, or methodological settings. While no generally accepted approach exists, there are a few characteristics shared by all risk concepts. The first is uncertainty about how the future will evolve.[4] The historic turn from a circular to a linear perception of time led to the insight that the future is not simply the repetition of the past and that the present reality is not the only reality: there is a difference between what is, what could be, and what will be. This insight gives rise to thinking in terms of probabilities, which is typical for risk issues.[5] Not coincidentally, therefore, the most common definition identifies risk as the product of the damage potential and the probability that an uncertain future event will occur.[6]

An undetermined and non-linear development over time further implies that the future is subject to human agency and can therefore be shaped by individuals.[7] Human beings are able to actively steer the course of their life, to make decisions, to shape the conditions of the environment in which they live, and to create the future they desire. Uncertainty about the future is thus strongly linked to the capacity for self-determined action, and human beings are able to establish causal links between actions and their possible consequences. These consequences are not fatalistically perceived as predetermined, but they can

4 Renn, Ortwin, 'Concepts of Risk: A Classification', in Sheldon Krimsky and Dominic Golding (eds.), *Social Theories of Risk* (Westport: Prager, 1992), pp. 53–79, at pp. 56ff.

5 Bonss, Wolfgang, 'Unsicherheit und Gesellschaft: Argumente für eine soziologische Risikoforschung', *Soziale Welt*, 42/2 (1991), pp. 258–77, at p. 267; Markowitz, Jürgen, 'Kommunikation über Risiken: Eine Theorie-Skizze', *Schweizerische Zeitschrift für Soziologie*, 16/3 (1990), pp. 385–420, at pp. 386ff.

6 For a more detailed discussion of the key characteristics of risk, see Habegger, Beat, 'Von der Sicherheits- zur Risikopolitik: Eine konzeptionelle Analyse für die Schweiz', in Andreas Wenger and Victor Mauer (eds.), *Bulletin 2006 zur Schweizerischen Sicherheitspolitik* (Zurich: Center for Security Studies, 2006), pp. 133–64, at p. 140–3.

7 Bonss, Wolfgang, 'Die Rückkehr der Unsicherheit: Zur gesellschaftstheoretischen Bedeutung des Risikobegriffs', in Gerhard Banse (ed.), *Risikoforschung zwischen Disziplinarität und Interdisziplinarität: Von der Illusion der Sicherheit zum Umgang mit Unsicherheit* (Berlin: Edition Sigma, 1996), pp. 165–184, at p. 175.

be influenced by either changing the initiating events or by mitigating the resulting negative effects. Consequently, the present we are experiencing at any given point in time is only one of many possible futures people may have imagined in the past, and it is impossible to state with certainty what the world will look like tomorrow. Risk is therefore only a meaningful concept in a "society that is future oriented [and] actively wants to break away from its past".[8] It necessitates a "goal-oriented system"[9] in which decisions are associated with certain goals, interests, and values, so that it is possible to establish criteria against which degrees of risk can be "measured".

This book emphasizes risks that arise on a macro-level in the sense that they potentially affect entire regions, countries, economies, or societies at large. These risks are particularly relevant in security policy, as they usually constitute major events with heavy consequences and transnational impacts, such as terrorist attacks or the spread of pandemic diseases. We may also characterize them as systemic risks because their potential impact challenges the integrity of entire systems – be they political, economic, societal, technological, or ecological. Such systemic risks are defined by "extreme uncertainty and a potential for extensive and perhaps irreversible harm".[10] They may arise from changes in the socio-economic or socio-political environment of institutions, be it in public policy or the corporate world, and the systems may be damaged by single catastrophic events or the cascading effect of a complex chain of events.

8 Giddens, p. 40.

9 Haller, Matthias, 'Risiko-Management: Eckpunkte eines integrierten Konzepts', in Herbert Jacob (ed.), *Risiko-Management*, Schriften zur Unternehmensführung 33 (Wiesbaden: Gabler, 1986), pp. 7–43, at p. 143.

10 OECD, *Emerging Systemic Risks in the 21st Century: An Agenda for Action* (Paris: OECD, 2003), p. 32.

2 Characteristics of today's risk landscape

While a consensus on risk is usually elusive, a few commonly agreed-upon features of the current risk landscape can be identified. Such a risk landscape reflects cognitive models by means of which possibilities and values residing the world are conceptualized[11] and refers "to the totality of risks faced by a specific community".[12] Three interlinked elements are constitutive of today's risk landscape: interdependency, complexity, and uncertainty, all of which are amplified by an increased dynamic of global change.

Tremendous advances in information and communication technology have greatly increased the international linkages and connections between states, international institutions, multinational corporations, civil society, and individuals. This process has created more interdependencies between persons, nations, markets, and societies than ever before in world history. Consequently, international governance is no longer confined to national actors engaged in inter-state relations. A growing number of transnational actors try to influence political processes on multiple levels of governance. While many of these new actors have good intentions, some have misused the transformative power of modern technologies for establishing communication and commercial networks that are intended to do harm to other people. In the case of "transnational terrorism",[13] for instance, small groups are now able to achieve extremely damaging effects that are absolutely disproportional to their "real" (political) significance.

Strong interdependencies combined with intense interactions between many independent actors or events create complexity. Today, "nothing happens in isolation. Most events and phenomena are connected, caused by, and interacting with a huge number of other pieces of a complex

11 Kamppinen, Matti and Markku Wilenius, 'Risk Landscapes in the Era of Social Transformation, *Futures*, 33/3–4 (2001), pp. 307–17, at p. 308; Swiss Re, *The Risk Landscape of the Future* (Zurich: Swiss Reinsurance Company, 2004), p. 5.

12 Swiss Re, p. 5.

13 Schneckener, Ulrich, *Transnationaler Terrorismus* (Frankfurt a.M.: Suhrkamp, 2006).

universal puzzle."[14] The functional sub-systems of our society are highly interconnected, and geographic boundaries in the form of state borders have lost much of their significance. High levels of interconnectivity across functional and geographic boundaries lead to "risk contagion",[15] spreading the effects of a particular incident rapidly and easily to other areas. The cascading effect of risks within tightly coupled interdependent systems makes it hard to predict the consequences of an incident and difficult to contain them to a specific functional or geographical sub-system.[16]

The complexity of the current risk landscape is intensified by three specific characteristics of systemic risks. First, they are often marked by a creeping evolution, meaning that they are difficult to recognize at an early stage. Obviously, contingency plans are easier to prepare for sudden incidents arising from a known threat. In terms of mitigation, the neglect of systemic effects leads to the harmful practice of fixing isolated problems without acknowledging the "complex, system-wide effects of particular interventions".[17] Second, systemic risks often only spread gradually, and the actual consequences cannot be recognized until a very late stage, by which time it might be too late to act. Third, if systemic risks occur simultaneously, emanating from different functional sub-systems and at different geographical locations, individual effects may be amplified reciprocally, and the planned mitigation measures, tailored to the manifestation of a single risk, may not work.[18] The simultaneous occurrence and interaction of risks may generate completely unforeseen effects: the character and the evolution of the risks over time may be

14 Barabási, Albert-László, *Linked: How Everything is Connected to Everything Else and What It Means for Business, Science, and Everyday Life* (New York: Plume Book, 2003), p. 7.

15 World Economic Forum, *Global Risks 2006* (Cologny/Geneva: World Economic Forum, 2006), p. 6.

16 World Economic Forum, *Global Risks 2007: A Global Risk Network Report* (Cologny/Geneva: World Economic Forum, 2007), p. 6.

17 Sunstein, Cass R., *Laws of Fears: Beyond the Precautionary Principle* (Cambridge: Cambridge University Press, 2005), p. 46.

18 Cf. World Economic Forum, *Global Risks 2006*, p. 7.

changed, and their impact in terms of damage potential will probably be much more significant than if each risk occurred individually.

The increased complexity of the risk landscape leads to a higher degree of *uncertainty*. Evidently, the future is always uncertain, and if risk analysis and management is concerned with identifying future events or issues, it entails by definition the need to deal with uncertainty. Uncertainty is also a key governing element of all political or economic activity[19] and "seems to be inherent in political life".[20] One fundamental challenge to international business and politics consists of detecting, out of the almost indefinite number of imaginable trends within the international system, those future trends that exhibit a certain probability of actually occurring. Beyond the uncertainty that has always resided in the international system and is inherent in all dealings with the future, the increased complexity of the current international system has elevated the "normal" degree of uncertainty to higher levels.

The three constitutive elements of today's risk landscape are logically interlinked – interdependency leads to complexity, complexity leads to uncertainty – and they are collectively affected by an accelerated *dynamic of change*: the speed of change and the frequency of change have increased, while the predictability of future events has decreased. Whereas technological progress always has a transformative effect by giving rise to new risks and by providing new tools for mitigating known threats, the modern technologies enable faster communication within more densely interconnected networks. Technological advancement not only creates the conditions for generating, but also for disseminating innovation, opportunities, and risks faster and at much lower costs than ever before.[21] This dynamic shortens innovation cycles and abbreviates the "time-to-market" for corporations. Businesses are forced to adapt quickly to new technologies and changed market conditions.

19 Frei, Daniel and Dieter Ruloff, *Handbuch der weltpolitischen Analyse*, 2nd ed. (Grüsch: Rüegger, 1988), p. 15.

20 Dahl, Robert, *Modern Political Analysis*, 5th ed. (Eaglewood Cliffs: Prentice Hall, 1991), p. 137.

21 Joseph S. Nye, Jr., *The Paradox of American Power* (Oxford: Oxford University Press, 2002), p. 43; Swiss Re, p. 11.

Consequently, governments must adjust the regulatory frameworks in order to stay internationally competitive in terms of providing an attractive investment climate and, ultimately, for retaining business activities. When the frequency of change increases, new opportunities open up for those quick enough to capture the potential benefits. However, more rapid change also leads to new risks that have not yet been considered because they simply did not exist in the past. It is evident that fast-paced change renders future developments less and less predictable. While it is possible in a relatively static environment to estimate how the future will unfold,[22] this task becomes almost impossible in a complex and quickly changing environment.

3 The process of risk analysis and management

Risks have the potential to dramatically diminish human, economic, environmental, and social capital. Armed conflicts, for instance, illustrate the high stakes involved: they induce human costs from death in combat and, often more importantly, war-related diseases and malnutrition;[23] economic costs arise in the form of destroyed infrastructures, disrupted trade, and reduced capital stocks; environmental costs emerge from contaminated battlefields, landmines that make it impossible to cultivate the land, and deliberately destroyed water supply systems; and the social costs are even more evident, as they not only create countless human tragedies, but also undermine public trust in institutions and elites.

The question of whether risks can actually be managed or not may be answered in a way that oscillates between two extreme positions:[24] on the one side are those who subscribe to the view that risks are external variables affecting an institution without any possibility of influencing

22 Cf., for instance, Tetlock, Philip E., *Expert Political Judgment* (Princeton: Princeton University Press, 2005), p. 26.

23 Human Security Report Project (HSRP), *Human Security Report 2005* (Vancouver, Human Security Center, 2005), Part IV: Counting the Indirect Costs of War, p. 125.

24 Cf. Denk, Christoph, *Politische Risiken für Banken: Charakter, Typologie, Management* (Berne: Haupt, 2003), p. 219.

their probability of occurrence or reducing their damage potential; on the other side are those who believe that risks can be absolutely controlled by scientific means and rational action. Both positions are mistaken in view of the common characteristics of risks as outlined above: as uncertain future events, risks can always be influenced by human behavior and decision-making, but it can never be predicted with absolute certainty whether or how they will arise and evolve over time. Any reasonable observer aiming to assess what risk analysis and management can realistically achieve would therefore come to the conclusion that a pragmatic approach must lie somewhere in between. The following paragraphs propose such an approach for the early identification of emerging risks, their timely assessment, and the development of appropriate mitigation strategies.[25]

3.1 Identifying risks

The first step is the identification of risks. Only if the risk landscape is observed in a broad manner can a holistic picture of the threat situation be drawn and the appropriate countermeasures be planned and implemented. Early risk identification helps decision-makers to prevent risks from developing into issues that are likely to threaten stated goals, interests, or values; and it provides them with sufficient time to take the appropriate measures for tackling risks before they arise and appear on the (political) agenda. The early identification of risks therefore reduces "surprise effects", increases the room for maneuver of decision-makers, and improves the overall flexibility of governance.

25 For such a process model, see, for instance, Banse, Gerhard and Gotthard Bechmann, 'Interdisziplinäre Risikoforschung: Von der Risikoanalyse zum Risikomanagement', in Marco Allenspach (ed.), *Integriertes Risikomanagement: Perspektiven einer chancenorientierten Unternehmensführung* (St.Gallen: Institut für Versicherungswirtschaft IVW-HSG, 2001), pp. 15–40; Baumann, Roger, Christiane Döhler, Jens Hallek, and Torsten Wintergerste, 'Implementierung des Enterprise-Risk-Managements', in Oliver Gassmann and Carmen Kobe (eds.), *Management von Innovation und Risiko*, 2nd ed. (Berlin: Springer, 2006), pp. 45–69; Renn, Ortwin, 'Three Decades of Risk Research: Accomplishments and New Challenges', *Journal of Risk Research*, 1/1 (1998), pp. 49–71.

The conceptual starting point is the insight that emerging risks can usually be detected long before they turn into real threats. An effective early-warning system, acting as a "strategic radar"[26] in all environments relevant to an organization, can detect discontinuities in trends hitherto perceived as stable and unchanging. These discontinuities are foreshadowed in the form of "weak signals", a term coined by Igor H. Ansoff, whose pioneering work gave the decisive scientific impulse for strategic early warning.[27] The concept builds upon the idea that risks do not emerge "out of the blue", but always have a history of development.[28] Consequently, the earlier the indicators pointing to discontinuities and upcoming threats are detected, the more options for action are available, and accordingly better risk mitigation measures can be initiated (see Figure 1 below).

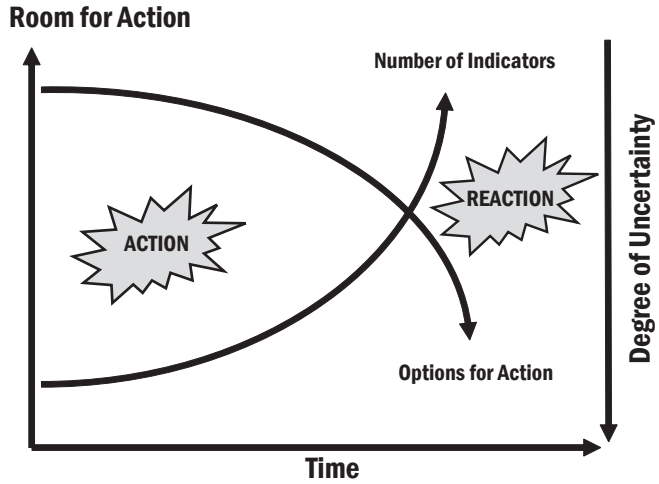


Figure 1: Rationale for early warning

26 Krystek, Ulrich and Günter Müller-Stewens, 'Strategische Frühaufklärung', in Dietger Hahn and Bernard Taylor (eds.), *Strategische Unternehmensplanung – Strategische Unternehmensführung*, 8th ed. (Heidelberg: Physica, 1999), pp. 497–517, at p. 505.

27 See for example, Ansoff, Igor H., 'Managing Strategic Surprise by Response to Weak Signals', *California Management Review*, 18/2 (1975), pp. 21–33.

28 Krystek and Müller-Stewens, 'Strategische Frühaufklärung', p. 501.

The key resource in this process is information. Collecting and processing information is the essential precondition for spotting upcoming issues at an early stage. The constant accumulation of information generates more structured and explicit evidence of potential changes in an external environment. The challenge, therefore, is to broaden the scope of available sources, to access the relevant sources, and to use the collected information in a more creative way. The emergence of an information society, fostered by the tremendous progress in information and communication technology, only appears to facilitate this process: while information is more easily accessible and available, it simultaneously becomes more difficult to filter out the decisive trends or signals from the vast amount of available information. It is not only the lack of data or precise information that contributes to the perception of a complex world, but the inverse trend of information overload may paradoxically even have the greater impact. Joseph S. Nye described this phenomenon vividly as the "paradox of plenty", meaning that a "plenitude of information leads to a poverty of attention".[29] Attention becomes the scarce resource, and those trying to spot the really important issues are constantly challenged to distinguish between valuable signals and routine noise.[30]

3.2 Assessing risks

The second step of a comprehensive risk management process is risk assessment. There are three activities to execute at this stage: the structuring, evaluation, and prioritization of risks. These steps do not necessarily follow each other in this order, but are rather part of a circular process that facilitates consensus-building among all involved stakeholders.

The *structuring of risks* aims to introduce order into a potentially vast amount of identified risks. The objective is to define certain categories around which the identified risks can be clustered. This procedure al-

29 Nye, *The Paradox of American Power*, p. 43.

30 Habegger, Beat, Chris Pallaris, and Vivian Fritschi, *Emerging Threats in the 21st Century; Seminar 1: The Changing Threat Environment and Its Implications for Strategic Warning* (Zurich: Center for Security Studies, ETH Zurich, 2006), p. 8 <http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=27872>, accessed 15 November 2007.

lows risk analysts to subdivide a risk landscape into political, economic, societal, technological, or ecological risks, or any other category they deem necessary or useful. In the publication "Risk Profile Switzerland 1999", for instance, a study commissioned by the Swiss Federal Ministry of Defense, the risk analysts clustered a total of 34 risk scenarios into nine categories, ranging from natural hazards to geopolitical risks.[31]

The objective of *risk evaluation* is to recognize the relative significance of some risks compared to others. The proposition stated above, that risks are only relevant in a goal-oriented system, is self-evident: in order to actually recognize potential hazards, it must first be clear what the objectives are. These objectives always depend on individually and collectively framed interests due to different social, religious, geographic, professional, or educational backgrounds. They are shaped by values referring to particular worldviews, because risk "necessitates value judgments" and should always be understood as a "product of historically, socially, and politically contingent perspectives."[32] Although risk evaluation evidently aims at consensus-building with regard to the character, behavior, or evolution of risks as well as the estimation of their likelihood of occurrence and damage potential, it is never a clear-cut exercise with objective determinants, but always displays subjective elements.

The next step in risk assessment is to ask what risks need to be tackled as a priority. Although the proposition concerning the subjectivities inherent to many risks has been empirically confirmed many times, it is not of great use for policy-makers who are forced to act upon emerging risks. The reason for *risk prioritization* is straightforward: in view of the almost unlimited number of potential risks, and due to the restrictions imposed by the limited amount of resources available, trade-offs are unavoidable, and there is an imperative to make the most effective and efficient use of available resources. Basically, risk prioritization is about

31 Federal Department of Defense, Civil Protection and Sport (DDPS/VBS), *Risikoprofil Schweiz: Umfassende Risikoanalyse Schweiz*, unpublished report (Berne: DDPS/VBS, 1999).

32 Horlick-Jones, Tom and Jonathan Sime, 'Living on the Border: Knowledge, Risk and Transdisciplinarity', *Futures*, 36/4 (2004), pp. 441–56, at p. 447.

determining the potential costs of particular risks in order to tackle those risks that "are likely, imminent, and have widespread consequences".[33]

3.3 Mitigating risks

Once the risks are identified, structured, evaluated, and prioritized, the most threatening ones should be mitigated. From a public management perspective, all previous steps are only relevant insofar as they provide decision-makers with relevant information for deciding about risk mitigation measures.[34] On the basis of the classical definition of risk as the product of damage potential and the likelihood of occurrence, two fundamental mitigation strategies can be distinguished: preventative measures and precautionary measures. The former are intended to prevent the occurrence of an adverse event and are therefore directed at removing the causes of particular risks. The latter are intended to alleviate the damage in the case of occurrence and are therefore directed at reducing the vulnerability of an institution or the society at large and to augment their resilience level.[35] These two mitigation strategies are complementary, and it would be dangerous to neglect prevention in favor of precaution, or vice versa.

In an operational perspective, it is usually impossible to eliminate a particular risk completely. Such an approach would not only require "total control" of future developments; it might also be 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, 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

33 Bremmer, Ian, 'Managing Risks in an Unstable World', *Harvard Business Review* (June 2005), pp. 2–9, at p. 5.

34 Banse and Bechmann, 'Interdisziplinäre Risikoforschung', p. 31.

35 Daase, Christopher, 'Internationale Risikopolitik: Ein Forschungsprogramm für den sicherheitspolitischen Paradigmenwechsel', in Christopher Daase, Susanne M. Feske, and Ingo Peters (eds.), *Internationale Risikopolitik: Der Umgang mit neuen Gefahren in den internationalen Beziehungen* (Baden-Baden: Nomos, 2002), pp. 9–35, at pp. 18–21.

of risk mitigation is thus not to completely eliminate every single risk, but to aim for an adequate and justifiable degree of residual risk.

In order to bring risks in line with opportunities proportionally, a sequence of three logical steps essentially suggests itself (see Figure 2 on p. 27):[36] First, risks can be avoided or eliminated. Research in the area of nanotechnology, for instance, could be stopped and banned. In this way, the unintended consequences of nanotechnology would not constitute a potential future risk anymore. The avoidance of these risks, however, would lead to other risks, such as a deceleration of economic development or a reliance on environmentally more problematic, because more polluting and outdated technologies. Second, risks can be reduced. This is the core idea behind risk mitigation. The two presented mitigation strategies – preventative and precautionary measures – are both based on the premise of reducing risks as much as possible. Third, beyond effective preventative and precautionary risk mitigation, some risks can be transferred to other (third) parties. Obviously, this possibility only applies to a selected set of risks, especially to those for which insurance coverage is available in terms of financial compensation in the case of loss, and it is only relevant for some institutional (often private) actors.

36 Boutellier, Roman and Vinay Kalia, 'Enterprise-Risk-Management: Notwendigkeit und Gestaltung', in Oliver Gassmann and Carmen Kobe (eds.), *Management von Innovation und Risiko*, 2nd ed. (Berlin: Springer, 2006), pp. 27–43, at pp. 35f.

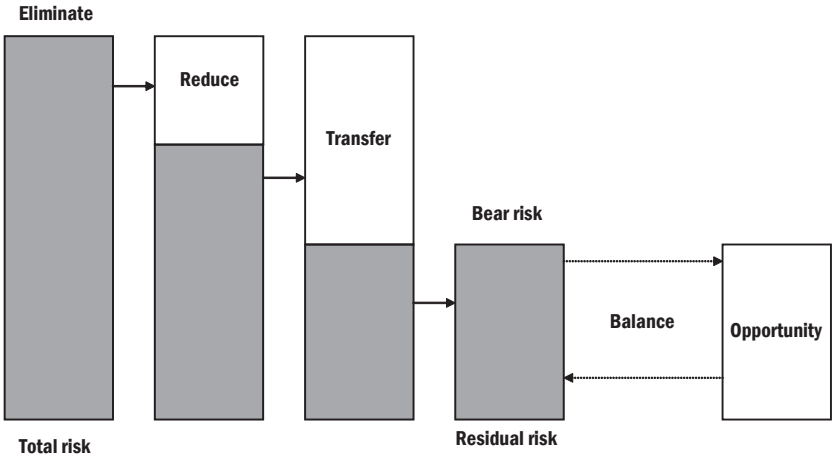


Figure 2: Options for risk mitigation[37]

The suggested process is a somewhat idealized approach to risk analysis and management that evidently needs to be adapted to the respective institutional circumstances. While the timely identification, adequate assessment, and appropriate mitigation of risks have indeed become decisive requirements for successful policymaking, analysts and decision-makers are accordingly confronted with a variety of organizational, political, financial, or knowledge constraints. Forced by a changed risk landscape to reconsider the way they think and plan for the future, they have chosen different means and ways to accept these challenges.

4 Purpose and structure of the handbook

The purpose of this handbook is to explore risk management policies in very diverse contexts and to show how risk professionals support decision-makers in thinking about, planning for, and coping with risks. While this brief introduction served to outline the concept of risk and the risk management process, in the following, experienced professionals write

37 Adapted from Boutellier and Kalia, 'Enterprise-Risk-Management', p. 35.

about the practical challenges they face in dealing with risks and threats. The chapters give insight into a variety of organizational and methodical practices of different institutions. They may stimulate reflection, facilitate communication, initiate a more intense knowledge transfer, and enhance the overall knowledge about risk analysis and management.

The chapters are divided into three parts, each covering a specific professional context, including civil defense organizations, intelligence services, armed forces, multilateral institutions, as well as financial and insurance companies. 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. *Giulio Gullotta* of the German Federal Office of Civil Protection and Disaster Assistance postulates that the main political risk in protecting the people is a failure of leadership on the part of top-level decision-makers that may lead to a decline in public confidence. The rationale for risk analysis thus is to provide decision-makers with reliable and timely information in order to act quickly upon emerging risks. The change in threat perception from a rather one-dimensional focus on (nuclear) war during the Cold War to a multidimensional perspective of a broad variety of potential threats triggered the modernization of the German civil protection system. At its core are joint hazard estimations by the 16 constituent states and the federal government, and joint crisis management exercises that also integrate private companies as the operators of many of today's critical infrastructures. Important lessons for effective risk management include focusing on interdisciplinary work, joint approaches of different agencies, and public-private partnerships.

Sara Myrdal of the Swedish Emergency Management Agency (SEMA) describes the preparations for a large project aimed at studying critical dependencies in Swedish society. It reflects the need to adjust policy priorities and institutional structures in order to adequately cope with post-Cold War security threats. The project focuses on cross-sector analyses and includes international perspectives for strengthening national emergency preparedness. Earlier experiences in other countries served as important sources of inspiration. Ideas derived from them were

fed into a transatlantic and European context, and the institutionalization of these ideas by the EU and NATO influenced the position of the Swedish government and increased SEMA's chances of winning political backing for this project. Preliminary lessons of this ongoing project include the usefulness of crisis scenarios to attract the attention of stakeholders and explain the complexity of critical dependencies, the importance of communicating with the right people at the right level to confer legitimacy, and the challenge of reconciling broad cross-sector overviews with depth in research and analysis.

Stefan Brem and *François Maridor* of the Swiss Federal Office for Civil Protection emphasize the power-sharing and task-sharing arrangements between the different levels of authority in a strongly federalized political system. In the Swiss civil protection system, the tasks on the federal level mainly pertain to conceptual issues, while the actual implementation of preventative or emergency measures fall into the responsibility of cantons and municipalities. The authors further stress the need to understand the broader politico-legal framework within which the civil protection mechanism works – historical legacies, geographical peculiarities, federalism, or direct democracy – and they trace the steps that led to the adjustment of the civil protection framework after the end of East-West tensions. While the methodological tools need to be adapted to the sector under consideration and to the specific task at hand, an open dialog with other security-relevant authorities, the private sector, academia, and particularly the broader public is always a key part of success.

In the second part, authors from security-related institutions and agencies present their views on risk analysis and management. *Matthias Klopfstein* of the Swiss Federal Service for Analysis and Prevention (SAP) claims that the key challenge of an intelligence service is to detect, identify, and indicate overt and potential threats at an early stage. He briefly sketches the strategic purpose, legal framework, and methodological approach of the SAP and particularly emphasizes the benefit of scenario planning for assessing responses to potential threats. He acknowledges that the problem is often not the timely detection of threats, but a lack

of appreciation of the fact that what is perceived as a local threat may have the potential for turning into a major political crisis.

Daniel R. Morris of King's College London and *Gregory Baudin-O'Hayon* of the Criminal Intelligence Service of Canada (CISC) demonstrate the advantage of a systematically developed strategic early-warning system that is focused on emerging threats and targeted to the specific needs of law enforcement decision-makers. They claim that the emergence of intelligence-led policing has altered the way law enforcement agencies must think and operate in the 21st century. Consequently, the traditional military indications and warning analysis has successfully been adapted for use in other domains because its central premise still holds true: events and conditions leading to a crisis situations often generate detectable signals or warning indications that, if correctly pieced together, can portend the coming calamity. The authors show how the CISC's approach to strategic warning intelligence is constructed and they highlight its benefit for the entire law enforcement community.

Roland Kaestner of the German Bundeswehr Academy shows how future analysis serves as a tool for supporting the long-term policy planning and conceptual development of armed forces. He argues that the methods that have been employed in the past for planning to build armed forces for future conflicts are based on assumptions that are only partially appropriate. The complexity of post-industrial force structures and the speed and extent of transformation implies that the planning for complex systems must sufficiently anticipate the future. Therefore, the Transformation Center of the German Bundeswehr has initiated a systematic, strategic analysis of future developments in order to identify security- and force-relevant potential for change at an early stage and to draw conclusions for long-term force planning.

Erik Falkehed of the Conflict Prevention Center of the Organization for Security and Co-Operation in Europe (OSCE) outlines early warning as a mode of operation and a key function of the OSCE. He presents a broad variety of tools that serve this purpose and emphasizes the OSCE's major strengths in early warning: on the one hand, the organization is closely in touch with developments on the ground through its extensive

regional presence in the form of field missions; on the other hand, the information available is very diverse due to a variety of communication channels. However, this diversity also poses the risk that early warning may be improvised, incomplete, and lose its impact due to a lack of organization-wide consolidation. For future endeavors, a pragmatic approach in line with the political nature of the OSCE and its manifold tools is needed to further strengthen its early-warning and political risk analysis capacities.

The third part contains contributions by risk experts from the financial and insurance business community. *Bruno Käslin* of the Institute of Insurance Management at the University of St. Gallen addresses the intensified discourse on emerging risks in many insurance companies. He argues that establishing a systematic approach to emerging risk management is of great benefit because it prevents surprises and provides more time for strategic maneuvers. Based on an in-depth empirical study, he outlines the institutions, processes, and tools and technologies, as well as the cultural factors associated with emerging risk management in four (re-)insurance companies. The critical factor of an effective early-warning system is its ability to effectively transfer its outcome in the institution's practices and procedures. If this attempt fails, it is often due not to "hard factors" such as deficient institutions or processes, but to social and cultural aspects such as a lack of support by top-level management.

Marco Lier of Swiss Re, a globally operating reinsurance company, focuses on the specific issues associated with political country risks. He describes the political country risk rating developed at Swiss Re, which intends to give underwriters a short and quantitative assessment of the country risk of business transactions, particularly in emerging markets. A few years ago, Swiss Re designed and established this tailor-made database for capturing those risk aspects that are actually relevant for the insurance business because the available ratings did not meet an insurer's specific needs. The customized rating system, which he outlines in detail, is currently used for feeding different ratings: while it is primarily used in the niche business of "political risk insurance", in other lines of

business it represents one of several factors to take into account when considering transaction decisions.

René P. Buholzer and *Manuel Rybach* of Credit Suisse, a globally active financial services company, claim that the debate on political risk and public policy issues has dramatically changed in recent years. Internationally active financial institutions face a dual challenge nowadays: they have to respond to the traditional public policy challenges of changes in their regulatory environment on the one hand, and to protect and enhance their reputation as they are increasingly in the spotlight of a critical public and the media on the other hand. With an elaborate process partitioned into three key phases – monitoring, assessment, and lobbying – Credit Suisse is able to contribute effectively to the policy debates that shape its regulatory environment and to protect and foster its reputation among key stakeholders. An important lesson is the need to secure a company-wide unified position on key policy issues and to ensure that all bank representatives speak with one voice on policy matters globally.

CIVIL DEFENSE ORGANIZATIONS

CIVIL DEFENSE ORGANIZATIONS

POLITICAL RISK IN CIVIL PROTECTION – A PRACTITIONER'S VIEW

Giulio Gullotta

Assuming that the main political risk in the field of the protection of the population is a failure in leadership, politicians need sufficient time to act upon and react to emerging risks. Public authorities have to produce timely findings in order to open windows of opportunities for counterstrategies. Germany finds itself in a multi-dimensional risk environment. Several federal authorities conduct risk analyses from their (specialist) angle. The Federal Office of Civil Protection and Disaster Assistance offers a platform for an interdisciplinary approach among the federal states (Länder), federal authorities, academia, and private enterprise. The article describes the office's approach to political risk analysis, i.e., the procedures for conducting the Joint Hazard Assessment, which has been produced together with the federal states ("Länder") since 2004–5. It covers the current and imminent threats to Germany and different methods of qualitative analysis. The article summarizes the practical application of these methods of analysis through an examination of the real-world "LÜKEX" exercise, which is conducted every two years. Through the exercise process, political decision-makers are confronted with the findings of experts before those topics become an issue in the general public. The exercise's subject is one of the outcomes of the regular (risk) selection process taking place in the BBK to deduce the office's working plan.

1 Basic assumptions

The so-called "new risks" to public safety are characterized by the fact that they are transnational in most cases and require a common reaction by all potentially affected states. But even though globalization has generally decreased the relevance of nation-states, the protection of the population remains the fundamental domain of nations and national governments.[1] A nation's culture, tradition, mentality, values, and history do not only constitute its political system (polity) but, even more, influence the perception of, and approach to dealing with, such risks.[2]

In a democracy, sovereignty resides with its citizens, who shape government policy by means of voting in elections for public officials. Politicians take the responsibility for making decisions on their voters' behalf. Assuming that the main objective of politicians is to remain in public office, they will do their best to satisfy the voters' expectations. People expect their political decision-makers to do everything necessary to ensure the public's safety. As soon as a threat to that safety is perceived by the public, action on the part of public officials is preferred to reaction, even if that action is just a statement (e.g., "yes, we are aware of that particular risk and we are taking care of it"). Therefore, the main political risk in the field of the protection of the population is a failure of leadership (and/or management)[3] that results in a lack of public confidence.

1 This article discusses the role of states as generators and facilitators of disasters. A good philosophical discussion of the attitudes of states concerning disasters is Adi Ophir, 'The Two-State Solution: Providence and Catastrophe', *Journal of Homeland Security and Emergency Management*, 4/1, article 2 (2007), 1–44.

2 Gotthard Bechmann (ed.), *Risiko und Gesellschaft, Grundlagen und Ergebnisse Interdisziplinärer Risikoforschung*, 2nd ed. (Opladen: Opladen, Westdeutscher Verlag, 1993), p. XVII, refers to anthropologists of the 1980s concerning the interrelation of culture and risk. The idea goes back to Montesquieu, whose accurate description of the coherence between regional/national peculiarities and the respective legal systems, De l'esprit des loix, was published as early as 1748. The appraisal of nuclear power in France and Germany can be taken as an example.

3 For examples, see, William L. Waugh Jr. (Special Editor), *Shelter from the Storm: Repairing the National Emergency Management System after Hurricane Katrina, The Annals of the American Academy of Political and Social Science*, vol. 604 (Philadelphia: Sage Publications, 2006); and chapter 13 of the National Commission on Terrorist Attacks upon the United States (ed.), *The 9/11 Commission Report* (New York/London, 2004).

It is crucial for politicians to get timely information so that they may (re-) act appropriately to the new risks. But in the present "information age", where any event – anywhere – can become an issue (or a crisis) within seconds, it is difficult for generalists to keep pace with the rapidly increasing complexity of the risk environment. Thus, politicians have to rely on specialists to track different risks and provide them with timely warning. If they refer to the experts, they can benefit in two ways: (1) they earn credibility with voters (since there is a general mistrust against politicians), and (2) they can blame responsibility for cumbersome and inconvenient decisions on the specialist.[4]

2 The German civil protection system

The threat perception of Germany's civil protection community has changed from a generally one-dimensional perspective during the Cold War to a multi-dimensional perspective today. While the possibility of a (nuclear) war was considered the largest risk to public safety until the 1990s, today, natural disasters and man-made threats (industrial risks, technological failure, crime, terrorism and so on) are perceived as more likely threats to civil order.[5]

4 Generally speaking, specialists and experts can be found in the science community. But research at universities in a constitutional state (Carl Schmitt, *Verfassungslehre*, 3rd ed. [Berlin: Duncker & Humblot, 1957]) is usually not linked to the needs of the government – except for government-funded projects, whose outcome, however, is often considered tainted by the interests of the funding authority. Secondly, research takes a lot of time, especially if phenomena have to be monitored. To ensure the permanent availability of, and rapid access to expertise, most governments set up agencies that are competent in dealing with one particular matter. These agencies function as a hinge between science and politics, although they strive to be independent from political attitudes. Only by doing so can they retain the trust of citizens and the science community and thereby continue to function as justification (or scapegoat) for political/government action. Of course, government officials have easier access to authoritative experts than anyone else. For a critique of the role of specialists in the field of risk, see Jobst Conrad, 'Risiko, Ritual und Politik', in Mario Schmidt (ed.), *Leben in der Risikogesellschaft: Der Umgang mit modernen Zivilisationsrisiken* (Karlsruhe: C.F. Müller, 1989), pp. 179–204.

5 The semantic distinction between "hazards" for events of natural origin, and "threats" for man-made incidents, is not common in Germany. The hyperonym "Bedrohung" is used in both cases and encompasses both meanings.

The Federal Republic of Germany has a long tradition of countering those risks by creating official bodies with responsibility for them. Generally speaking, Germany used to have four pillars of security for the protection of its citizens on the federal level. These consisted of three strong and established ones: (1) the military (armed forces); (2) the police (the police departments of the federal states and the "Bundeskriminalamt", the Federal Criminal Police Office); and (3) the intelligence services; and a fourth department that, until 2001, was tiny and negligible: (4) civil protection. The ubiquitous menace during the Cold war worked as an umbrella for these four pillars. Collaboration and information-sharing were crucial for a successful "total defense" approach. When tensions between East and West eased in the 1990s, the agencies began to look for new roles and unique threats to justify their respective existence. The lack of a shared and common sense of urgency led to a lack of cooperation on the federal level – even in the field of strategic risk analysis. But there had been another challenge for disaster prevention: Due to the artificial distinction between civil protection in times of war, on the one hand, and peacetime emergency management and planning, on the other hand, responsibilities for the management of civil emergencies had been distributed among four different governmental levels (the federal government, the Länder, towns/counties, and municipalities). However, as a consequence of the terrorist attacks in the US of 11 September 2001, and even more so, in response to the severe floods of 2002, this system of distributed responsibilities has been adjusted. In 2002, the traditional German civil protection system was modernized when the federal government and the states agreed upon a New Strategy For The Protection Of The Population In Germany ("New Strategy").[6] The four traditional pillars of security were supplemented

6 This "New Strategy" is characterized by a joint coordinated approach of the federal authorities and the Länder concerning the crisis management of unusual and nationally significant disaster and damage situations. See 'Beschluss der Ständigen Konferenz der Innenminister und -senatoren der Länder vom 06.06.2002 in Bremerhaven, TOP 23' and 'Beschluss der Ständigen Konferenz der Innenminister und -senatoren der Länder vom 06.12.2002 in Bremen, Top 36', in Bundesverwaltungsamt (ed.), *Neue Strategie zum Schutz der Bevölkerung in Deutschland*, Schriftenreihe: WissenschaftsForum, vol. 4 (Leipzig, 2003), pp. 63–7.

with struts, and the security network was woven tighter.[7] While no laws concerning the traditional allocation of responsibilities were changed, the mindset or political will was readjusted to address the new reality. Today, responsibility for risks is better coordinated between the various agencies and administrative levels, and they interact more often and more effectively.

3 Risk analysis – the BBK approach

Since the proper protection of the population demands good knowledge of the extant threats, the New Strategy required that the Federal Government and the Länder should conduct hazard and risk analyses. On the federal level, the Federal Office for Civil Protection and Disaster Response ("Bundesamt für Bevölkerungsschutz und Katastrophenhilfe", BBK) was established to function as the central point of contact for all matters of civil protection,[8] and plays a vital role in conducting the required hazard and risk analyses.[9] In the next section, the BBK's main approach to risk analyses is described. Some of the methods that can be found in the glossary of this handbook are used in the risk analysis process, even though they are not explicitly mentioned here.[10]

7 For a brief description of the German civil protection structure, see Swedish Emergency Management Agency SEMA, *International CEP Handbook 2006: Civil Emergency Planning in the NATO/EAPC Countries* (Helsingborg, 2006), pp. 81–5.

8 All tasks of the BBK can be found in the *International Civil Defence Directory* <http://www.icdo.org/pdf/struc/germany-en.pdf>, accessed 8 August 2007.

9 Due to the duration of the legislation process concerning the establishment of the BBK, its precursor, the "Zentralstelle für Zivilschutz" (Central Department of Civil Protection), represented the federal side at the beginning.

10 During the survey for this book, it became obvious that many methods employed by the BBK were not known under the glossary's term. This seems to be an old problem. William D. Rowe, *An Anatomy of Risk* (Malabar, FL: Robert E. Krieger Publishing Company, 1988), wrote in the preface of the reprint edition that there had been much progress in the development and use of risk analysis, but that in most cases, the fundamental aspects remained the same. "However, there has been a change in terminology" (p. ix).

3.1 Joint hazard estimation

In the past, the main objective of the Länder and the federal government had been the identification of hazards exceeding day-to-day events and of crisis situations of national concern. In 2003, a working group of representatives from the respective ministries of the Länder and from the Federal Ministry of the Interior agreed upon a Joint Hazard Estimation ("Bundeseinheitliche Gefährdungsabschätzung").[11] The document was implemented in 2004–5, marking the first step towards a risk analysis.

The following articles in the Joint Hazard Estimation were defined for the working process:

- Collaborative/joint identification of hazards and threats that should be analyzed/monitored at first
- editing the results in a standardized structure
- confidential exchange of information between all involved parties[12]
- integration of experts from other authorities and science
- analyses of regional hazards by the Länder (e.g. floods, storm surges)
- analyses of nation-wide hazards/threats by federal agencies (e.g. break down of critical infrastructure, pandemics)

There was a broad consensus about the fact that the objective of the Joint Hazard Estimation, i.e., the support of decision-makers, could only be successfully achieved by constant information exchange, new data integration, and a permanent review of the results.[13] *The Joint Hazard Estimation* pursues an "all-hazards approach" that covers natural disasters as well as

11 Memorandum of agreement of the 61st meeting of the working group V (Feuerwehrangelegenheiten, Rettungswesen, Katastrophenschutz und zivile Verteidigung) of the Permanent Conference of the Ministers of the Interior of the German 'Länder', 21–22 October 2003, Saarbrücken, Germany, agenda item 3.1.

12 If vague scenarios would be discussed publicly, the current analysis (and the credibility) might suffer. The interchange of views could lack creativity, but even worse, the public could be scared. The authorities would create a risk (an issue).

13 Of course new findings can be added at any time but in any case a regular yearly updating/review is agreed.

human/technical failure, terrorism, crime, and war. In order to get a good estimate of the importance of hazards/threats for civil protection, all available information is to be collected. For every identified hazard/threat, the *Joint Hazard Estimation* contains:

- a general description of the hazard/threat[14]
- protection goals
- an overview of the existing emergency planning[15]
- a list of measures and actions that decrease vulnerability
- a list of measures and actions that increase the capacity to deal with them
- a list of additional required (specialized) capabilities at the level of the federal states

In instances where other federal authorities have responsibility, the BBK has asked for their participation in the *Joint Hazard Estimation* process (e.g., the Robert Koch Institute for biohazards, the Federal Office for Information Security for CIIP, the Federal Network Agency for telecommunications, etc.). By December 2005, all sixteen Länder as well as the federal government had compiled their individual hazard estimations and thus contributed to a common picture of the risks Germany faces from a civil protection perspective. For the first time in the history of the Federal Republic of Germany, a survey of all relevant hazards – including those that are currently still on the horizon – had been produced.

This intensive examination of threats and hazards in cooperation with other authorities during the *Joint Hazard Estimation* resulted in a detailed identification of emerging risks in terms of possible future

14 Since valid data concerning impact and likelihood were lacking they were neglected during this first approach. A qualitative analysis could be conducted for every hazard/threat – extension by quantitative elements is envisaged. Insofar as possible, the suggestion of Harry Markowitz that procedures "should combine statistical techniques and the judgement of practical men", has been followed. See Glyn A. Holton, 'Defining Risk', *Financial Analysts Journal*, 60/6 (2004), p. 21.

15 For some events (mainly high impact, low probability, like large meteoroids hitting the earth) there is currently no explicit emergency planning (due to the large uncertainty). Nevertheless these topics are included in the list of hazards.

issues. One of the examined threats, the breakdown of the bulk electric power supply system, tufrned out to be a viable political issue, as had been presumed during the preliminary work (2003).[16]

3.2 Exercise "LÜKEX"

The purely scientific analysis of a risk does not take into account political points of view and might therefore miss the political risk dimension. To provide decision-makers with more pragmatic and useful information, an identified and analyzed risk should be transferred into an exercise scenario. Numerous new findings will occur if people with different backgrounds interact within the framework of an exercise. This creates a win-win situation in which (political) decision-makers have an opportunity to practice their crisis management skills and where risk analysts can broaden their horizon (and identify the need for further investigation).

The *New Strategy* stated that combined joint crisis management exercises involving top-level executives should be conducted in order to counter the stovepipe problem.[17] This development recognizes that the discontinuance of such exercises in Germany after 1990, due to the so-called "peace dividend", had contributed to stovepiping and fragmented emergency response.[18]

In 2004, the BBK prepared and supervised the LÜKEX exercise .[19] Since the German emergency management system had not yet faced a real-world crisis that exceeded its resources, the LÜKEX scenario had to be designed on a large scale – envisaging events that affected at least two Länder. Because a power outage affects almost every aspect of society due

16 See Bundesamt für Bevölkerungsschutz und Katastrophenhilfe BBK (ed.), *Problemstudie: Risiken für Deutschland*, Reihe WissenschaftsForum, vol. 6 (2 vols, Bonn, 2005), which is a shortened, unclassified version of the original restricted study 2003.

17 Combined: all authorities/departments on the same level; joint: different administrative levels together.

18 During the Cold War, such exercises had been regularly carried out under the auspices of the military within the framework of total defense.

19 LÜKEX is the abbreviation for 'Länderübergreifendes Krisenmanagement Exercise'.

to its cascading effects, this scenario was selected.[20] The script contained a series of heavy winter storms that caused the breakdown of the electric power supply system in large parts of two Länder, lasting anywhere from a couple of days to several weeks.[21] The ambitious aim of those writing the scenario was not only to involve public administration at a top level of management, but also to integrate the responses of private enterprises, since most critical infrastructures today are owned and/or operated by private companies. Apart from the general benefit for (operational) crisis management, the aim of LÜKEX was to give risk analysts an opportunity to look into the black box of how private enterprises function and how they would react to large-scale crises.[22] Accordingly, another outcome of the exercise was to create mutual understanding of the needs and capabilities of "the other side" between public administration and private enterprise, thus reducing uncertainty.

Preparations for the exercise began more than a year in advance. Under the headline "power outage", risk analyses were conducted in a series of workshops with power suppliers, ministries, agencies, public administration on different levels, different private enterprises (including large food store chains, telecommunication companies, water suppliers, logistics corporations, and so on). Starting with a brief description of the scenario, the workshops conducted focused brainstorming sessions among the experts present. In most cases, these specialists left the workshops with a number of homework assignments. Depending on the scientific background of the experts, feedback to the preparation group ranged from qualified descriptions to case studies (and more scenarios) to fault-tree-analyses. Putting together those puzzle parts enabled planners to assemble a risk analysis of the complex systems in Germany. Many

20 For a good and quick overview of the topic, see the Dutch Rathenau Institute's study, *Stroomloos Kwetsbaarheid van de samenleving; gevolgen van verstoringen van de elektriciteitsvoorziening*, Studie V26 (Den Haag, 1994).

21 In November 2005, a five-day power outage caused by bad weather hit the Kreis Steinfurt region in Germany, leaving approximately 250,000 people without power and validating the assumptions of the LÜKEX planners.

22 Contingency planners and business continuity managers of private enterprise had the same interest concerning the public administration. Their risk analyses take into account public response capacities and capabilities.

interdependencies were identified, and a lot of unforeseen problems, including unclear divisions of responsibilities, were discovered in preparation for the exercise. After the initial working-level meetings, the director-general level and even deputy ministers also prepared for the final exercise. In scenario-based briefings and concise table-top exercises, they were confronted with the findings of their staff – especially the unsolved problems.

During the final three days of the computer-supported exercise, numerous crisis management teams in ministries (of both the federal and state governments), regional administrations and private enterprises were tasked with the management of the outcomes from the workshops. The crisis management groups of all federal ministries and the *Länder* for large-scale hazard situations (*Interministerielle Koordinierungsgruppe von Bund und Ländern für großflächige Gefahrenlagen*) met regularly at the director-general level. Since this is about as close to the ministerial level as it is possible to get during an exercise, there was an unusual opportunity for direct exchanges between lower-level analysts and top-level decision-makers. The participants did well and, as expected, they raised additional (political) questions during the exercise.[23] For the risk experts involved, it was interesting to see whether their analyses and proposals would be understood, how their findings contributed to decisions, and which way of editing was expected by the decision makers. The exercise method proved its usefulness, and the Federal Ministry of the Interior decided to hold follow-up exercises every two years – thus, the LÜKEX series was born.[24]

23 A number of organizational changes have been executed in the meantime. A uniform structure of crisis management groups has been implemented at the federal and Länder level, and the coordination between them has improved. The *Interministerielle Koordinierungsgruppe* is evolving into a forum for the assessment of emerging risks, producing (pre-crisis) recommendations for decisions at the political management level.

24 Due to the very intense preparation, a biennial pattern of exercises was instituted. For the sake of preparations for the FIFA World Cup 2006, an exception to this rule was made with LÜKEX 2005.

3.3 "An issue ignored is a crisis invited"[25] – horizon scanning

The BBK employs scientists from some 25 different disciplines (e.g., political scientists, chemists, sociologists, biologists, medical doctors, physicists, and geographers) who are integrated in (national and international) expert networks. Within those networks, special risks are constantly discussed, monitored, and analyzed, while new findings are validated and assessed. The networks serve to detect emerging risks in the scientists' respective fields of expertise. The BBK's experts appraise the relevance of information and communicate the results into the BBK, functioning as a filter. Internal interdisciplinary boards discuss the relevance of those research findings, which are presented by their colleagues, for the protection of the population. Chaired by the president, a committee composed of the BBK's heads of divisions considers different scenarios and matches them into a probability and impact matrix.[26] Then the risks are evaluated with respect to their current relevance for the BBK's mission and, where applicable, transferred into its working plan. If circumstances change, risks regarded as irrelevant at one stage may be assessed differently in the next evaluation process.[27]

3.4 Are we on the right track?

Analyzing and assessing risks means dealing with uncertainty. Whereas experts accept uncertainty within a concrete risk analysis, they try to minimize it when choosing the object of their investigation. This is even more important because, concerning the choice of their object of investigation, creativity and unorthodox thinking are necessary to detect future risks. A

25 This aphorism by Henry Kissinger is quoted by numerous PR and risk management consultants.

26 The common matrix and process are well described in the UK Government (ed.), Emergency Preparedness: *Guidance on Part I of the Civil Contingencies Act 2004, its Associated Regulations and Non-Statutory Arrangements* (Easingworld, 2005).

27 At the time that a topic is detected and monitored, it is impossible to tell whether or not it will be a matter of concern in the future. But the political administration has to be informed in sufficient time to allow a suitable reaction. Concerning "the right moment", see Rowe, p. 299, discussing chances and risks of early reporting.

number of measures can foster a productive atmosphere to create valuable and even revolutionary results,[28] for example:

- Interdisciplinary work has proven to be a very effective way to not only of analyzing complex risks, but also of assessing them.
- The same effects can be reached through joint approaches of different agencies.
- Public-private partnerships, the cooperation with partners from private enterprise and universities create a win-win situation in terms of gaining knowledge (and fostering mutual understanding).
- The (temporary) integration of individual experts into an agency – e.g., for selected projects – has similar advantageous effects.
- At the same time, these measures function as quality assurance (and alert the experts if they are heading into a blind alley).

In addition to the efforts of the experts on the BBK's payroll, there is also an independent Advisory Board for Civil Protection (*Schutzkommission beim Bundesminister des Innern*), which reports directly to the minister of the interior. The BBK provides the secretariat for this board, which consists of scientists representing those disciplines covering a large variety of potential risks. The board gives an assessment of both the broad spectrum of imminent threats facing Germany and the provisions needed to meet them.[29] Since these experts have a purely scientific background (and no fiduciary relation to the government), they can identify deficiencies frankly and suggest priorities for actions to be taken from their point of view.[30] The "Risk Reports" of the *Schutzkommission* complement the findings of BBK

28 Risk analysis is typically done in an evolutionary way – starting from an event or known facts. "Revolutionary" in this context means that even the "unthinkable" is thought.

29 The website of the Advisory Board for Civil Protection <http://www.schutzkommission.de> (accessed 8 August 2007) contains publications, such as risk reports. A summary of the Third Risk Report is available in English.

30 An authority might be tasked to find out which risks are affordable, instead of asking which threats the country faces.

and can trigger a review of the BBK's own findings, judgments and assessments – as the regular co-operation and exchange of opinions often do.

The public expects openness and independent advice from government agencies. To gain and keep such a reputation in an environment where political aspects might overwhelm scientific findings is a challenge for every authority. In the end, it is important not only to produce valid and reliable information, but also to contribute to open communication, which leads to a society-wide consensus on acceptable levels of residual risk.[31]

4 Conclusion

Germany has a variety of government authorities that deal with, and have responsibility for, risks. Altogether, all developments that might have a severe impact on large parts of the population (health, means of existence, vital resources, peaceful coexistence), the environment, the constitution (basic rights, rule of law, democracy), the existence of Germany as such, and international peace are tracked.[32]

The BBK is a fairly new player in the field of risk analysis in Germany. Its role is that of an early-warning system – scanning the risk environment and sounding the alarm once information and analysis reveals its potential to be an (high impact) issue.[33] The BBK concentrates on risks that affect at least two federal states, large parts of the population,

31 Adalbert Evers, 'Umgang mit Unsicherheit. Zur sozialwissenschaftlichen Problematisierung einer sozialen Herausforderung', in Bechmann, *Risiko und Gesellschaft*, pp. 339–74, at p. 364 claims that scientific expertise might produce a variety of alternatives and specify scenarios as well as make their likelihood more calculable. But in the end, only social and political debates help to reach a consensus on (prescriptive) limits and ultimately legitimize the assessment of likely alternatives.

32 This list sums up the basic rights (Articles 1–19 of the *Basic Law for the Federal Republic of Germany/Grundgesetz für die Bundesrepublik Deutschland*) as well as other subjects of protection of Germany's constitution (e.g., Articles 20, 20a, 26 of the *Basic Law*).

33 The idea of an early-warning system is very common. A good description is provided in several SwissRe publications concerning the companies "Systematic observation of notions associated to risk – SONAR" (e.g., <http://www.trainex.org/risk2006/Plenary/Hett-EPA02May06Final.pdf> [accessed 8 August 2007], slide 12).

or vital resources. An all-hazards approach was chosen by the BBK to meet the growing complexity of society and the risk environment. In view of the fact that interdependencies and cascading effects cannot be discovered through solitary analyses, the combination of a wide range of expertise (as well as of approaches and data) and the interchange of views are the most promising solutions for dealing with uncertainty.[34] Therefore, the BBK provides a platform for various authorities and scientific disciplines that have extensive experience in analysis (from their respective perspectives). Through an intelligent combination of existing approaches/findings/data, as well as by analyzing and examining various findings for their relevance to the protection of the population, the BBK produces added value for the government (and the population).[35]

At the same time, the interdisciplinary and joint analysis of potential issues discloses the need for further activity (including research and development), producing a common situational picture and bringing about a coordination of efforts. Politicians still bear responsibility for risk management and have the final responsibility to take the measures they feel to be appropriate.[36] Successful risk communication is therefore essential for the BBK's success.[37] It ensures that timely information is

34 Emerging risks, like the fading of the earth's magnetic field, currently have to be tracked and the consequences analyzed by a variety of agencies. Others, such as high-altitude nuclear explosions, for which there is already an empirical scientific basis, have to be examined regarding the possible economic (and other cascading) effects and judged concerning their likelihood: What would happen if North Korea fired a missile with a nuclear warhead vertically above its territory?

35 Whereas the scientific work of risk analysis is done by the BBK, the (political) risk assessment is performed by the Ministry of the Interior. According to the ministerial hierarchy, responsibility for the assessment proceeds upwards, depending on the assumed relevance of a risk: from desk level for minor risks (or emerging risks at a very early stage) up to the minister himself for the more pressing scenarios.

36 Niklas Luhmann, *Soziologie des Risikos* (Berlin: Gruyter, 2003), p. 185 names two alternative decisions for politicians: a) immediate regulation that places the responsibility for the consequences on the authority in question, or b) wait, ask for professional opinion and/or (written) expertise. The latter could lead to a more relaxed situation or to an increasing aggravation, increasing costs and a decreasing window of opportunity.

37 Risk communication (as a two-way process) involving the BBK takes place at different administrative levels (with federal and other authorities), with experts outside administrative bodies, with social groups, or with the general public – depending on the topic. Concerning "issues", the Ministry of the Interior is the recipient of information and partner in risk communication. It decides who to address next: the public, the parliament, or other ministries.

provided to politicians and reduces their risk of failing and, at the same time, decreases Germany's vulnerability. Of course, the BBK's reputation is closely linked to the success of the (political) risk management. For this reason, the BBK is subject to the paradoxical fate of all authorities dealing with emerging risks: If the BBK does a good job in identifying risks and preventing them, then politicians and society may think it is dispensable, since those risks do not evolve into catastrophes.

CIVIL DEFENSE ORGANIZATIONS

ANALYZING CRITICAL DEPENDENCIES IN SWEDISH SOCIETY

Sara Myrdal

The purpose of this chapter is to describe the preparations at the Swedish Emergency Management Agency (SEMA) for a large project aimed at studying critical dependencies in Swedish society. The first part of the chapter traces the gradual emergence of the ideas underpinning the project and shows how the interest in mapping and analysing dependencies between critical functions in society has evolved as part of a "societal security approach" capturing many of the ideas represented in the field of CIP and CIIP. Initial experiences of dependency analysis in Canada and the Netherlands represent a point of departure for conveying the emergence of these ideas. The work carried out in Canada, in particular, is a significant source of inspiration for SEMA. The chapter also shows how the ideas developed by these pioneers in CIP were fed into the transatlantic and European context at moments when the receptiveness was high due to terrorist attacks. The institutionalization of ideas by the EU and NATO created "idea paths" that gradually influenced the position of the Swedish government on CIP and increased SEMA's chances of winning political backing for its project. The second half of the chapter offers an account of lessons derived from the more practical aspects of the preparatory work. They focus above all on methodological issues, such as the use of crisis scenarios, structured interviews, and exercises as tools for data collection and for creating a broad cross-sector process bringing together public and private stakeholders.

1 Setting the stage: the emergence of the societal security approach

Terrorist attacks at the beginning of the new millennium contributed to preparing the way for a whole range of ideas forming part of what has been termed a "societal security approach", emphasizing the protection of critical infrastructure (CIP) and vital functions in society.[1] Such ideas already emerged in the 1990s and were shaped by the fear of the millennium bug (Y2K), but the collective efforts springing from the fight against terrorism gradually led to a consolidation of this approach to security.

In societal security, less emphasis is placed on protecting the national territory from large-scale military attack than on maintaining an uninterrupted supply of services and functions essential to society such as energy, communication, transport, financial services, and health care. The societal security approach includes a category of threats that have been labeled "transboundary emergencies" because of their "potential to jump the borders of nations and systems, snowballing into disasters of international proportions".[2]

An excellent example of this type of transboundary threats – transboundary both in a functional and a geographical sense – were the viruses that were spreading around the globe after the new millennium: SARS and H5N1. SARS, which claimed almost 800 deaths on different continents between the years 2002 and 2003, did not develop into a pandemic, but was still a powerful wake-up-call illustrating the societal paralysis and the huge economic costs that could result from a

1 For a concise summary of the fundamentals of the societal security approach, see the contribution by M. Rhinard, 'Societal Security: An Emerging Role for the European Union', in European Policy Centre, EPC (ed.), *Building Societal Security in Europe: The EU's Role in Managing Emergencies*, working paper no. 27 (Brussels: EPC, April 2007), pp. 8–21. The Working Paper may be downloaded at <http://www.epc.eu> (accessed 13 August 2007). See also Daniel Hamilton, Bengt Sundelius and Jesper Grönvall (eds.), *Protecting the Homeland: European Approaches to Societal Security – Implications for the United States* (Washington, D.C.: Center for Transatlantic Relations, Johns Hopkins University, 2006).

2 For further definition of the concept "transboundary emergencies" and an interesting exploration of the challenges of transboundary emergency management in a European context, see Arjen Boin and Bengt Sundelius, 'Managing European Emergencies: Considering the Pros and Cons of an EU Agency', in EPC, *Building Societal Security in Europe*, pp. 33–46.

transboundary health-related crisis. When the aggressive avian influenza virus H5N1 reached the European continent in 2004, the awareness of the potential effects of a pandemic on society had thus already been raised. If H5N1 were to mutate into a virus that could be transmitted between humans, a catastrophe could ensue. With its broad impact and devastating potential for wiping out up to 50 per cent of a country's workforce, an influenza pandemic would very soon have severe consequences for society at large, making it very hard to maintain a minimum level of critical societal functions in the afflicted regions. In Sweden, as in many other countries, the analysis of the pandemic scenario helped to highlight the dependencies running across businesses, governmental bodies, organizations, and institutions in charge of critical societal functions, within and between countries.

This chapter will describe the launch of a project aimed at mapping and analyzing critical dependencies in Swedish society. The project was formally initiated at the Swedish Emergency Management Agency (SEMA) in spring 2006 and will continue until the end of 2008, but preparations for the project already started in 2004. The focus will be on the preparatory stages – from the project's conception at the agency to the point when the government formally charged SEMA with carrying out the project. Inspired by literature in political science on the role of ideas, how they are formed, and the impact they may have on policy, the chapter will seek to describe the national and international context of ideas during this period and the effect they had on the definition and launch of the project.[3] The description of the process leading up to the formal tasking by the government will also include a few lessons learned by the project team during the preparatory stages concerning the involvement of the private sector, methodology, and the need for high-level support.

3 See, e.g., Judith Goldstein and Robert O. Keohane (eds.), *Ideas and Foreign Policy: Beliefs, Institutions, and Political Change* (Ithaca, NY: Cornell University Press, 1993).

2 SEMA – an agency with a cross-sector mandate

In March 2000, a special investigator was appointed by the Ministry of Defence to lead a commission of inquiry, the *Swedish Commission on Vulnerability and Security*. In May 2001, the investigator presented a report to the Swedish government.[4] He concluded that the increasing integration and interdependency of vital technical systems in society was an important factor that, in combination with the overall changes in the security environment, required reforms in the Swedish framework for emergency preparedness. One year after the publication of the commission's report, in the summer of 2002, SEMA was established.

SEMA was created as a centrally placed actor within a new structure for emergency preparedness that was better adapted to the security challenges of the post-Cold War world. The agency's role may be described as that of a "soft coordinator", providing support to municipalities, county administrative boards, other central government agencies, the government offices, and the business community.[5]

In contrast to most other central government agencies in Sweden, SEMA has an explicit cross-sector mandate. Its *raison d'être* actually consists in the agency's ability to adopt a holistic perspective on emergency preparedness, spanning functions and sectors within both the public and the private spheres. A core mission of SEMA is therefore to achieve a broad overview of how and to what extent functions and

4 The Swedish Commission on Vulnerability and Security, *Vulnerability and Security in a New Era: A Summary*, SOU 2001: 41 (Stockholm, 2001) <http://www.regeringen.se/sb/d/108/a/55762;jsessionid=aO-Jp8wutGKe>, accessed 13 August 2007.

5 SEMA offers training and education, compiles knowledge through strategic analysis and research funding, and develops technical solutions for information-sharing and coordination. Another important task of the agency is to distribute funds from the Swedish national budget for strengthening emergency preparedness. SEMA was primarily created as a planning agency with few operative responsibilities in times of crisis. However, after the tsunami crisis in 2004, SEMA's responsibilities in crisis were accentuated, and the Situation Centre within the agency has been boosted. Currently, SEMA's role and mandate are being reviewed. A special investigator has been appointed by the government to explore the means and consequences of a fusion between SEMA, the Swedish Rescue Services Agency, and the National Board of Psychological Defense. The results were presented on 7 May 2007, but the outcome remains unclear at the time of writing.

sectors depend upon each other, and particularly how these patterns of dependence are affected in times of crisis.

3 Early experiences of dependency analysis

From the very beginning of the agency's existence, SEMA studied, or was sometimes directly involved in efforts at carrying out, more limited forms of dependency analysis. This was mainly a result of the agency's responsibilities in the area of risk and vulnerability analysis.

SEMA's role as described in the agency's instructions from the government is to support the other actors within the emergency preparedness system with the necessary methodological tools to conduct risk and vulnerability analysis. SEMA is also responsible for bringing together the various pieces of analysis into a synthesis. Dependency analysis is seen by the agency as an implicit, but important part of this work on risk and vulnerability.[6]

However, the overall quality of the risk and vulnerability analyses that SEMA received during the first years was rather poor, and more often than not, they contained very little qualified information about dependencies. Frequently, the analysis was limited to general conclusions about the dependency on electricity, telecommunications, and IT, without describing the degree or nature of this dependency in any more detail. Furthermore, the perspective was generally confined to the sector or the geographical area in question.

In some cases, crisis scenarios were used as a point of departure. However, these scenarios tended to reflect crisis situations that were local or in other ways restricted in scope, causing only limited cross-sector

6 All actors within the emergency preparedness structure (central government agencies, municipalities, county administrative boards, and county councils) are required by law to submit annual risk and vulnerability analyses to the government. SEMA has produced several guidelines on how to conduct risk and vulnerability analysis. However, these guidelines only contain recommendations. SEMA has had no mandate to force the actors to apply the analytical framework suggested by the agency. All guidelines may be downloaded from the SEMA website. Some of the guidelines contain English summaries, which may be found at <http://www.krisberedskapsmyndigheten.se/4435.epibrw> (accessed 13 August 2007).

consequences on a national level. Examples of such scenarios include local transport accidents, a computer-crash, or a regional storm.

Seen from a holistic, societal security perspective, many pieces of the dependency puzzle were missing. The fragmented and disparate information from the risk and vulnerability analyses did not meet SEMA's needs to achieve overview and synthesis. Although many central agencies also produced other types of valuable studies, analyzing the vulnerability of critical services and products, the focus often remained intra-sectoral.[7]

Among the missing pieces of the puzzle were the dependencies involving the private sector and the international links. In a society where an increasing number of critical societal functions were being partly or wholly privatized and delegated to companies that often operate in an international arena, interaction with the business community had become essential. However, private actors conducting business in Sweden were not legally required to hand in information from their business continuity plans describing vulnerabilities and critical dependencies. The problem was even more complicated when critical dependencies extended across the national borders.

Questions concerning the consequences of a serious disturbance in one part of society (a disturbance originating in Sweden or in another country) on entire chains of dependent services and products in other sectors, and their effect on the overall capacity to handle a crisis situation, were largely left unanswered. In order to be able to prioritise resources and measures aimed at strengthening emergency preparedness on a national level, the agency needed to conduct more comprehensive cross-sector analyses that included international perspectives.

7 One example of a sector where there have been many attempts at analysing risk and vulnerability is the energy sector. This is due to the cold Swedish climate, which demands a robust power infrastructure. The "HEL project" carried out by the Swedish Energy Agency between 2001 and 2004 was dedicated to improving the reliability and security of electrical power supply. As part of the work, the agency also studied the dependencies of other functions in society on electrical power. For more information and project reports, see <http://www.energimyndigheten.se/> (accessed 13 August 2007).

4 Inspiration from abroad: the Canadian and Dutch examples

The idea of starting a larger project to map and analyze critical dependencies in Swedish society took shape within the agency in 2003–2004. At that time, several countries had begun to look more closely at the issue of infrastructure dependencies from a broader security perspective. This interest in dependency analysis was part of the increasing focus on protecting and upholding critical functions in society – a sphere of activities that was subsumed under the amorphous heading of CIP (Critical Infrastructure Protection). Although the fight against terrorism had a big influence on CIP agendas all over the world after 11 September 2001, the earlier panic surrounding the alleged Y2K problems became an important trigger for various efforts in the area of CIP, and above all in the more limited sub-area of CIIP (Critical Information Infrastructure Protection).

Canada was one of the countries that developed extensive knowledge of CIP and CIIP at a very early stage. Among the European members, the Netherlands was one of the forerunners. SEMA had well-established contacts with both Canada and the Netherlands, and the work done in these countries was an important source of inspiration for the agency.

Initial lessons from the major Canadian National Infrastructure Risk Assessment (NIRA) conducted by the National Contingency Planning Group (NCPG) – which aimed at preparing Canada for the transition to the year 2000 – had already been shared with representatives from the Swedish Agency for Civil Emergency Planning (SEMA's predecessor) in 2001.[8] The NCPG had set out to identify and examine important infrastructure elements, determine their criticality, and assess the probability of their failure as a result of the "millennium bug". The results of the NIRA's research were developed further in 2000 by the Infrastructure

8 A description of the work with NIRA was provided at the first workshop organised by the CRN (Crisis and Risk Network, formerly Comprehensive Risk Analysis and Management Network) in Uppsala, 3–4 May 2001. For more information about this event, see <http://www.crn.ethz.ch/events/past-events/> (accessed 13 August 2007). More information about NIRA and the achievements of NCPG and CIPTF may also be found in Myriam Dunn, Jan Metzger, and Andreas Wenger (eds.), *International CIIP Handbook 2002* (Zurich: Center for Security Studies, 2002), at pp. 121–6 <http://www.crn.ethz.ch/publications/crn_team/detail.cfm?lng=en&id=15206>, accessed 13 August 2007.

Analysis Group (IAG), which produced so-called Infrastructure Profiles (IPs) containing a more detailed analysis of dependencies. When the Analysis Group was converted into the Critical Infrastructure Protection Task Force (CIPTF) within the Department of National Defence in Canada, the exploration of dependencies increased. SEMA followed this work closely.[9]

In the Netherlands, too, the fear of the alleged Y2K bug had led to awareness that essential business processes were becoming increasingly interlinked, and that a breakdown or disruption within the supply chain could have serious negative consequences across a wide range of dependent processes. Although some work had been done to prepare the country for the new millennium, it was only after the terror attacks in 2001 that a more comprehensive intergovernmental project on CIP and dependencies was launched. The first step was a Quick Scan aimed at providing a rough overview of the sectors, products, and services that could be considered to be critical from a national security perspective, and how they depended upon each other.[10] When SEMA visited the Dutch Ministry of the Interior and Kingdom Relations and the Netherlands Organisation for Applied Scientific Research (TNO) in the beginning of 2004, the project was moving beyond the Quick Scan, and initial conclusions could be derived from the results of the first step.

9 An important forum for exchange of ideas and lessons learned was the CRN (Crisis and Risk Network). CRN workshops with representatives from Sweden, Switzerland, Canada, the Netherlands, Norway, Denmark Germany, and Austria were held on a regular basis starting in 2001. In spring of 2004, SEMA hosted a CRN workshop entitled "Societal Security and Crisis Management in the 21st century", which included an in-depth session focusing on lessons from the Canadian dependency project. For more information about this workshop, see <http://www.crn.ethz.ch/events/past-events/> (accessed 13 August 2007).

10 Ministry of the Interior and Kingdom Relations, *Critical Infrastructure Protection in the Netherlands* (Den Haag, April 2003) <http://www.minbzk.nl/contents/pages/5018/DGOOVNCC-QuickScan.pdf>, accessed 13 August 2007). The CIP project and the Quick Scan were part of the "Action Plan for Security and Combating Terrorism" that was presented by the Dutch cabinet in October 2001.

5 Getting government support in the context of transatlantic and European cooperation

One of the lessons derived from the Canadian and the Dutch work on critical dependencies was that in order to achieve relevant results, high-level support was crucial – both political support and support from the rest of the stakeholders that were to participate in the analytical effort. For SEMA, acting as an independent agency under the Ministry of Defence, the formal support of the Swedish government was crucial in advance of its exploration of "weak links" in society.[11]

The position of the Swedish government towards CIP and societal security was in its initial stages in 2003. Within the Ministry of Defence, awareness of the vulnerabilities of modern society was increasing. It was the Ministry of Defence that had initiated the Swedish Commission on Vulnerability and Security in 2001. The commission's report, as well as a government bill on security and emergency preparedness presented in 2002, both pointed to the existence of critical interdependencies in society.[12] However, the focus of the government in terms of thinking about and acting upon threats to society's essential functions remained essentially limited to a number of critical technical systems often referred to as "the technical infrastructure".[13] Compared to the holistic view applied by the Canadian Task Force (CIPTF), the perspective of the Swedish government was narrow.

SEMA had studied the work of the Canadians and had seen the possibilities of a broader approach to CIP. In its aspiration to get government

11 According to the Swedish administrative model, the central government agencies enjoy a comparatively large degree of independence. They are, of course, controlled by the government, but not in the administration of their day-to-day business (an involvement on such a detailed level would be described as "ministerial rule", which is forbidden in the Swedish constitution). The government's control is exerted through laws and regulations and through the distribution of funds, the setting of targets, and following up of results.

12 The Swedish Government, *Samhällets säkerhet och beredskap*, government bill 2001/02:158 (Stockholm, 14 March 2002).

13 A common definition of the term "technical infrastructure" is "the systems involved in the provision of power, telecommunications, and IT". See, e.g., Swedish Commission on Vulnerability and Security, *Vulnerability and Security in a New Era*, p. 8.

support for a more extensive exploration of dependencies, the project team was helped by the developments in the context of Transatlantic and European cooperation. The ideas that became embedded in the work on CIP within NATO and the EU contributed to the Swedish government's view of CIP also in a national context.

5.1 Transatlantic cooperation on CIP

NATO has a long tradition of working with issues in the area of Civil Emergency Planning (CEP), and it was as part of this cooperation, and together with the members of the Euro-Atlantic Partnership Council (EAPC), that CIP was introduced as a new topic by the Canadian representatives in November 2002.[14]

The relevance of CIP was perceived as being high in the aftermath of the attacks on 11 September 2001. At the end of 2003, the Senior Civil Emergency Planning Committee (SCEPC) was able to present a CIP Concept Paper and a Road Map for the work of its subcommittees. The Concept Paper was very much influenced by the ideas developed in member states where work on CIP was already well underway – such as Canada and the US.[15] For NATO as an organization previously dominated by a more classical security outlook and focused on state-based enemies and military resources, the CIP Concept Paper was part of a reorientation towards a security approach emphasizing vulnerabilities within societies and peacetime transboundary threats.

It was SEMA that represented Sweden in the Ad-Hoc Group for CIP that was formed under one of the subcommittees to SCEPC. For the government of Sweden (as a non-member of NATO), the co-operation in the framework of EAPC was important, as it gave Sweden the possibility to take part in the transatlantic security dialogue.

SEMA was, from the beginning, an active participant in the Ad-Hoc Group, working closely with the other members to carry out the tasks

14 It was at the Summit Meeting in Prague that year that CIP was formally included as part of the common agenda.

15 NATO/EAPC, *Critical Infrastructure Protection – Concept Paper,* EAPC(SCEPC)D(2003)15 MULTIREF, 10 November 2003.

included in the Road Map. As a contribution to the work in the Ad-Hoc Group, the agency offered to host a large seminar on CIP together with its Canadian sister agency, the Office for Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), in November 2003.[16]

The seminar was part of the mission of the Ad-Hoc Group to increase the understanding of CIP among the EAPC countries. The seminar dealt with many of the fundamental issues in CIP, such as the need for cross-sector and transboundary co-operation, examples and models of public-private partnership, and methods for dependency analysis. The latter was addressed by the head of OCIPEP in his keynote speech, which related the experiences of the Canadian work on interdependencies. The Swedish representation at this event was strong, including among others the state secretary at the Ministry of Defence, the director of the Confederation of Swedish Enterprise, and the Swedish king.

This emphasis on CIP and infrastructure dependencies in the context of trans-national co-operation was soon reflected within the Swedish government. Before 2003, CIP-related issues had been an almost exclusive concern for the Ministry of Defence. However, as a result of the increasing pressure to administer cross-sector CIP issues in a more efficient way, an informal working group on CIP was put together in 2004 with representatives from several ministries. Although the working group was an ad-hoc constellation and only remained active for a period of time, it was a sign of the broad approach that was necessary to manage the challenges of societal security.

The institutionalization of CIP in the transatlantic context was an important first step. More important in terms of the impact on the government's policy, however, was the co-operation that was initiated in the European Union in 2004.

16 Documentation (in the form of a brochure and a comprehensive CD-ROM containing the transcripts of most of the presentations and workshops) from the seminar, which took place in Stockholm on 17–18 November, may be found at SEMA's English homepage <http://www.krisberedskapsmyndigheten.se> (accessed 13 August 2007).

5.2 European cooperation on CIP

If the attacks of 11 September 2001 had been an important trigger for the work on CIP within NATO, the bombings in Madrid and London in 2004 and 2005 played a similar role for the efforts in the EU context. Both attacks on European soil involved the destruction of central transport infrastructure and they were carried out in the centres of the capitals, in broad daylight, with several hundred people dead.

At the European Council meeting of June 2004, the Commission was asked by the governments of the EU member states to prepare an overall strategy in the area of CIP. Already in November the same year, the Commission received a new mandate to propose a European Programme for Critical Infrastructure Protection (EPCIP) and the establishment of a Critical Infrastructure Warning Information Network (CIWIN). This resulted in a Green Paper one year later and eventually in a proposal for a Council Directive on EPCIP.[17]

The scope and content of EPCIP was defined in a broad consultation process involving participants from government, industry, and academia in all member states. In June and September 2005, seminars were organized by the Commission to receive feedback on the policy options outlined in the Green Paper. The Commission also asked for continuous submission of comments and examples from member states as a basis for developing the program on CIP. One of the more active contributors was the Dutch government, together with the Netherlands Organisation for Applied Scientific Research (TNO), which shared their experiences from the work with the Quick Scan and the Dutch CIP program.

In the Green Paper, particular attention was devoted to the issue of interdependencies. The Commission argued that studies in interdependencies should be considered a necessary tool in assessing the potential impact of threats against specific CI (Critical Infrastructure) within and

17 European Commission, *Green Paper on a European Programme for Critical Infrastructure Protection*, COM 2005(576) Final (Brussels, 17 November 2005); and *Proposal for a Directive of the Council on the Identification and Designation of European Critical Infrastructure and the Assessment on the Need to Improve Their Protection*, COM(2006) 787 Final (Brussels, 12 December 2006).

between member states. It further suggested that the Commission should work together with the member states and the owners/operators of CI to identify those interdependencies and apply appropriate strategies to reduce risk and vulnerability where possible.[18]

The EPCIP process in the EU context created incentives for centrally placed decision-makers in Sweden to deepen their understanding of the protection of society's critical functions. That the government had acquired a more holistic perspective on CIP and security was apparent in the bill on security and emergency preparedness that was presented in March 2006.[19] The bill included a national security strategy that spelled out the targets and means of managing transboundary threats to individuals and society.[20] The perspective was no longer confined to the protection of "technical infrastructure" in a narrow sense, as had been the case in the bill from 2002. The government now clearly emphasized the many critical dependencies linking functions within a wide array of sectors and acknowledged the complex, multi-dimensional nature of those dependencies (technical, organizational, human, legal, geographical, and financial). The need for coordination between national efforts in the area of CIP and the work carried out in the European and transatlantic context was also stressed.[21]

This approach was very much in line with the ideas endorsed by SEMA. Although the project team had started preparations in 2004, it was not until December 2005, when the work within the EU was well under way, that the agency asked the government to be formally tasked with a large-scale project aimed at exploring critical dependencies in Swedish society. The answer was positive and the official starting date for SEMA's undertaking was set for May 2006.

18 See European Commission, *Green Paper on a European Programme for Critical Infrastructure Protection*, p. 7.

19 The Swedish Government, *Samverkan vid kris – för ett säkrare samhälle*, government bill 2005/06:133 (Stockholm, 22 March 2006).

20 See Swedish government bill 2005/06:133, pp. 44–7.

21 See government bill 2005/06:133, pp. 83f.

6 Private sector participation and the use of the pandemic crisis scenario

One of the issues that was of great importance to the project team was finding ways to get the private sector to participate in the work. In all of the areas of society that SEMA hoped to explore, a significant number of the stakeholders were private. The experiences derived from the Canadian and Dutch work on CIP had also clearly shown that getting the attention and engagement of a wide spectrum of private actors was rewarding for the final result.

During the preparatory stages in 2004 and 2005, the Swedish project team established various contacts with businesses in sectors of interest for the project. The aim was to introduce the work ahead and get some feedback on the project design and the relevance of the expected outcome. At the same time, it was an opportunity to hold a structured discussion on the business continuity plans of the different companies, their preparedness for managing various crisis scenarios, and their perception of critical dependencies in those crisis situations. One of the scenarios used by the project team in the dialogue with the companies was that of a pandemic crisis. It was this scenario that really attracted the attention of the business representatives.

The topicality of the pandemic influenza scenario at the time was significant. Although the first lethal case of avian influenza infection (H5N1) had been detected as early as 1997, the virus only appeared in Europe in 2004 and 2005. At this time, frightening comparisons also started to appear between H5N1 and the virus that had caused the Spanish flu in 1918, killing approximately 20 million people globally. The previous experiences of SARS in 2002 and 2003 had raised the awareness of the effects of a pandemic scenario, and it was now gradually becoming clear to an increasing number of crisis managers all over Europe that the pandemic threat could not be framed as a mere medical problem and a concern for the Public Health sector. A pandemic influenza was a concern for society as a whole.

The consequences of a full-blown pandemic would be felt across all sectors and levels of society, affecting the overall supply of human resources, strategic products, and back-up facilities. There was a risk of severe disruptions in a wide array of fundamental systems and services, such as the production and distribution of electricity, telecommunications, money transmission and cash access, postal services, rescue services, the police, private security services, hospital care, supply of medicine and food, child care, etc. Since a pandemic would spread globally, the possibilities of getting assistance from neighboring countries would be limited. The number of critical dependencies that would be affected in such a scenario was almost incalculable.

Many of the businesses that were approached by SEMA's project team had not realized the vast consequences of the pandemic scenario. Few of them had included a pandemic scenario in their business continuity plans. Where such a scenario had been considered, often only the aspect of an unusual reduction in the own workforce had been taken into account. The companies' dependencies on other essential services in society were generally not part of the analysis. In the face of this daunting scenario, a majority of the business representatives showed an interest in receiving guidance from SEMA and other responsible government bodies on possible ways to increase their emergency preparedness, including methods for dependency analysis.

The business representatives who were part of SEMA's survey were generally risk managers, chief security officers, or sometimes the heads of IT security or human resources. They carried responsibility for business continuity planning in their respective companies, but were not part of the management, and frequently had no mandate to take decisions regarding their company's participation in SEMA's project. Such an involvement could imply the sharing of sensitive information, and it would also take time and cost money. In order to increase the chances of encouraging more extensive participation, SEMA had to get the attention of the managerial level.

One way of reaching these top-level executives was to involve a prestigious institution within the Swedish society that included a great

number of managing directors, heads of associations within trade and industry, and highly esteemed academics – the Royal Swedish Academy of Engineering Sciences (IVA). After some initial contacts in 2005, it was decided that SEMA and IVA would engage in a loose partnership where SEMA would be able to draw on IVA's wide-ranging networks. IVA would also take on the task of preparing a document on Emergency Preparedness Foresight – an analysis identifying the vulnerabilities and dependencies that would be critical for society's emergency preparedness for the next 10–20 years. One of the scenarios used by IVA would be "pandemic crisis".[22]

7 Drawing the contours of the dependency project

In parallel with the efforts to gather support at the political level and among both private and public stakeholders for the project ahead, the members of the team elaborated the design of the project. For SEMA, it was of great value to have been able to study the methodology, the results, and the lessons learned from the work that had been carried out by the project teams in Canada and in the Netherlands. The project team was also able to draw upon the experiences gained from the activities within NATO and the EU. Although SEMA was not starting from scratch in the area of CIP, the design of the Swedish dependency project demanded some important exploratory and definitional work:

1. Formulating goals
2. Defining key concepts
3. Mapping society
4. Identifying the limits of analysis
5. Testing methodology through a pilot study

22 More information about the partnership between SEMA and IVA, as well as IVA's work with the *Emergency Preparedness Foresight*, may be found at the IVA homepage at <http://www.iva.se> (accessed 13 August 2007).

7.1 Formulating goals

Among the first tasks of the project team was that of formulating goals for the work ahead. The following goals were agreed upon:

- The overarching goal for the dependency project at SEMA is to produce new knowledge on cross-sector dependencies that may cause or contribute to serious crises with consequences on a national scale. This knowledge should form the basis for taking concrete measures to reduce the identified vulnerabilities and thus strengthen society's emergency preparedness. The measures may range from exercises and educational activities to proposals for new co-ordination structures, legal reforms, or investments in back-up systems.
- A more specific goal is to support various internal processes at SEMA, such as: providing a more solid analytical ground for the agency's distribution of funds within the emergency preparedness system; contributing to a more holistic view in the area of risk and vulnerability analysis and identifying knowledge gaps suitable for research initiatives.
- Another specific goal is to contribute to SEMA's efforts at establishing public-private partnerships. On the most fundamental level, this is a matter of raising the awareness within both the public and the private sectors concerning the existence of critical dependencies. The results of the project should also provide incentives for new forms of cross-sector cooperation that may range from loose networks to more formalized forums for information-sharing of the kind initiated by SEMA in the area of information assurance.
- A fourth goal is to compile the results of already existing research, analysis, and exercises, carried out in a variety of areas of society, and provide a "virtual library" with reference material on dependencies, risk, and vulnerability.
- Finally, the analytical process established by the project team should be designed in a way that permits it to "live on" (after the termination of the project) as part of the ordinary work at the agency.

7.2 Defining key concepts

Defining key concepts was also part of the early preparations of the project team:

A *dependency* is a relation between two products/services – one dependent and one supplying. The relation may sometimes be one of *interdependency*, meaning that the dependency is mutual and the two products/services thus are both dependent and supplying. The dependencies may be of varying nature. The relation may, for example, consist in the provision of a *technical* service, of *logistical* support, of key *expertise*, or of a *legal* framework.

A *critical dependency* is a relation between two products/services where the dependent product/service would be seriously disrupted if it should become impossible to deliver the supplying product/service. A condition for criticality is that the supplying product/service could not be replaced with another product/service. Another condition is that the consequences of the disruption of the dependent product/service would have the effect of either causing a crisis or seriously inhibiting the management of an existing crisis situation. In many cases, the disruption of the dependent product/service would lead to indirect, cascading effects, causing disruptions in other sectors.

7.3 Mapping society

In order to be able to study such a complex subject-matter as that of a modern society, the Swedish project team had to establish some form of rough map describing the products/services, functions, and sectors that would be used as a point of departure for the analysis. At the time when preparations for the project began, there was no official list of critical sectors or functions in Sweden. The project team thus had to start with an inventory of existing criticalities in Sweden and in other countries. Within Sweden, the project team did, for example, consider the previous system of civil support functions that had been an integrated part of the Total Defence concept. Foreign examples of critical sectors were found in Canada and in the Netherlands.

The ambitious multi-dimensional Canadian "layer model" that was developed by the CIPTF was seen as interesting, but too advanced and theoretical to be of practical use within the SEMA project.[23] The Canadian division of society into 36 "infrastructure elements" (used in combination with the layer model) was studied carefully, however. So was the list of critical sectors, products, and services drawn up by the Dutch project team as part of their work with the Quick Scan. The Dutch list of 11 sectors and 31 critical products and services was deemed to be quite close to the needs identified by the Swedish team. With the exception of a few specific elements, such as the focus on different types of water management (a result of the country's topography), many of the Dutch sector categories also seemed relevant in a Swedish context.

After combining various possible alternatives, agreement was reached on a rough list with eleven tentative sectors and an unspecified number of functions.[24] The vast body of material made it particularly hard to pinpoint the relevant functions. One of the difficulties consisted in determining the right level of analysis. For example, were the functions within the Public Health and Medical Services sectors to be described on the level of "emergency care", or was it better to subdivide that function further into "sub-functions" such as "intensive hospital care" and "ambulance services"? Should those sub-functions perhaps be broken down further into other supportive services and systems?

These questions illustrated the central dilemma between reaching a sufficient degree of concreteness and detail in the results and the wish to cover as many sectors as possible to capture cross-sector dynamics.

23 The Canadian multi-dimensional model is divided into five levels of analysis (the international, federal, provincial, municipal, and private-sector levels). These are combined with three vertical sector-specific layers (operations layer, technical application layers and control layer), which in turn rest on two "common foundation layers" (a terrain layer and a feature layer). For more information on the layer model, see Dunn, Metzger, and Wenger, *International CIIP Handbook 2002*.

24 The list of eleven sectors and a number of critical functions are presented on a Societal Security fact sheet recently published by SEMA. The fact sheet may be found at the English version of the SEMA homepage. SEMA, *Critical Societal Functions: Suggested Definitions of Essential Functions from an Emergency Management Perspective* (March 2007) <http://www.krisberedskapsmyndigheten.se/templates/Page____1989.aspx>, accessed 28 August 2007.

The dilemma of how to achieve the right balance between depth and breadth was part of the task of identifying the limits of analysis.

7.4 Identifying the limits of analysis

In the Canadian work on dependencies, the universe of analysis consisted of the 36 critical infrastructure elements that had been sorted out by the NCPG and the levels of analysis contained in the multi-dimensional layer model. The direct dependencies of the infrastructure elements were evaluated by crosschecking all elements against each other. The degree of dependency was then rated and presented in a dependency matrix. The indirect, ripple effects of some of these dependencies were also analysed by means of a specific application called RAFLS (Relational Analysis For Linked Systems). The evaluation of dependency was based on input from approximately 60 experts who were engaged within the project over a period of many months.

For SEMA, this type of set-up was not feasible. To begin with, the available resources were more modest. The ambitious Canadian process with its elaborate theoretical framework had required a large body of project staff and significant support from external experts. SEMA had to apply a less personnel-intensive method. Furthermore, the search focus had to be limited in different ways.

Among the views that had been presented in the informal survey made by the project team in the beginning of 2004 was the importance of producing results that would be perceived as useful by the practitioners. There was a fear that broad overviews of dependencies on a macro level could become too superficial and abstract. If the output of the project was to form the basis for concrete measures aimed at reducing vulnerability in society, the results had to be more tangible. At the same time, it was recognized that it was not SEMA's role to be involved on the micro level and help individual companies with their business continuity planning. SEMA had to maintain its holistic cross-sector perspective.

One way of striking the balance between breadth and depth was to direct the enquiry towards a more limited number of "focal points" (critical functions) with the aim of analyzing, as thoroughly as possible, the

chains of dependency affecting those functions. One problem with this approach, however, was to choose the most rewarding focal points.

The project team decided to let different crisis scenarios provide some guidance to the choice. Functions that were perceived as specifically critical for the response in a certain scenario – but also a number of "support functions" – were picked out as focal points.[25]

Since the scenarios used by the project team served as analytical frameworks, guiding and delimiting the choice of focal points for dependency analysis, it was important to pick scenarios that would highlight different types of dependencies. The team opted for three main scenarios: "pandemic crisis", "power outage combined with international oil crisis", and "severe disturbance in electronic communications (involving SCADA systems)".

7.5 Testing methodology through a pilot study

After having studied a number of methods with a quantitative orientation as well as techniques for simulation and modeling, the project team opted for a straightforward qualitative approach. Its main ingredients were structured interviews with representatives for the focal points, scenario exercises combined with seminars and workshops involving different constellations of experts.

This method was tested in a pilot study that was carried out in 2005 and entitled "A Pilot Study: Critical Dependencies in a Pandemic Crisis".[26] The pilot study was confined to the dependencies affecting

25 The project team posed a number of questions to add focus to the selection process: Is the function essential for leading and co-ordinating the response; providing information to the public; responding operatively in other ways; restoring other functions? How would a serious disturbance within this function affect people's lives and health, as well as financial, societal, and environmental values and public trust? What levels of society would be affected? How would the consequences propagate geographically? In the first scenario, "pandemic crisis", focal points were chosen within eight different sectors. In the sector for Public Health and Medical Services, the focal points were "emergency care", "primary care", "infectious disease control", "pharmaceutical supplies", "medical counselling", and "social services for children and the elderly".

26 The English title is a direct translation from Swedish. The study 'Pilotstudie: beroendeförhållanden vid en influensapandemi' may be requested from SEMA by contacting the current project manager Ms Malin Fylkner at malin.fylkner@kbm-sema.se.

the systems for public health and social insurances. A pandemic scenario consisting of three phases was used. During the most acute phase, thousands of Swedish citizens were assumed to have died as a result of the pandemic. In certain workplaces, as much as 70–80 per cent of the workforce were missing.

One of the chains of dependencies that was mapped and analysed in the pilot study was the supply of "critical medicine".[27] Structured interviews were made with representatives of the Swedish Organisation of the Pharmaceutical Industry, the two competing wholesalers of medical products in Sweden, the state-owned chain of pharmacy retailers, relevant transport companies, IT companies, emergency hospitals, primary care, the National Board of Health and Welfare, and the Medical Products Agency. A seminar and a large exercise were also arranged with the stakeholders. The focus was on logistical, IT-related, and legal dependencies.[28]

The results of this analysis revealed a large number of critical dependencies. It showed, for example, that the majority of the agreements concluded with the various transport companies involved along the supply chain contained *force majeure* clauses that would be activated in a situation of pandemic crisis. The transport companies had also reduced their staff, and there was very little extra personnel to draw upon in emergency situations, making them a vulnerable link in the chain of dependencies.

In the analysis of IT-related dependencies, it further became clear that in order to maintain a continuous supply of medical products to the emergency hospitals, the primary care system, and the other end-consumers, a large number of highly interconnected systems governing stock control and order processing had to function – systems linking the international producers with the Swedish wholesalers, the transport

27 The "critical medicines" did not include vaccine and anti-viral drugs (which were dealt with separately), but for example cardiac medicine, insulin, and asthma medicine.

28 The term "legal dependency" was defined by the project team in the following manner: "A legal dependency arises when a product/service is dependent on the enactment of a regulation or the promulgation of a specific permission in order to be able to deliver in the circumstances created by a crisis situation."

companies, and the retailers. In many cases, the operation of these systems had been outsourced to an external provider. The interviews also showed that both the wholesalers and the state-owned chain of pharmacy retailers essentially relied upon the services of a single IT company.

Besides the logistical and IT-related dependencies, a broad range of legal dependencies were activated in the pandemic scenario. There was, for example no legal support that would allow the prescribing doctors or the retailers to identify key individuals in charge of critical services who would be given priority in the distribution of certain types of medicines. The rules concerning the need for a doctor's certificate would also need to be made more flexible in order to save labor.

All in all, the work with the pilot study contributed valuable insights into the vulnerabilities within the areas that were explored, but it also provided the project team with a few lessons concerning the choice of methodology.

The use of structured interviews proved very time-consuming, but was necessary for performing the detective work involved. By engaging in in-depth discussions with people at different levels within the various companies and agencies, the project team was able to acquire important information that seemed hard to extract in other ways. These interviews were also a great help in the mapping process. The importance of contacting people at the appropriate level was apparent. It was a great help to have the support of the managerial level when addressing the risk manager or the CEO at a company.

Furthermore, the pandemic scenario functioned very well and provided a powerful illustration of the many secondary effects of simultaneous disturbances in different sectors. The scenario-based exercises did, however, just like the interviews, prove to be rather time-consuming both in terms of preparations and in the assessment of the results. Nevertheless, the exercises allowed the project team to bring together actors from different sectors to discuss relationships of dependency that often required solutions based on new forms of private-public partnerships. The exercises were thus very rewarding and were highly appreciated among those involved. They also helped to reveal the value of the actual

process of interaction in which contacts were forged, perspectives were changed, and facts were established in broad co-operation.

8 Summary and concluding remarks

The purpose of this chapter was to describe the preparations at the Swedish Emergency Management Agency (SEMA) for a large project aimed at studying critical dependencies in Swedish society. The chapter has traced the gradual emergence of the ideas underpinning the project. It has shown how the interest in mapping and analyzing dependencies between critical functions in society has evolved as part of a new approach to security labeled "societal security", which captures many of the ideas represented in the areas of CIP and CIIP.

One point of departure in conveying the emergence of these ideas consisted in the early experiences of dependency analysis in Canada and the Netherlands. In particular, the work carried out in Canada has been described as a significant source of inspiration for SEMA. The chapter has also shown how the ideas developed by these pioneers in CIP were fed into the transatlantic and European context at moments when receptiveness was high due to the previous terror attacks. The concept of CIP and societal security dovetailed with the sense of vulnerability and interdependence that was created in the aftermath of the 2001 attacks in the US and the subsequent bombings in Madrid and London. When these ideas were institutionalized in NATO and the EU, their impact and their potential for shaping policy among the members increased.

At the time when SEMA was studying the holistic approach of the Canadians, the Swedish government had a more narrow view of CIP. However, through the work with CIP in NATO and the EU, "idea paths" were created that contributed to broadening the perspective of the Swedish government. The new approach of the government was reflected in the bill in 2006, which was very much in line with the ideas contained in the plans for SEMA's project. The principles guiding the government's security policy were captured in a National Security

Strategy that confirmed the importance of identifying and reducing vulnerability in critical functions across sectors and national borders. SEMA had also received the formal support of the government for its project a few months before the publication of the bill.

Besides describing the context of ideas and their effect on the definition and launch of the project, the chapter also sought to provide a few lessons from the more practical aspects of the preparatory work. One of the first lessons learned by the project team was the usefulness of crisis scenarios as a tool for attracting the attention of the stakeholders and explaining the complexity of critical dependencies. The pandemic scenario proved particularly valuable for illustrating how simultaneous disturbances in many sectors could affect chains of dependencies with consequences on a national scale. Another lesson was the well-known importance of communicating with the right people at the right level in order to confer legitimacy to the work and establish a trust-based dialogue. A third lesson learned by the project team was the challenge of reconciling broad cross-sector overviews with depth in research and analysis. The project team opted for a middle path consisting of a number of "focal points" within different sectors that were used as points of departure in mapping and analysis. This approach was tested in a pilot study in 2005 and found to be valuable.

The preparations described in this chapter came to an end in the spring of 2006, as the "real work" began. The new project team that was formed then has already made headway. By summer 2007, nine sectoral reports will be published that will map and analyse dependencies in the "health care", "financial services/social insurances", "energy", "trade", "media", "security and protection", "water and waste management", "food", and "telecom" sectors. The sector reports will be followed by a synthesis report.[29] Hopefully, their conclusions will provide the basis for measures that can diminish the vulnerability of Swedish society.

29 For further information on the project and its documentation, please contact the project manager, Ms Malin Fylkner. She may be reached at the following e-mail address: malin.fylkner@kbm-sema.se.

RISK MANAGEMENT IN THE CONTEXT OF SWITZERLAND'S CIVIL PROTECTION MECHANISM

Stefan Brem and François D. Maridor[1]

This essay provides an overview of developments in the field of risk and vulnerability analysis in Switzerland, especially from a civil protection perspective. Switzerland – like other countries in continental Europe – has experienced a fundamental shift in its security environment since the end of the Cold War. However, it is encumbered by a rather tight political decision-making process that is not always suited to the adaptation of rapid changes, as became clear after the attacks on New York and Washington on 11 September 2001. Nevertheless, Switzerland has been able to cope successfully with the challenges it has experienced in the last years. A more proactive approach is taken, however, when it comes to conceptual work and methodology. Recent milestones are highlighted in this context. Some possible future developments are also discussed.

1 The views presented in this chapter do not necessarily represent the position of the Federal Office for Civil Protection or the Swiss government.

"There can be no vulnerability without risk; there can be no community without vulnerability; there can be no peace, and ultimately no life, without community."

Morgan Scott Peck, American psychiatrist

1 Introduction

This essay provides an overview of the developments in the field of risk and vulnerability analysis in Switzerland, especially from a civil protection perspective. After giving an overview of the institutional and historical background of Switzerland's security structure, we will address some methodological considerations and highlight recent milestones in Switzerland's risk analysis and management context. We conclude by sketching some possible future developments.

2 Institutional change in Switzerland's security and civil protection structure

2.1 Historical and institutional background

Due to Switzerland's geographical characteristics and its socio-political background, analysing risk and vulnerabilities has a long tradition in the country. For centuries, communities living in the alpine valleys have faced several kinds of risks, natural or man-made, such as avalanches, landslides, isolation, famine, or fire in the village. Most of these events had to be managed at the level of the local community. However, solidarity between neighbours has been a well-established tradition for centuries.

Nowadays, direct democracy shapes the process of political decision-making in Switzerland and makes it a rather time-consuming, but fascinating endeavour. This is particularly true at the federal level as laws are developed either through parliament or as the result of popular votes (initiatives and referenda). At the beginning of the 21st century, when

enormous amounts of information are circulating at unprecedented speed, this systemic slowness tends to favour the principle of reactivity over pro-activity.

Nevertheless, information and communication are essential elements of modern societies. For governments as well as companies, it is crucial to communicate in an open and transparent fashion – a task that is not always easy in times of crisis or uncertainty. It is therefore interesting to note that in Switzerland, a distinction is made between *warning* the authorities, emergency services, and service providers on the one hand, and *alarming* the broader population on the other. The first group receives precise and actionable information; the second should not be overwhelmed with too many details, but know how to react in general. Hence, in extraordinary situations and in the face of increased media attention, the authorities have to strike a balance between over-reaction and lack of reaction – also with regard to their communication policy.

2.2 Historical developments

During the Second World War, the coordination and management of scarce resources was a necessity for the armed forces as well as for civilians in Switzerland. This experience influenced the creation of the concept of General Defence and its instruments, which were geared to respond comprehensively to all possible threats and dangers, including a major armed conflict in Europe with mass casualty weapons. The end of the Cold War and the emergence of a wider spectrum of imprecise, mainly non-military dangers and risks called for a modification of the concept of a defence structure that focused on inter-state wars as worst-case scenarios. It had to be replaced by a new, more flexible form of collaboration, which was to counter shifting challenges more quickly and with less resources.[2]

2 Swiss Government, *Security through Cooperation: Report of the Federal Council to the Federal Assembly on the Security Policy of Switzerland of 7 June 1999*, SIPOL B 2000 (Berne, 1999) <http://www.vbs.admin.ch/internet/vbs/en/home/documentation/bases.html>, accessed 7 September 2007.

2.3 Civil protection as an umbrella system

Nowadays, civil protection in Switzerland is an integrated system comprising protection, rescue and relief tasks. It has a mandate under federal law to protect the population, its livelihood, and its cultural heritage in the event of disasters and emergencies, as well as in the event of armed conflict. The five partner organisations – the police, fire departments, public health services, technical services, as well as protection and support services – are in charge of their specific tasks and provide mutual support to each other. Joint management and cooperation ensures coordinated planning and preparation, as well as operational command in case of deployment. The Federal Office for Civil Protection (FOCP) supports the cantons[3] and municipalities as well as the partner organisations in their civil protection activities.

2.4 Civil protection and risk management

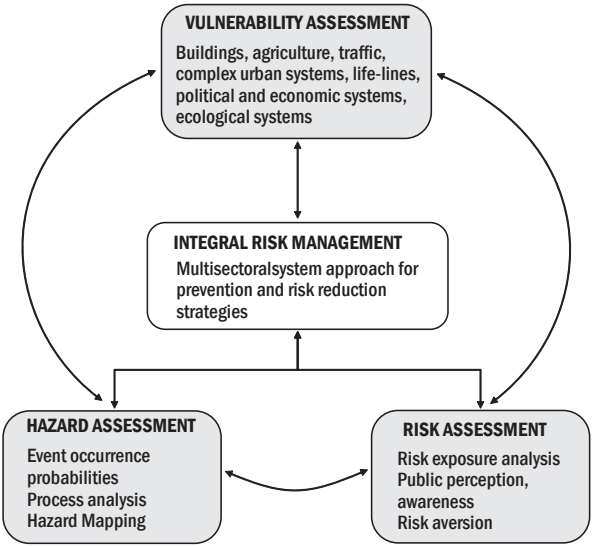
The federal government is responsible for the early identification of threats and dangers and for providing the public with the necessary information. In principle, the cantons are responsible for dealing with disasters and emergencies – especially from a local to regional scale – while the federal government's competence lies with armed conflicts and specific disasters and emergency situations (e.g., threats from radioactivity, dam bursts, or epidemics). As a matter of fact, the scope of risk and vulnerability analysis in the FOCP has to consider not only the typology of the threats, but also the functioning of a system (federal government) of systems (cantons). While the federal government has a much larger conceptual role in identifying threats and risks and in the preparation phase, subsidiary echelons are much more important when it comes to actual implementation and risk management.

3 The cantons are the constituent states of Switzerland.

3 Risk analysis and management in Switzerland

3.1 Methodological considerations

The most important task of politicians and managers is to make decisions and to execute them. Risk and vulnerability analysis is one important element of the decisionmaking process. It integrates different methodologies and techniques. Generally speaking, risk analysis and management is based on three interlinked processes: risk assessment, hazard assessment, and vulnerability assessment.



Source: Gheorghe, Adrian V. (ed.), *Integrated Risk and Vulnerability Management Assisted by Decision Support Systems* (Dordrecht: Springer, 2005), p. 23.

This methodology helps the analyst to preserve a global perspective while still focusing on the 'Achilles' heel'; it facilitates anticipation and enables the decision-maker to make adequate use of the available means and resources.

According to Paul Slovic, knowledge (information) and experience (affect) strongly determine the perception and the acceptance of risk.[4]
In Switzerland, a variety of risk analysis methodologies are used, depending on the sector and relevant activity. Responsibility is an essential criterion in risk management. Among other things, it depends on legal considerations and ownership.

Risk and vulnerability analysis is a process involving partners from different administrative bodies from the federal, cantonal, and municipal levels as well as the private sector. This process has to take into account political, strategic, and operational parameters.

Risk matrix techniques are widely used in both the public and in the private sectors, particularly for risk communication. They are useful for merging opinions (i.e., "common sense", experience) with expert knowledge and statistical evidence. In the public sector, the risk matrix technique is widely used by the army, civil protection authorities, and the police. In the private sector, banks and insurance companies frequently apply this methodology. Other techniques include checklists and fault tree analysis. They are often applied in "closed systems" (i.e., nuclear plants, chemical factories, transportation networks, etc.).

When considering natural risks, it is important to differentiate between the local, regional, and supra-regional levels: In order to establish a hazard register, for example, methodologies are needed that include mainly qualitative information (i.e., soil, geology, demography etc.). At a higher level (region, canton, country), it is necessary to apply methodologies that are able to integrate qualitative and quantitative aspects (i.e., financial, environmental, and social impact) in addition to calculating damage and monetary costs.

3.2 Practical application and milestones

In Switzerland, the municipalities and cantonal authorities as well as the private sector have primary responsibility for risk and disaster management. Most of the emergency response capabilities are located at the cantonal level.

4 Slovic, Paul (ed.), *The Perception of Risk* (London: Earthscan, 2000), p. 405.

However, there is a long-standing tradition of inter-cantonal solidarity: the neighbouring cantons help each other when a disaster strikes and the resources of one canton are exhausted or when several cantons are affected simultaneously.

At the federal level, the most powerful tool is the army. When the cantonal resources are exhausted and upon request by the cantonal authorities, the army may provide support that may include subsidiary security forces, military disaster relief, transport capacities, and engineering work. However, the federal authorities are only responsible in a few cases (epidemics, dam bursts, nuclear disaster, airplane and satellite crash, terrorist attack), but in all cases, the federal activities depend on the lower political levels and the private sector assuming their tasks:

1. Concerning technical risks (i.e., chemical accidents, dam ruptures, and nuclear accidents), the operators or the owners of the infrastructure are responsible for initial disaster management;
2. Concerning natural risk, municipalities are responsible for disaster relief and management;
3. In case of epidemic or epizootic diseases, the cantonal authorities are primarily responsible for crisis management.

In most cases, involvement of the federal authorities is subject to the three principles of legality (only when the law attributes responsibility to the federal government), proportionality (only to the extent necessary), and subsidiarity (only when the resources at the lower level are exhausted or unavailable).

These principles also apply to the civil protection mechanism, where risk management also starts at the local level, using mainly local resources from the partner organisations (police, fire brigade, public health services, technical services, and protection and support services). As stated above, the federal role is more prominent in the area of conceptual development.– It is in this area that the competencies of the Federal Office for Civil Protection (FOCP) and its predecessor agencies are to be found.

Renewed efforts to conduct risk analysis in a more comprehensive way have been launched since the end of the Cold War confrontation, as it has become important to identify and understand new risks and challenges in a changing world. Obviously, the new security concept was not only related to military threats. The first post-Cold War security policy report, entitled "Swiss Security Policy in Times of Change: Report 90 of the Federal Council to the Federal Assembly on the Security Policy of Switzerland" and published in fall of 1990, highlighted the preventive dimension in security policy. This provided a platform for a broader and more comprehensive approach to risk analysis in the field of security policy, including a general assessment of existential dangers.

As a concrete follow-up to this call for a new approach to risk analysis, an interdepartmental working group was launched in 1991. It was led by the now-defunct Central Office for General Defence (within the former Federal Military Department) and comprised experts from the public and private sectors as well as academia. After almost eight years, the working group produced a (non-published) brochure entitled *Risk Profile Switzerland* ("Risikoprofil Schweiz"), which described major risks to Switzerland by using a scenario-based methodology.

Almost simultaneously, i.e., between 1993 and 1997, several research units at the Swiss Federal Institute of Technology Zurich conducted a project on risk and safety of technical systems ("Polyprojekt Risiko und Sicherheit technischer Systeme"). The purpose of this interdisciplinary research project was the development of user-oriented risk analysis methods to enable risk assessment and management of technical systems at regional levels. Eighteen research papers and a final report were published, covering not only technical aspects of risks in general, but also legal considerations and various single-issue and interdisciplinary aspects of technical systems, processes, and protective measures.[5]

During this period, the former Federal Office for Civil Defence – the predecessor to the FOCP – published a study entitled "Katanos" on the prevention of natural disasters in 1995. It showed that Switzerland

5 Further information can be found at <http://www.vdf.ethz.ch/loadAllFrames.asp?showHtmlSite=themen/polyprojekt.html>, accessed 7 September 2007.

is – at least in principle – well prepared to respond to 90 per cent of the risks that can reasonably be foreseen and that were covered by the study. Secondly, it highlighted the relationship between areas of high-density population and infrastructures as well as the increasing amount of damage in case of a disaster. Thirdly, it recommended establishing hazard assessment to define preventive measures and further expand appropriate preparedness levels.

Five years later, the Federal Office for Civil Defence released "Katacheck", a computer software to be used by communities and regional authorities to asses, quantify, and rate local disasters and possible risks. Additionally, it helped to assess whether the existing mitigation means were appropriate.

In 1999, the Swiss Federal Council commissioned the National Platform for Natural Hazards (PLANAT) to develop a comprehensive strategy for improving protection against natural hazards. The Federal Council emphasized that protection against natural hazards should not only be provided for residents of the alpine region, but for the entire population of Switzerland. PLANAT was also tasked with establishing comparable security standards throughout Switzerland based on extensive risk management. Additionally, it was to improve ways and means for protecting the public and their livelihood as well as important material assets.

Two years later, the Federal Chancellery published its "leadership principle during, after, and before crises", which was intended as a checklist for senior decision-makers. It was to help them in complex crises to achieve a shared vision concerning decisions and to initiate appropriate action. As they were formulated in succinct and general terms, these leadership principles have found broad application. They have been tested and further developed by senior crisis managers under the lead of the Strategic Leadership Training within the Federal Chancellery.

Between 2001 and 2003, the federal administration established, under the lead of the Federal Department of Finance, an interdepartmental inventory of risks related to the administrative and financial assets and to the cultural heritage of Switzerland. This analysis should provide the

foundation for a fundamental revision of a national risk and insurance policy.

After the end of the Cold War, the Federal Council had submitted a second report on Switzerland's security policy to the Federal Assembly. By the end of the 1990s, the security-related organizations in Switzerland had to adapt to the new risks. The downsizing of the army, the restructuring of the intelligence services, and the changing of social paradigms are leading to fundamental modifications in the defence network. The new paradigm is prominently encapsulated in the title of the report, "Security through Cooperation". Two kinds of efforts are required for the protection of the nation and its assets. On the one hand, the report addressed the comprehensive cooperation between all civilian and military assets serving security policy interests. On the other hand, it promoted an enhanced collaboration with international security organisations and like-minded states in order to contribute widely and more actively to stability and peace. It also made a link between economic stability and security policy:

> *"Political, social and economic stability are closely interconnected. Democracy is at risk if the economic and social environment is precarious. In turn the development of a market economy is also at risk in states without adequate provisions and institutions to maintain the rule of law."*[6]

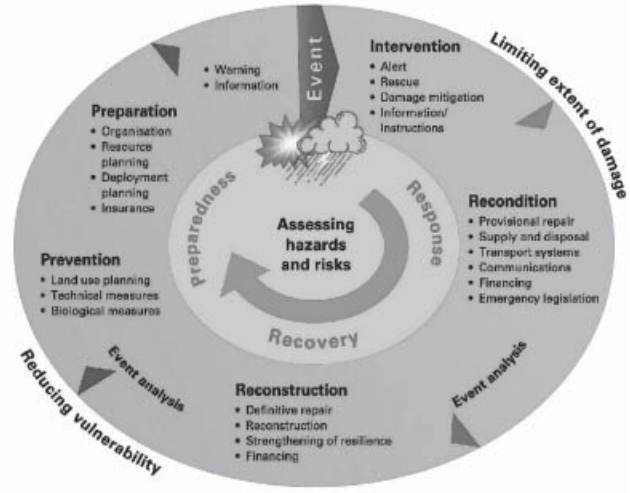
The report clearly stated that it is not possible to prevent all severe events at all times. However, it is possible to reduce the nation's vulnerability, reduce the likelihood of the occurrence of such events, and minimize their consequences. Vulnerability and disaster impact are influenced by many factors. It is therefore necessary to combine methods and knowledge from various academic disciplines and from all relevant sectors of society.

Based on this report and taking into account the experience of the attacks of 11 September 2001, the senior levels the of security services were reformed in 2002. At the very top, the Federal Council's Security

6 Swiss government, *Security through Cooperation*, p. 26.

Committee ("Sicherheitsausschuss", SiA) was established, comprising the heads of the Federal Department of Defence, Civil Protection and Sport (DDPS), the Federal Department of Justice and Police (FDJP), and the Federal Department of Foreign Affairs (FDFA). Its main task is to support the Federal Council in shaping security policy. The Security Steering Group serves as the staff of the SiA and prepares the relevant decisions. The work of these newly founded bodies is supported by the Assessment and Detection Bureau.

In 2003, the newly established Federal Office for Civil Protection (FOCP) within the Federal Department of Defence, Civil Protection and Sport published "Katarisk" – a study of risk assessment from the point of view of civil protection. In the context of the joint civil protection system, it provided risk-oriented and scenario-based planning guidelines for natural and technical disasters and emergencies. However, hazards and risks such as the breakdown of key parts of the information infrastructure, crime, violence below the threshold of war (e.g., terrorism), and armed conflict were not subject of this report. However, it already made the case for a systematic assessment of all risks and particularly highlighted the relevant elements of a comprehensive risk reduction mechanism.



Source: Federal Office for Civil Protection, *Katarisk – Disasters and Emergencies in Switzerland: Risk Assessment From a Civil Protection Perspective* (Berne, 2003), p. 29.

In June 2005, the Federal Council gave the Federal Office for Civil Protection the mandate to coordinate CIP activities at the national level. The FOCP launched an interdepartmental working group to establish a common understanding by clarifying key concepts and identifying critical infrastructure sectors.

In 2005, the Federal Chancellery published the final report of the leadership exercise "Epidemic in Switzerland". During this exercise, special attention was paid to cooperation and coordination among the various federal departments, the definition of responsibilities within the lead organisation, and the level of information and communication that served the leadership process. Furthermore, it was assessed how these elements played out under time pressure, during a crisis situation, and within a federal and international setting. The evaluation stated that short-term crisis management could be considered adequate, but strategic decision-making was mostly absent.

In 2005, the Federal Council abolished the Assessment and Detection Bureau and the position of the intelligence coordinator for the Swiss Confederation as its head. The Bureau was replaced by the staff of the Federal Council's Security Committee, which also took on a supportive role for the Security Committee and Security Steering Group.

On 4 July 2007, the Federal Council approved the first report on Critical Infrastructure Protection (CIP) by the interdepartmental working group headed by the FOCP. The report represents a first major step towards the elaboration of a national CIP strategy for Switzerland. It highlighted threat scenarios ranging from natural and technical hazards to violent and armed conflicts. It further defined the need for future action in the area of CIP.

4 Consequences and future developments

There is no doubt that the importance of risk analysis and management will further increase in the coming years, both nationally and internationally. As the improvement of security is an ongoing process (see figure 2), there is a real necessity to assess the risks and the mechanisms to deal with them on a regular basis. The need for constant assessment has even increased with the rapid change in the security environment. Today, threats are no longer direct (inter-state conflicts), intended, and calculable, as during the Cold War, but asymmetric and indirect, diffuse, and highly uncertain.

At the operational level, under current legislation, the implementation of civil protection measures is primarily a cantonal responsibility. Cantons can use the guidelines of joint, risk-oriented planning and expertise from the federal level to improve their own risk assessment and preparedness. Still more targeted risk assessments will be required for local, regional, and cantonal planning.

On the other hand, there is also much at stake for the federal government. Many key actors are involved, and the FOCP tries to support these endeavours.

In line with the results of the "Katarisk" study, the relevant threat spectrum should be expanded beyond the natural and technical disasters and emergencies and also include hazards and risks such as the breakdown of critical infrastructures, violence below the threshold of war (e.g., terrorism), and armed conflict. This inclusion provides particular methodological challenges that have to be addressed early on in the process. In this regard, research and development, and cooperation with the academia and the private sector in particular, play an important role. By fine-tuning risk-oriented planning, civil protection managers as well as other security-relevant actors at the cantonal and national levels can profit from this effort.

Also, elements of risk management and risk-oriented planning should be integrated in training and education courses. The curriculum of the Master of Advanced Studies in Security Policy and Crisis Management

course at the ETH Zurich plays an important role in this effort, as does the Training Division within the FOCP.

In the context of CIP, national civil protection regulations and plans that come under federal regulation and jurisdiction (e.g., increased radioactivity, nuclear power plant accidents, dam failures, and epidemics) should be re-examined for their risk-orientation.

In conclusion, dialogue is crucial in this regard: dialogue with other security-relevant authorities at various administrative levels, with the private sector, and academia, and, last, but not least, the broader public. This dialogue should also include considerations of risk acceptance/tolerance and striking the right balance between security measures and effectiveness. As the Prussian king Frederick II cautioned in the 18th century, the alternative course may be even more perilous: "In trying to defend everything, he defended nothing."

INTELLIGENCE SERVICES, ARMED FORCES, AND MULTILATERAL INSTITUTIONS

INTELLIGENCE AND EARLY DETECTION OF THREATS IN SWITZERLAND

Matthias Klopfstein

Early detection of acute or potential threats is among the chief tasks of an intelligence service. There are overt threats to a nation and its citizens in the guise of terrorism and extremism; and there are potential, less obvious threats and dangers, for instance, from illegal intelligence activity, criminal organizations, or trafficking in arms and war material. In either case, the challenge is to detect these threats at an early stage and to point them out. The intelligence community continually provides opinion leaders and national political leaders and officials with the essence of the information it has gathered. It is up to these decision-makers to make the most of that information and to integrate intelligence reports in their response planning. The Swiss Federal Service for Analysis and Prevention (SAP) operates on a multilayered intelligence system to evaluate and analyze acute and potential threats to domestic security and to discern potential future threats. Starting from current situation analysis, the threat assessment process gradually evolves to include elements relevant to mid- and long-term threat assessment. Close cooperation with experts at home and abroad allows for findings to be compared and threat analyses consolidated and assessed. Scenario planning helps to discern potential future risks and to work out appropriate responses for preventing or minimizing risks.

1 Introduction

It can prove worthwhile to catch a glimpse of the future. Some rely on horoscopes and fortune-telling to prepare for what tomorrow may hold; others provide professional trend research and future prognostics on behalf of business enterprises and interest groups. The luckier ones occasionally even hit the jackpot.

Trying to see beyond the present is an intrinsic urge of intelligence services. Indeed, in order to properly respond to potential threats and risks, states rely on the expertise and analysis capacity of intelligence services. Overt threats to a state and its citizens may appear in the guise of terrorism and extremism; they are complemented by potential threats and risks from illegal intelligence activities, criminal organizations, or trafficking in arms and war material. In either case, the challenge is to detect, identify, and indicate these threats at an early stage.

Opinion leaders and the political leaders of nations and their authorities are continuously provided with the essence of the information that the intelligence community has gathered. Warnings given by intelligence services usually do not go unheard in these circles; nor are they ignored by the public, for that matter. It is hard to say, however, how political decision-makers perceive such warnings or how these warnings affect their actions.

Intelligence encompasses the areas of risk analysis, risk perception, risk acceptance, and precautions to reduce risk. Among the core tasks of intelligence are early detection and appraisal of the risk posed by terrorist attacks, extremist groups, and criminal organizations. This report thus spotlights these core tasks. Various specific criteria apply in correctly assessing acute and potential future risks emanating, for example, from illegal intelligence activity or trafficking in arms and war material. Other principles apply in protecting critical infrastructure.

This report aims to present the underlying principles of early threat detection from the perspective of those working in the intelligence business. A general introduction is followed by a description of the methods that the Service for Analysis and Prevention (SAP) applies to

fulfill these core tasks and to help ensure domestic security. The SAP – a federal agency within the Federal Office of Police (fedpol) – serves as Switzerland's domestic intelligence service.

2 Fundamental considerations

The SAP is subject to the Federal Act on Measures to Safeguard Internal Security (ISMA),[1] or "Internal Security Act". Article 2 of the ISMA stipulates that the competent federal authorities take timely and appropriate precautions to discern and counter terrorist threats, illegal intelligence activities, violent extremism, and violence at sports events.

The Internal Security Act explicitly states the strategic purpose of early threat detection: The findings are to serve the competent federal and cantonal authorities, which act upon them to take timely action, subject to applicable legal provisions.

Thorough analysis of the capabilities, goals, and mode of operation of terrorist or extremist organizations and individuals is a fundamental element of correctly assessing acute and potential future risks. Terrorist acts are hard to predict, as extremists are largely flexible in determining a point in time in which to strike, or may call off their activities altogether, depending on the window of opportunity. Operation planning must be on schedule and coupled with a high probability of success. Terrorist groups would rather opt to forego an operation than jeopardize it simply by attacking on a predetermined date.

In today's hi-tech society, people are becoming increasingly aware of their individual vulnerability. Indeed, the awareness has grown that internal and external security may be challenged at any time with little or no forewarning. While military conflicts are traditionally preceded by telltale signs of imminent attacks, acts of terrorism usually occur without warning, crippling large parts of civil life. Recently, there has

1 Federal Act of 21 March 1997 on Measures to Safeguard Internal Security, ISMA (Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit, BWIS) <http://www.admin.ch/ch/d/sr/120/a2.html>, accessed 9 August 2007 (German, French, and Italian versions available only).

been a tendency to move away from statistical threat assessment and pragmatic risk management after an emergency has occurred. The trend is rather toward a more down-to-earth awareness of threat.

In judging acute or potential future threats in terms of complex societal risks, potentiality is, unlike in the past, rated second to the vulnerability of the people and the probability of a contingency. In linear technical risks, threat assessment is rather to be understood as the product of the potentiality and the probability of a contingency.

3 Methodology of early threat detection

The SAP operates on a multilayered intelligence system in order to evaluate and analyze acute threats to domestic security and to discern potential future threats. Another pillar of intelligence gathering consists of close cooperation with other federal and state agencies and contacts with foreign partners.

As the agency responsible for day-to-day analysis of domestic security, the National Intelligence Center (NIC) gathers information from both open and confidential sources. All NIC findings are summarized in situation reports, offering comments on the short-term development of the national security situation. In an emergency, NIC assumes a leading role among the national intelligence-gathering organs and collects, evaluates, and disseminates information.

Starting from basic situation reports and drawing on internal and external sources, the SAP drafts analyses that spotlight strategic aspects, with priority given to the mid-term time horizon. Apart from national security, SAP analysis covers all areas of crime investigation for which the federal government is responsible. Thus, the findings from overlapping investigations on organized crime, economic crime, and money laundering are chiefly analyzed based on information supplied by the Federal Criminal Police (FCP).

Addressing specific topics, these analytical reports are provided to prosecution authorities, political bodies, and also to the general public.

The SAP thus contributes to keeping the Federal Council informed on the latest evidence of potentially looming issues relevant to national security.

The Security Steering Group – a political organ – provides the Federal Council Security Committee with situation reports and approaches to security issues. While the Federal Council is the decision-making body on national strategic issues, the cantonal governments are responsible for security in the cantons. The Federal Council, the Council Security Committee, and the Security Steering Group have been assisted by the Staff of the Federal Council Security Committee since October 2005. This staff's function had previously been assumed by the Intelligence Coordinating Unit together with the Assessment and Detection Bureau, which was led by the National Intelligence Coordinator.

The SAP maintains constant contact with numerous other federal agencies dealing with early threat detection. Findings on long-term developments in technology, economy, and society obtained by exchanging information among national and international partners are taken into consideration in drafting situation reports.

4 Scenario planning – a model of supposed events

Scenario planning is a useful strategic method for assessing responses to potential threats without the pressure of a real-life emergency. Simulating and meticulously deliberating a scenario can help the responsible authorities to discern and understand threats. A thorough understanding of a threat is an essential element of counterstrategies and other efforts for safeguarding a nation and its people.

In our efforts to prevent undesired occurrences, we are often challenged by a reality that goes beyond imagination. Scenario planning should therefore include anticipatory-thinking elements that prepare participants for possible unexpected important situations and problems.

More often than not, scenarios – or rather, the people who devise them – lack a certain visionary courage, resulting in tame, uninspired exercises. A number of reasons may account for this restraint in drafting slightly less run-of-the-mill scenarios; for example, scenarists' apprehension that a draft scenario be dismissed as exaggerated or as mere fantasy. But then, different kinds of threats are by no means of equal magnitude, and thus preparation for them requires out-of-the-way approaches.

When devising a scenario, it is advisable to strike a sound balance between options and requirements. It takes a pinch of imagination to evaluate and analyze, for instance, what objects are most at risk or where the most damage and casualties may occur. The much-denounced sand-table exercises are definitely not desirable formats; however, when they are meticulously planned and played out, threat scenarios can help to set priorities and to decide between options in coping with a contingency.

5 Client-oriented early threat detection

The Internal Security Act defines the authorities that the SAP provides information to. As a domestic and police intelligence service, the SAP furnishes information to the federal security organs and to any federal agencies charged, even if only peripherally, with security police tasks. As the entities that are responsible for domestic security on a day-to-day level, the cantons are the major clients for intelligence provided by the SAP.

Only part of the information that the SAP processes is derived from open sources. The SAP therefore relies on information supplied by domestic and foreign partners. Furthermore, the SAP is authorized to inspect official files and documents, and – within the narrow statutory limits accorded to SAP – to collect information on its own.

In some areas that are pertinent to intelligence, the sheer amount of available information makes it inevitable to prioritize and evaluate information by applying strict criteria. All the while, in presenting intelligence to clients, their needs are to be taken into consideration. Most

of the products that the SAP provides are disseminated online through secure communication channels.

6 Where are we today?

Intelligence services assess the impact and the probability of a potential future threat with a view to assisting the political and administrative leaders in taking precautions or responding to an emergency.

Surprising though it may seem, the problem often consists not so much in timely detection of a potential threat to a nation and its people. Rather, it may prove much more challenging to realize that what is perceived as a local threat or a risk to a seemingly limited area of life may have the potential for turning into a major national political and security issue.

No less of a challenge to intelligence services is posed by those domestic circles that indulge themselves in the quite unjustified belief that these services are engaged in some kind of windmill-tilting effort, fighting imaginary foes. A similar attitude is often displayed by bureaucrats who fail to recognize that a threat may very well be real or at least possible, even though it is not readily visible. These quarters often have a hard time both conceptualizing and taking seriously possible future threats. Accordingly, it is all the more difficult for intelligence services to have resources allocated for early threat detection and assessment of potential threats – let alone to adapt the law to render information-gathering and processing easier and to clarify gray areas in the law.

Indeed, catching a glimpse of the future can prove worthwhile. However, given an increasingly interlinked society, the surging flow of readily available information, and the speed at which information is exchanged, the intelligence community faces new challenges every day.

STRATEGIC WARNING FOR CRIMINAL INTELLIGENCE[1]

Daniel R. Morris and Gregory Baudin-O'Hayon

The professional craft of intelligence analysis is continually evolving. Perhaps nowhere has this evolution been more pronounced in recent years than in the domain of law enforcement. There is a growing recognition in the law enforcement community that, to be truly proactive, police must be prepared to act against emerging and future threats. To be proactive, law enforcement must be armed not only with the best current intelligence, but with foresight on the threat environment of tomorrow. In an effort to provide the Canadian law enforcement community with advanced warning of emerging and future threats, the Criminal Intelligence Service of Canada (CISC) embarked on a project in 2004 to develop a Strategic Early Warning System for organised and serious crime (SEWS). Built upon well-established concepts and principles from such sectors as national defence and public health, and adapting methodological practices from the social sciences, the SEWS project seeks to provide guidance and insight through highly focused criminal forecasts. This article provides a conceptual overview of the warning function and outlines a novel approach to strategic warning intelligence.

1 This paper has been adapted with permission from a longer paper produced by the Criminal Intelligence Service of Canada (CISC). The original paper, which includes a detailed description of the strategic warning methodology developed by CISC Central Bureau, is available online at <http://www.cisc.gc.ca>.

1 Introduction

The professional craft of intelligence analysis is continually evolving. Perhaps nowhere has this evolution been more pronounced in recent years than in the domain of law enforcement. The emergence of intelligence-led policing both as an organizational doctrine and as fundamental practice has profoundly altered the way law enforcement agencies must think and operate in the 21st century. There is a growing recognition that the law enforcement community, in order to be truly proactive, must be prepared to act against emerging and future threats – if it waits until a threat becomes fully realized, it will have failed. In order to be proactive, therefore, law enforcement must be armed not only with the best current intelligence, but with foresight on the threat environment of tomorrow. With adequate forewarning of future threats, law enforcement decision-makers are in a better position to develop and implement proactive planning measures, and front-line officers are better equipped to recognize and deal with the earliest indications of a threat's emergence. For both leaders and operators, warning is a tool to help avoid being surprised by their principal adversary: organized crime.

Criminal Intelligence Service Canada (CISC) is a key player in the development and implementation of intelligence-led policing doctrine on a national scale. CISC is a National Police Service comprised of a central bureau in Ottawa and 10 provincial bureaus spanning all provinces. Individually and collectively, all eleven bureaus provide strategic criminal intelligence analysis as one of their core functions. This service is provided to the CISC membership, which consists of the country's police forces and government agencies/departments (federal, provincial, territorial) with a criminal intelligence mandate.

In an effort to provide the Canadian law enforcement community with advanced warning of emerging and future threats, CISC embarked on a project in 2004 to develop a Strategic Early Warning System for organized and serious crime (SEWS). Built upon well-established concepts and principles from such sectors as national defense and public health, and adapting methodological practices from the social sciences, the SEWS project seeks to provide guidance and insight through highly

focused criminal forecasts. This paper provides an overview of the theoretical framework upon which this project was developed, followed by a brief overview of the process by which warning is produced and communicated to the law enforcement community.

2 Surprise and warning

Surprise is an enduring feature of human conflict. The competitive advantage afforded by confounding an adversary as to one's true capabilities and intentions means that there are powerful – if not natural – incentives to confuse, and deceive one's enemy wherever and whenever suitable. This fact alone ultimately explains why intelligence exists as a discipline and a profession – if everyone was always completely forthcoming about their plans, there would be little need for spies, spy satellites, and intelligence analysts. However, by ignoring or misinterpreting the observable indications of our enemies' intentions, we can – and often do – deceive ourselves. The history of strategic military surprise reveals that surprise attacks are rarely ever pure 'bolts from the blue' – in almost every case, there has been a host of warning signals leading up to the attack that, had the defender interpreted them correctly, could have averted or mitigated disaster. In many such cases, surprise was the result of an unwillingness to let go of erroneous strategic preconceptions in the face of the changing tactical situation observed on the ground. Military indications and warning (I&W) analysis is now a well-established component of most professional militaries for this very reason. The events of 11 September 2001 only served to underscore the centrality of the warning function for intelligence. The central premise behind I&W analysis is that events and phenomena do not occur in a vacuum; they affect, and are affected by, various forces and conditions in both the national and international environments, some of which are directly or indirectly observable. These indications, interpreted in a proper context, can help us warn of an emerging or future threat. With strategic warning, appropriate action can be taken to anticipate and deal with a threat before it becomes unmanageable.

2.1 The warning concept and function

It would be appropriate here to define what we mean by warning in this context. Cynthia Grabo, a veteran US Defense Intelligence Agency (DIA) warning analyst (ret.), characterizes warning as "an intangible, a theory, a deduction, a perception, a belief. It is the product of reasoning or of logic, a hypothesis whose validity can neither be confirmed nor refuted until it is too late."[2] Warning should not be confused with facts or information. For instance, to note that the enemy is mobilizing his forces is a fact or a piece of information; to conclude from this and other indications that the enemy intends and is preparing to attack is a warning. Warning is the product of an intelligence judgment on the level of threat and risk posed by a particular enemy or scenario. Most importantly, however, warning must be communicated; an analytical judgment only becomes a warning when it is communicated and understood as such by the receiver. As Grabo points out, "warning that exists only in the mind of the analyst is useless."[3]

We can distinguish warning analysis from other forms of intelligence analysis by its scope, principal client, and function. In terms of scope, strategic warning is principally focused on the future. In contrast to basic intelligence or current intelligence, each of which seeks to accurately describe past and present realities, warning intelligence is speculative and forward-looking, aiming to characterize a future threat. Although strategic warning analysis is a type of estimative intelligence, I&W is unique in terms of the scope of the question it seeks to address. Whereas estimative intelligence seeks to broadly address the question of a threat's future or that of the threat environment, strategic warning analysis is concerned with answering a highly specific question about the nature of a particular threat: for instance, "Does country *x* have the intention and capability to attack country *y*?" In contrast to most intelligence problems, warning questions can often be answered with a qualified "yes" or "no" answer: It is possible to state unequivocally whether or not there is cause for alarm. This narrow, forward-looking focus makes strategic

2 Cynthia M. Grabo, *Anticipating Surprise: Analysis for Strategic Warning* (Washington, D.C.: Joint Military Intelligence College, 2002), p. 4.

3 Ibid., p. 14.

warning intelligence particularly suited for consumption by senior decision- and policy-makers. Thus, whereas basic and current intelligence are primarily geared towards an operational support function, strategic warning is more tailored to those in a position to direct operational resources on a strategic level.

Intelligence scopes and foci:
Basic, current, estimative, and warning intelligence

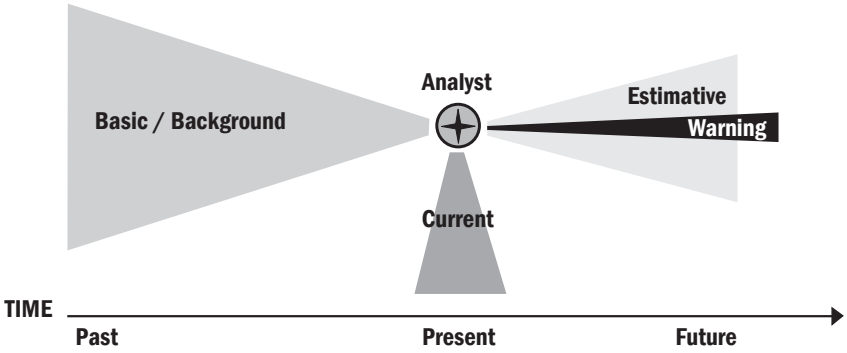


Figure 1: Contrasting four types of intelligence

The strategic warning function serves a straightforward, but vital purpose: to avert *strategic surprise* – a condition caused when a defense system has failed due to a misconception surrounding *the nature* of a particular enemy or threat. This can be distinguished from tactical surprise, which stems more from a failure to anticipate specific operational realities rather than broader strategic capabilities and intentions. For instance, being attacked by a supposed ally would be a case of strategic surprise – the nature of the enemy was drastically misunderstood. On the other hand, to err in the presumed timing of an anticipated attack would constitute a tactical surprise – the enemy was appropriately understood, but the operational attack details were not. Strategic surprise can be averted or mitigated by providing leaders with timely and convincing warning of an enemy's intention and capacity to threaten the nation's security interests. Without the broader threat context illuminated by strategic warning, tactical warning

capabilities are severely handicapped, rendering national defenses more or less blind up until the last minute.

2.2 Indicators, indications and warning

I&W analysis is inherently paranoid; more than any other type of intelligence analysis, it operates on the presumption of surprise, and is intrinsically suspicious of widely held beliefs and assumptions about the enemy. This is for good reason: the history of strategic surprise teaches us that unchallenged bias is the dark side of overwhelming consensus; when a prevailing opinion becomes so accepted and unchallenged that it is equated with "common sense", the risk of strategic surprise is at its zenith. I&W analysis consciously avoids hegemonic thinking by focusing on the hypothetical; instead of starting with the question, "What is likely to happen with *x*?", I&W begins with the hypothetical question, "If country *x* was planning to attack, what behaviors and conditions would we expect to see?" The starting point for analysis therefore does not overly rely on a presumption on the likelihood of an occurrence — if it did, many inquiries would never move beyond this point because of the impact of preconceptions and cognitive pathologies on threat perceptions. Instead, it begins with the presumption that a threat potential exists in order to develop an *indicator list*, which becomes a key mechanism by which we evaluate a threat potential.

Indicators are just what their name implies: conditions that, if observed, could be indicative of a threat's emergence or its potential to emerge. Major military operations, for instance, often present a host of indicators that could provide a window to intent. Individually, an indicator may seem quite benign and insignificant, or possibly indicative of any number of possible scenarios. However, when a range of indicators are taken together, ambiguity is reduced and a clearer picture begins to form as to what the enemy might be up to. Specific indicators, then, are always developed and interpreted as parts of a whole: the complete indicator list. Military I&W units maintain indicator lists for a wide range of possible scenarios, and are continuously scanning the global environment for possible *indications* (observed indicators) of a threat. Indicator lists are the product of an in-depth research effort and, ideally,

produced by – or in consultation with – experts in the relevant subjects or regions concerned. The task of the warning analyst is to incorporate an understanding of the enemy's culture, history, and politico-military doctrines into his/her interpretation of the indications and the broader geopolitical context. If a threat is perceived, the warning mechanism is activated and the relevant commanders and political leaders are alerted.

2.3 Adapting I&W analysis for criminal intelligence

Adapting practices and principles developed for the military for use in criminal intelligence first requires us to address and reconcile the important differences between the two domains as they relate to the warning mission. Most of the differences stem from the contrasting natures of their adversaries. Military I&W analysis was designed to help anticipate the moves of a known state adversary. The nation state – with fixed map coordinates, national economy and infrastructure, and clear political and military leadership structures – presents a stunning contrast to the fluid, mobile, and networked entities that make up much organized crime. Unlike most nations, many organized crime groups have neither coherent strategic vision nor established doctrine that could assist an outsider in anticipating their moves. In some cases, then, we may be faced with the task of warning of potential future threats that the organized crime groups themselves may not have yet fully considered. Moreover, in many cases, the strategic threats that concern criminal intelligence are not specific entities at all, but rather criminal *phenomena*, such as new criminal applications of technology, or the expansion of an illicit commodity. As a result, warning analysis for criminal intelligence must contend with a far greater number of variables and a conceivably limitless array of possible outcomes.

Unlike I&W analysis in other domains, where the outcome variables (such as state failure, nuclear missile launch, or global flu pandemic) are clearly defined, the number of possible outcomes in the criminal domain is virtually unlimited. While we may mitigate this problem by restricting our assessments to analyzing a specific threat scenario (that is, clearly outlining the outcome variable in question), the outcome we are trying to forecast is, nevertheless, formulated on a case-by-case

basis. This significantly complicates the warning mission for criminal intelligence. Instead of starting with a known potential outcome and then employing a methodology to forecast and anticipate that outcome, we are, in a sense, left wandering in the dark, constantly looking for the "unknown unknown" – the potential threat that we have not even contemplated, let alone identified. This invariably means that the practice of providing strategic warning for criminal intelligence becomes more *ad hoc* in nature, and its topic selection more analyst-driven as opposed to outcome-driven. This does not negate the value of this work to the intelligence community, but it does limit the degree to which we can identify and warn of all potential strategic threats.

Notwithstanding these and other differences and difficulties, the principal aim and method of military indications and warning analysis has been successfully adapted for use in other domains, most notably in the public health and corporate sectors. Regardless of whether the issue in question is the potential for a military invasion, an influenza pandemic, a hostile corporate takeover, or the emergence of a new criminal market, the central premise behind I&W analysis holds true: that crisis situations are often the culmination of a series of events and conditions, some of which will generate detectable signals or warning indications that, if correctly pieced together, can portend the coming calamity. A feasibility study conducted by CISC in 2004 demonstrated that this premise is applicable to events and conditions in the criminal underworld. This study, carried out in collaboration with researchers from the Centre for Security and Defence Studies at Carleton University, sought to understand the apparent intelligence failure surrounding the unexpected arrival and establishment of Russian organized crime in the West in the 1990s. The study concluded that observable and potentially predictable linkages do exist between domestic and international indicators on the one hand, and criminal activity in Canada and abroad on the other. In other words, this particular intelligence failure was not inevitable; a sound I&W approach could conceivably have led to early warning and response.

3 Strategic warning methodology

The process for the development of warning intelligence mirrors the traditional intelligence cycle with one key exception: its inception. The traditional cycle begins with a managerial or executive directive informed by what the intelligence decision-making echelon determines are its priorities. For instance, the process for developing an intelligence assessment on the *Hells Angels* motorcycle club would normally begin at the planning and direction stage, where decision-makers would task intelligence officers and analysts with the project based on a decision that Outlaw Motorcycle Gangs (OMGs) are an intelligence priority. Planning and direction is therefore a critical stage in the traditional intelligence cycle, as it ensures that intelligence resources are best utilized to address higher priority threats. This stage, however, assumes a significantly different form and function in the warning process. In contrast to a focus on known threats, strategic warning is, by definition, concerned with the unknown or unexpected dangers over the horizon – that is, that which has *not* yet been deemed a priority issue, or perhaps even contemplated by the law enforcement community. Warning analysis does not have the benefit of knowing one's enemy, but is rather confronted with an array of possible enemies limited, in theory, only by the informed intuition of the individual analyst.

Given that a warning assessment will rarely be initiated by a top-down directive, a threat identification and selection mechanism must be built directly into the process. Thus, strategic warning is a case of bottom-up intelligence – the process is initiated by the analysts, and the finished intelligence is moved upward to senior decision-makers. Rather than beginning with a known target, CISC's SEWS process begins with the search for a target. This will usually take the form of an environmental scan – a continuous process of monitoring various open- and closed-source data streams. This broad scan is virtually boundless in the scope and depth of possible coverage; the analyst must cast an exceptionally wide collection net and, consequently, must sift through a significant amount of information, the vast majority of which will not

be directly relevant to any eventual product. Some of the key sources of information consulted during the environmental scan include: foreign broadcast media; domestic news; grey literature; academic periodicals; other intelligence assessments; closed-source databases; internet websites; on-line discussion forums and web-logs; environmental scans prepared by different agencies; and, importantly, other analysts and investigators.

The environmental scan often gleans possible threat issues for consideration. In the process developed by CISC, once potential topics have been identified and selected through a collaborative review process, they are added to the *Sentinel WatchList*, where they then undergo further research and analysis. Throughout this scan, SEWS analysts are specifically – though not exclusively – looking for what is new or unusual. The key questions being addressed for each possible threat scenario are: 1) What is the likelihood that the scenario will occur, and what is its estimated timeframe? 2) What impact could be felt if the threat scenario were to occur?

When the assessments of likelihood and impact potential are adequately addressed, a decision can be made as to whether or not warning is necessary. If not, the issue remains on the *WatchList* for continued monitoring and re-evaluation. If warning is deemed necessary, the topic enters the *Sentinel Assessment* stage, which produces the primary mechanism resulting in the delivery of a warning judgment to the intelligence consumer. Throughout the entire cycle, the environmental scanning process never ceases, and threat scenarios are regularly revisited to evaluate whether an important change has occurred that might require the issuance of a new or revised warning. In some cases, further research on an issue may reveal that, while no warning is necessary, there is a need for a dedicated assessment on the topic. In such cases, the issue may, for instance, instead be developed into an intelligence brief or a more comprehensive threat assessment.

The flow chart below illustrates the SEWS process through the three broad stages, from threat perception to evaluation and monitoring and

to assessment and warning.[4] As the chart depicts, the law enforcement community is not simply the end-point of this process, but also feeds into both the threat perception and the WatchList stages. This reflects the important role played by members of the law enforcement community in offering insight into new possible future threat scenarios, as well as supplying much of the indicator data (indications) for existing WatchList and Sentinel topics.

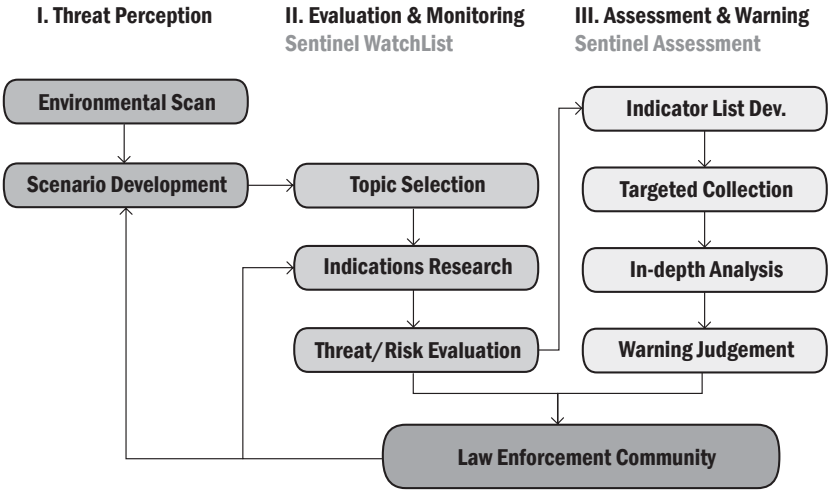


Figure 2: Overview of CISC's approach to strategic warning intelligence

As discussed above, the two principal analytical products in the SEWS process are the *Sentinel WatchList* and the *Sentinel Assessment*. The *WatchList* functions as both an analytical tool and an early-warning reporting mechanism. In the former function, the *WatchList* serves as a topic clearinghouse

4 A parallel can be drawn here between our three-stage SEW process and the "scan, monitor, forecast" model employed by the well-established Los Angeles Terrorism Early Warning (TEW) Group. The TEW Group pioneered the adoption of indications and warning methodology for the law enforcement counter-terrorism domain, and has been successful in developing a network of fusion centres to facilitate the sharing of information and intelligence on terrorist threats. We would like to acknowledge the important contribution of the TEW Group's co-founder, Lt. John P. Sullivan, who has been an instrumental collaborator throughout the development of the SEWS project.

for *Sentinel Assessment*s, allowing the warning analyst to record and observe changes over time for a range of possible threat issues, thereby making it easier to see when a particular topic meets the threshold for a *Sentinel Assessment*. The *WatchList* is also a mechanism for promoting awareness and stimulating the sharing of intelligence and ideas on different threat issues that may otherwise evade the attention of the law enforcement community. The *WatchList* ensures wide exposure to potential threat scenarios that may lack sufficient research development to be the subject of a full assessment. In so doing, the *WatchList* acts as an incubator where information and understanding on potential threats can grow and develop. It should be emphasized that the *WatchList* is not intended as a means of identifying new law enforcement priorities — its function does not go beyond the promotion of awareness and discussion of potential emerging and future threats.

The *Sentinel Assessment* constitutes the primary mechanism by which warning of an emerging or future threat is communicated to the law enforcement community. The *Sentinel Assessment* is designed to provide in-depth and focused research, relevant tactical information, and clear strategic judgments in a concise and accessible format for senior law enforcement officials. The principal goal of the *Sentinel Assessment* is to raise awareness of a potential threat in order to avert strategic surprise and to facilitate more informed decision-making. It is also hoped that the release of a *Sentinel Assessment* will generate discussion within the law enforcement community, promote intelligence sharing on the topic, and raise situational awareness among the eyes and ears of the intelligence community.

3.1 Communicating warning

"It is an axiom of warning," notes Grabo, "that warning does not exist until it has been conveyed to the policy-maker, and that he must know that he has been warned." The analyst "must find the means to convey what he believes to those who need to know it."[5] Unlike the vast majority of criminal intelligence in Canada, which is geared predominantly towards operational support, strategic warning intelligence is specifically tailored for senior law enforcement decision- and policy-makers. As such, there are important considerations with regards to the principles and methods of reporting for warning intelligence.

Though senior decision- and policy-makers constitute the primary intended audience for strategic warning intelligence, the products are not limited solely to the executive echelon. Intelligence officers and analysts are important secondary consumers of CISC warning intelligence. These intelligence practitioners are key partners in the production of strategic warning intelligence and are well-placed to identify emerging threats and to detect subtle changes in local threat conditions. Additionally, front-line investigators constitute the third level of warning intelligence consumer. While the appeal and perceived usefulness of these products to the investigator is more limited, these front-line officers are nevertheless vital to the strategic warning process, as they are often both the first to identify the earliest indications of an emerging threat, and also those primarily responsible with dealing with a threat once it emerges. The goal with this latter audience is less to aid in decision-making than to facilitate situational awareness. It is hoped that by simply scanning the assessment, the officer will internalize the warning so that, when later confronted with new indications, the member will be able to recognize them as such and take whatever action is deemed most appropriate (ideally, sharing this information with the intelligence community).

Strategic warning intelligence is intended to alert decision- and policy-makers to an approaching threat so that appropriate action can be taken to avert it or at least mitigate its negative impact. The clarity of

5 Grabo, p. 14.

the warning judgment in a *Sentinel Assessment* is therefore of paramount importance. Each *Sentinel Assessment* sets out to address a single warning problem, which can be expressed as a specific question with an equally specific answer on the potential for a threat scenario to be realized; fence-sitting on threat issues is not a luxury that the warning analyst can afford. The *Sentinel* is therefore designed in such a way that the consumer, after reading the warning notification on the cover page, should know what the analysts believe is most likely to occur with respect to a particular threat issue. This judgment is restated and further qualified at the end of the document to ensure that the warning has been clearly communicated. The remainder of the *Sentinel* is intended to provide the context and rationale for this warning judgment, and what this possibly means to the law enforcement decision-maker, in a concise, practical, and intuitive format. An upper limit of eight pages ensures that each *Sentinel* can be read in less than 10 minutes. Color-coded scales are one means to convey meaning quickly and intuitively while reducing the amount of text needed. Lastly, the use of both print and electronic versions of the *Sentinel* products balances ease of distribution with the need to accommodate a preference among some senior officials for hard copies.

4 Lessons learned and future developments

The construction of a strategic early-warning system for organized and serious crime in Canada has gone through a number of phases, the first being a feasibility test, followed by methodology and product-line development. The next steps include a drive to demonstrate and teach the methodology developed by the Central Bureau to CISC member agencies, and the development of a national warning system. The latter refers to a series of policies and procedures that would allow the CISC community to serve the warning function effectively on a national level. Such a system should: facilitate the horizontal and vertical flow of information in an appropriate time frame; insure the quality of the products issued; and make

warning an essential feature and standard practice in all law enforcement intelligence units.

Reflecting on what we have learned through the development of SEWS, the single most important challenge has been and continues to be an analytical one, given that we are dealing with hypothetical futures, as opposed to empirically proven pasts. This is compounded by the problem that the traditional emphasis in most intelligence agencies has been on collection rather than analysis. Therefore, the role of analysis must be brought to the forefront, while at the same time keeping in mind that not all analysts are equally at ease with warning analysis, as many of them are either incapable or unwilling to draw conclusions and put forth judgments on the basis of analysis and not on facts alone. Though common practice in academe, this is a radical shift for many in the intelligence analysis profession, showing that although warning is a key part of the intelligence function, it is ultimately a different type of analysis. Consequently, it requires a different approach and way of thinking, as well as a different skill set; indeed, not all analysts are well-suited for strategic warning. Hiring or assigning the right people for the task is therefore critical when developing a strategic warning capacity.

Another general challenge has been the packaging and dissemination of the warning analysis. In terms of packaging, what is most important is to know one's audience. Often, intelligence analysts write assessments as if the primary audience were made up of other analysts, as opposed to providing decision-/action-oriented reports. This is why a conscious decision was made to issue *Sentinel* assessments and *Watchlists* that could be read less than 10 minutes with the aid of intuitively understood color codes. In terms of dissemination, the eternal struggle for intelligence agencies has been that of security classifications. CISC Central Bureau decided to seek the lowest classification level possible in its warning assessments in order to facilitate the broadest possible dissemination to the Canadian and international law enforcement community. This can be a difficult task, given that we utilize an indications and warning methodology that uses discrete indicators from tactical information. The

challenge is to capture the essence of that information without revealing names, sources, or methods.

Lastly, there is the paradox of buy-in. The paradox is that we needed community support for the project to work, but we needed the project to work in order to obtain community support. We were able to overcome this challenge by appealing first to the senior decision-makers with assessments that we knew would be salient to them and their organizations. Their positive response was leveraged to build greater credibility with the mid-level managers, who were then more inclined to help us get the information we needed to make better assessments. At the same time, we made a conscious effort increasingly to bring frontline officers into the process by going out to interview them. Thus, getting around the problem of securing buy-in involved much relationship-building and listening.

5 Conclusion

In our context, a warning is a hypothesis that is informed by reasoning, knowledge, and – critically – by piecing together and analyzing the indications of a potential threat. Strategic warning analysis is a systematized method for developing and issuing sound warnings to those who need them, when they need them. While strategic warning analysis is not a modern innovation, its application within the criminal intelligence community is a recent development. Although relatively new to the law enforcement domain, strategic warning analysis is neither a departure from established analytical practices, nor is it divorced from the broader intelligence cycle. It is, rather, a method of analysis that is uniquely focused on the future threat environment and specifically tailored to meet the needs of law enforcement decision and policy-makers. As such, a different approach is required than the one used to produce assessments of the past or present. In this paper, we have outlined one such approach that is currently being employed by the Criminal Intelligence Service of Canada.

FUTURE ANALYSIS AS AN INSTRUMENT OF STRATEGIC PLANNING

Roland Kaestner

This article shows how future analysis can be used to shape the conceptual planning of the German armed forces. In general, future analysis offers a broad methodological toolbox that can be roughly subdivided into three groups: inductive methods, explorative approaches, and normative prediction. These methods are also used by many other scientific disciplines. This article portrays the methodological approaches of trend analysis and – to some extent – of scenario development. A risk analysis for the security policy environment, based on these foundations, can reveal the capabilities that the German armed forces will require for a very long-term time span (e.g., until 2030 or 2035) in order to meet its mission goals. The methodological approach described in this article allows verification of statements about the future and confirmation of events by way of documentation. It also offers a foundation for systematic further methodological development.

1 Issues

In security political terms, the East-West conflict was a period of stasis. The military forces of both sides were geared towards their respective opponents, mutually setting the pace of developments. The arms race had a qualitative and quantitative dimension, although 30-year planning horizons were the rule for the complex systems of political bureaucracies, arms industries, and military apparatuses on both sides. A stabilizing factor was the aim of maintaining the fragile balance of power, which helped to prevent a war between the two camps. No single advantage in the field of armaments was able to counterbalance the consequences of escalation to full-blown nuclear conflict.

The results of the economic globalization process, which helped put an end to this conflict of hegemonies and political systems, have also changed the framework of the international order. They are creating new security challenges at the local, regional, and global levels that affect the countries of the West not just politically, but also in economic and social terms. These changes also entail far-reaching outcomes for the armed forces in post-industrialized societies.

The adage that in current conflicts, military commanders are always fighting the last war over again points to a fundamental problem in planning for armed forces: How can one plan appropriately to build armed forces for future conflicts against the background of decision-making processes that are based on long-term planning?

The method employed so far, which is based on continuously adopting the armed forces to current military conflicts, assumes that the face of war changes only gradually, and that these changes do not cause the prospects of success to deteriorate fundamentally. There are two basic reasons why these assumptions are only partially appropriate today: The first is the complexity of post-industrial force structures, as well as of the global framework in which they must prove their mettle. The second, related reason is the speed and extent of the transformation we are currently experiencing. Therefore, planning for complex systems such as armed forces must anticipate the future sufficiently in order to avoid ending up in developmental dead ends years later when the

outcomes of planning are actualized. However, this can no longer be guaranteed by conventional approaches to planning, which must therefore be complemented by new approaches.

In view of these factors, the Office of Studies and Exercises, as it was known then (today: Transformation Center), was tasked by the Deputy Inspector General of the Bundeswehr in 1998 with a study investigating the "Armed Forces, Capacities, and Technology in the 21st Century". The underlying assumption was that a targeted conceptual development of Germany's armed forces demanded that mission-relevant challenges, technological developments, and interdependencies be identified in a timely manner and that the appropriate conclusions be drawn for building force capacities over a 30-year period.

The results of this research are to serve the further development of conceptual planning for the Bundeswehr in order to avoid misinvestments or shortcomings of equipment and to create maximum security for long-term planning of Germany's armed forces. The intention was to initiate a systematic, strategic analysis of future developments that would allow the early identification of security- and force-relevant potential for change and to draw appropriate conclusions for long-term force planning taking into account risk management approaches.

After the presentation of the SFT 21 2030 study in 2002, the decision was made to create an institutionalized element of continual "strategic future analysis". This was done taking into account the insight gained by the first study,[1] according to which future analysis could not be accomplished through occasional studies. Instead, it was acknowledged that unawareness, uncertainty, and suspected errors necessitate an ongoing process of verification of insights as well as their further development with respect to an uncertain future. Furthermore, the methodological

1 Cf. Amt für Studien und Übungen der Bundeswehr, *Streitkräfte, Fähigkeiten und Technologie im 21. Jahrhundert*, SFT 21 2030 (Waldbröl, 2002), part I, chapter 1.1: "It makes sense to establish strategic future planning as a discipline in the armed forces and in political science departments of academic institutions, especially in the field of international relations, and to further develop the subject methodically and topically."

basis derived from the economic sphere[2] was promising, but required further specification with regard to its applicability for the field of security and defense policy.

The goal of the subsequent SFT 21 "Strategic future analysis" 2005 (SFT 21 2035) was therefore to continue the continual process of strategic future analysis begun with the SFT 21 2030 study in methodological and topical terms in order to derive an ongoing instrument of innovation with respect to the conceptualization of Germany's armed forces. The conceptualization of the Bundeswehr describes long-term goals from which guidelines can be derived for the next steps in current force planning. Against the background of a continuing future analysis, to be presented every five years (the next being due in 2010 and relating to the period until 2040), the armed forces' planning staff is tasked by the inspector general with investigating how the goals of the Bundeswehr conceptualization should be adapted in the light of the analysis and its recommendations, and which recommendations require further investigations in additional studies. Future analysis is therefore an instrument of the main planning process, which serves the subordinate process of targeted conceptualization.

2 Methodology of future analysis in the German armed forces

Strategic future analysis applies academic insights to consultancy for decision-makers in the political and military fields as well as the arms industry. The analytical process is based on the exploitation of scientific methods; however, part of the analysis also builds on the creativity and experience of internal and external participants in the research process.

The results of strategic future analysis are intended to offer early indications of options and alternatives, and thus to provide decision-makers with ways of shaping the future in terms of force capabilities. They are not intended to pre-empt decisions. The goal of improving

2 Cf. Alexander Fink and Andreas Siebe, *Handbuch Zukunftsmanagement: Werkzeuge der strategischen Planung und Früherkennung* (Frankfurt am Main: Campus Verlag, 2006).

long-term planning for the armed forces can only be reached if the armed forces are understood as being shaped by the role they are to play at the international level as well as by the attendant social framework. The research underlying these results must therefore take into account more than simply the search for efficient military options in waging war. The fundamental assumption is that warfare and instruments for waging war – i.e., armed forces or other forms of organized violence – reflect the attendant social framework.

The unfamiliar concept of "strategic future analysis" leads us to the question of what we can know about the future. This article assumes that there is no authority in the social sciences – as opposed to the natural sciences – that is able to predict future events based on generally applicable laws. In this sense, empirical trends as generally employed in the social sciences cannot replace generally applicable laws. According to Popper, the shortcomings of sociological prognoses are generally due to the complexity of social developments, their interdependency, and the qualitative nature of sociological terminology.[3]

Purely as a matter of principle, it will never be possible to predict social events with the same degree of accuracy as is possible in the natural sciences, such as in Newtonian physics. Since we are part of the social developments, and furthermore are able to and intend to influence future developments by virtue of our predictions, it is impossible to make accurate and detailed scientific statements in the social field relating to individual events.[4] The future is open, and all participating actors have a hand in shaping it. But the future is determined by the laws, frameworks, and possibilities of cosmological and biological evolution as well as of the process of civilization. The differentiation of these processes makes new developments conceivable, but none of these processes is able to go against the laws and framework of the three abovementioned evolutionary processes. This means that only a finite number of future scenarios can occur, since not everything is possible. Even if individual events cannot be predicted, it is possible to analyze

3 Karl R. Popper, *Das Elend des Historizismus*, 5th ed. (Tübingen: Mohr, 1979), p. 30.

4 Ibid., p. 11.

trends to describe sample spaces that allow the observer to reduce risks relating to the planning process. If we regard them as possible futures, we can identify directions, indicate courses of action, and subsequently may even investigate why certain developments followed a course that was contrary to our expectations. This allows us to deal with such social prognoses methodologically and conceptually.

Collective human behavior can, if it is repeated in stable patterns, be summarized as trends. These are identifiable courses of developments that are generated based on the analysis and the experience of previous events and continue across time. They allow predictions to be made about an unknown and uncertain future environment that is discrete in temporal, spatial, and topical terms and can be used to describe possible future sample spaces and structures. They do not relate to individual events, but are statistic in nature. Furthermore, they are an instrument for reducing complexity[5] that relates relevant circumstances to events in an explanatory manner. Trends can thus be used to reduce the complexity of the world to a few essential traits. The evaluation of a large corpus of literature dealing with security policy issues has, however, generated a great number of trends and statements about them – which prima facie contravenes the goal of reducing complexity – and these results, which were retrieved in a disordered manner in terms of quality and quantity, then had to be structured and ordered according to a specific hierarchy in order to be useful for deriving conclusions as well as for eliciting mutual effects between the trend statements. As a rule, this is achieved both in academia and in practical application by constructing models,[6] theorems, or, where assured knowledge is available, theories.

5 Niklas Luhmann, *Vertrauen – ein Mechanismus der Reduktion sozialer Komplexität* (Stuttgart: Enke, 1968).

6 For the use of models, cf. Herfried Münkler, 'Modelle im politisch-militärischen Bereich', *Debatte*, 2: Modelle des Denkens: Streitgespräch in der Wissenschaftlichen Sitzung der Versammlung der Berlin-Brandenburgischen Akademie der Wissenschaften am 12. Dezember 2003 (2005), pp. 75–80, at p. 75: "Ihre Funktion besteht im Wesentlichen darin, die Fülle der für Entscheidungen notwendigen Informationen zu reduzieren und gleichzeitig Präferenzen für bestimmte Optionen aufzubauen. Sie sind also die Antwort auf ein Problem, das von Wolf Singer kürzlich als das der Planbarkeits- und Beherrschbarkeitsdefizite von Systemen aufgrund der nichtlinearen Dynamik lebensweltlicher Prozesse und der begrenzten kognitiven Fähigkeiten der Steuernden bezeichnet worden ist."

One such model that can be used to link trends is the aforementioned process of civilization. The literature about this process fills entire libraries and can be traced back to Adam Smith and Immanuel Kant. In the following, we refer to the description of this phenomenon by Norbert Elias in his work "The Civilizing Process".[7] He defines it as

> *"Plans and actions, the emotional and rational impulses of individual people, constantly interweave in a friendly or hostile way. This basic tissue resulting from many single plans and actions of men can give rise to changes and patterns that no individual person has planned or created. From this interdependence of people arises an order sui generis, an order more compelling and stronger than the will and reason of the individual people composing it."*[8]

This process of civilization changes the behavior and perception of people in a specific direction. At its core, this process relates to the conscious or subconscious organization of a deepening or dissolving form of cooperative egotism, the driving power of human action.

The development of civilization as outlined above occurs in a reciprocal process. No final goal is discernible, save that the process of civilization facilitates the securing of the needs and interests of an increasing number of people at ever-increasing standards. This is based on the emergence of increasingly complex social, economic, and political entities. Globalization has imparted a new quality to the process.[9] The process has a clear direction. However, the egotistical behavior of individual actors means that we can also conceive of phases in which the process is reversed or in stagnation due to the dissolution or reshaping of existing interdependence; furthermore, its speed may change. This is expressed in trends and countertrends.

7 Norbert Elias, *The Civilizing Process* (Oxford: Blackwell, 2000).

8 Ibid., p. 366.

9 Cf. Schlussbericht der Enquete-Kommission der Bundesregierung, *Globalisierung der Weltwirtschaft: Herausforderungen und Antworten*, BT-Drs. 14/9200 (12 June 2002).

In this sense, the instrument of strategic future analysis examines a broad spectrum of trends with a view to their relevance to security and the armed forces, which are derived in the academic research from a broad variety of disciplines or other sources and fields of knowledge application. The model of the "civilization process"[10] is used to weight these trends and to structure them in trend fields.[11] This approach is based on a subdivision into the following seven trend fields that encompass all trends and trend statements:

- Demographic development
- Development of resources and environment
- Development of science and technology
- Cultural development
- Social development
- Economic development
- Political development

These result in an analysis of how individual trends as well as a network of effects affect the security-relevant environment and the future face of war. The security-relevant environment in this context is equivalent to the sum of all developed scenarios.

The analyses are structured geographically and topically. In the geographical category, selected local actors identified as relevant to security policy (political entities), regional developments, and a global analysis of the seven trend fields are selected and described. Topical processes that defy clear geographical classification can be investigated separately for their relevance in terms of future developments by applying the same pattern. Examples include the topical areas of "organized crime" or "climate change".

10 Cf. SFT 21, part III, chapters 1.3.3 and 1.3.4.

11 Ibid., chapters 2 and 2.1ff.

The results generated in the trend analysis are translated into security policy scenarios and describe a fictitious future security-relevant environment that goes beyond the Bundeswehr's planning horizon (ca. 15 years). Some of these trends are long-term ones (such as demographical trends); in such areas, abrupt changes are unlikely to occur. Others may have a shorter-term applicability and may change within relatively short time if new trends are introduced. This is particularly true for complex trends (e.g., globalization), which are therefore more difficult to assess. The triggers for change in such trends can be regarded as indicators allowing early identification of change from one scenario to another. Furthermore, insight about the correlations and interdependencies between various trends is scarce and unsystematic. These deficits can only be removed through long-term empirical investigations. The permanent observation of complex trendsetting factors and their effects that determine specific developments is an important precondition in this connection. Therefore, strategic future analysis must also have the character of a continuous process.

Trends and underlying explanatory patterns and models are extrapolated from scientific publications derived from various disciplines, data collections, and studies of national and international institutions as well as other publications. They constitute an inexhaustible reservoir for strategic future analysis at very different levels of abstraction and with highly differentiated possibilities of reducing complexity as proposed by Luhmann.[12]

The fundamental aim of trend analysis is to represent the basic directions of developments relevant to security policy (trends) as a basis for further analysis.

12 Cf. Luhmann, *Vertrauen*.

Results derived so far in trend research are evaluated and bundled in the seven trend fields.[13] Initially, the drivers of the process of civilization in the trend fields of demographic trends, resource and environment development, science and technology development, and cultural development are described. Subsequently, the major trends that determine the overall process of civilization are described in the trend fields of economic development, social development, and political development. Then, the phenomena to be expected in future forms of armed conflict are outlined in fundamental terms. The salient trend statements are summarized, and initial conclusions for the nature of risk potential in the 21st century as well as implications for security are derived from them. Thus, the Bundeswehr's strategic future analysis is conducted as a continuous process in three broad steps: Permanent trend analysis; its translation into scenarios that add up to a description of the security-relevant environment for the respective timeframe (until 2030 or 2035, etc.) and constitute the basis for the main transformation potential relating to security and the armed forces, resulting in a trend field of "the future face of war"; and as a third step, the identification and investigation of options for future important capabilities using methods of risk analysis and risk management, resulting in recommendations for action.

Timely political decisions on the development of the armed forces require improved communication between security-policy elites and the society that supports them. A discussion on future questions that is based on political impetus, scientific foundations, and broad public support can contribute to such communication. These are essential elements for evoking an understanding of one's own political goals in the

13 To this end, SFT 21 uses individual studies such as Ingomar Hauchler, Dirk Messner, and Franz Nuscheler (eds.), *Globale Trends 2002: Fakten Analysen Prognosen* (Frankfurt am Main: Fischer Taschenbuch Verlag, 2001); National Intelligence Council NIC 2000–02, *Global Trends 2015: A Dialogue About the Future with Nongovernment Experts* (Pittsburgh: NIC, 2000); as well as metastudies (i.e., studies on studies) such as: Sam J. Tangredi, *All Possible Wars? Toward a Consensus View of the Future Security Environment, 2001–2025*, McNair Paper 23 (Washington, D.C.: Institute for National Strategic Studies, November 2000), or Simon Davies, Ben Bolland, Kirsty Fisk, and Mike Purvis, *Strategic Futures Thinking: Meta-analysis of Published Material on Drivers and Trends*, DERA/DSTL/CR00979/2.0 (Farnborough, UK: Defence Evaluation and Research Agency, 2001).

course of bilateral and international academic discourse. An independent contribution to the international debate, which so far is dominated by Anglo-Saxon approaches, would also strengthen the German influence, particularly with important partners and international organizations.[14] Global corporate actors are open for such an approach, as they increasingly realize the extent to which the success of their business ventures depends on an environment that is free of violence and where the law is enforced.

The Bundeswehr's strategic future analysis indicates courses of action for long-term force planning. Planning issues depend largely on the challenges to be taken on, and on the reaction patterns to be deployed against them. These conditional factors generate the political goals that the armed forces in conjunction with other security policy instruments strive to achieve.

Trends are translated into scenarios to generate a security-policy environment as a basis for analyses.

3 Developing scenarios

Scenario technique is a way of limiting insecurity. This approach requires a multi-track approach: Futurologists develop multiple, but equally plausible possibilities of what could happen, and analyze possible outcomes of these various scenarios. In this context, the future and its interpretation are regarded as consisting of a finite number of different development vectors. In this way, highly disparate blueprints for the future can be joined methodologically. Scenarios attempt to generate points of reference for the future. They do not deliver unambiguous prognoses on results, however, but offer a simulation of "what-if". They delimit a specific spectrum of possible sample spaces and thus indicate a range of possible future developments. They can also be used to make transparent the effects of decisions for a

14 In the Anglo-Saxon world, the instruments of future analysis have been employed for political consultancy for many years. In Germany, such methods are primarily employed in business and corporate environments. In terms of its relevance to security and the armed forces, this discipline is still in its infancy.

system. Scenario technique does not claim to be able to predict the future, but provides a foundation for interpreting it. The necessary precondition for useful scenarios consists of trends and counter-trends that delimitate the problem field.

Trend and countertrends from the seven trend fields describe the scenarios relating to geographical spaces such as a state, a region (e.g., Europe), or the world. Furthermore, scenarios can be developed for specific important topics such as climate change, organized crime, globalization, etc. This process begins with the description of a departure scenario and potential variations of scenarios determined by a variety of trends. The various trends are used to describe the topography of alternative scenarios. Using the Cross Impact Matrix technique,[15] these variations can be juxtaposed for interpretation. The analysis is concluded with a search for interference values (so-called wild cards) in all trend fields, which may have a fundamental effect on the scenarios. Examples include a meteorite with a diameter of 10km, the impact of which on our planet would radically alter all scenarios. All trends and scenarios are documented and continuously updated. Where necessary, new trends are added and obsolete ones are removed. This kind of trend management also serves to identify important trend indicators that, if changed, would also change the scenarios. To this end, the actual scenarios are documented and updated. Like trends and scenarios, wild-card scenarios are also collected and systematically developed.

This approach to trend and scenario management constitutes the basis for continuous, indispensable training of the staff members in the Department of Future Analysis. Trend and scenario management also serve to improve communication of the results of future analysis within the Bundeswehr, as well as to other partners (NATO, EU) and the interested public.

Furthermore, other methodological approaches to future analysis beyond those described above are employed. For example, in order to

15 Cf. Fredric Vester, *Die Kunst, vernetzt zu denken* (Stuttgart: Deutsche Verlags-Anstalt, 2000), chapter 13, pp. 196ff.

evaluate the in-house approach, a "historical trend analysis"[16] was conducted as a workshop to elaborate indications of the usefulness (scope and limitations) of historical analogies for explaining causal connections. Currently, the use of computer programs for supporting analysis, scenario development, and validation and identification of important trends (indicators) through simulation is being evaluated.

Although the process cannot be described here in detail, the following description aims to clarify the methods of future analysis and to present some of the most important results as they apply to the resulting trend field of "the future face of war".

4 Conclusions from analysis

The most important impending changes for the face of war in the 21st century and for the relevant environment by 2035 will be briefly summarized in the following. The four main transformation potentials for the development of future security policy and armed forces are:

- The transition from the industrial to the post-industrial society
- The vulnerability of modern societies
- The changing face of war
- Asymmetric violence

4.1 Transition to the post-industrial society

First, we will discuss the transformation from the industrial to the post-industrial society: A new social system is emerging on the basis of the information and knowledge revolution.

In this society, the focus is on the creation, distribution, management, use, and conservation of knowledge. Knowledge means the creative use

16 Zentrum für Transformation der Bundeswehr, *Historische Trendanalyse – Vergangenheit verstehen – Zukunft gestalten*, workshop report (Munich: IAP-Dienst Wissenschaft, 2004).

of information in order to resolve challenges and problems. Knowledge is becoming a production factor in its own right, and in this sense, knowledge determines all social processes and entities. In the course of this development, access to knowledge and the exchange of information becomes universal to include individuals, social groups, politically and economically relevant actors, states, and alliances. Any form of social power and legal rule has the tendency to constitute itself either as non-state entities and groups, as (global) economic institutions, or as actual states. Generally, the possibilities provided by modern technology will also increase the range of means of influence and control for all actors.

The consequences of the development from industrial societies into post-industrial ones – a process that is mainly characterized by the revolution in information processing and generating knowledge – will also necessitate an adaptation of the armed forces to the principles of the new form of society. Such principles currently include knowledge as a production factor, integration, flexible and task-oriented structures and organizations, and an ongoing dematerialization of all production processes. They imply an increase in productivity based on a human workforce that is decreasing in size. For the military, this means that fewer soldiers can have an increasing and more targeted effect. Therefore, a quantitative superiority is no longer an advantage – or at least, not until greater numbers are also imbued with a qualitative advantage.

On the one hand, these fundamental changes introduced by accelerated[17] social change, which coincide with the abolition of constraints on global development processes, offer a huge potential for development, while on the other hand, they open new avenues of attacking these complex and networked societies. However, potential hostile actors would need to have a sufficient concentration of capital and knowledge at their disposal.

17 Hartmut Rosa, *Beschleunigung* (Frankfurt am Main: Suhrkamp, 2005); cf. pp. 311ff., 'Beschleunigung und ihre Wirkung auf zentrale Institutionen der Gesellschaft', notably the diagram at p. 329.

4.2 Vulnerability of modern societies

The fundamental processes of social transformation as outlined above lead immediately to the second salient potential for transformation, namely the vulnerability of modern societies.

The increasing vulnerability of the complex resources and structures in post-industrial societies, where the uninterrupted functioning of networks is a crucial part of the everyday survival of each individual, constitutes an important point of attack for violent actors. Under these conditions, primary goals include securing basic needs (supply of food, water, energy, etc.), as well as ensuring information security and the uninterrupted use of the information and communication infrastructure.

The broad range of potential violent actors and their spatial and temporal freedom of action means that they can leverage their knowledge about the vulnerability of modern societies in order to cause large-scale[18] damage in the form of direct and surprising destructive acts. Early-warning time is reduced even where knowledge about actors is available.

This implies a degree of vulnerability that is determined by the following aspects:

- Accessibility of knowledge
- Complexity of the supply chain and other infrastructure
- Concentration of management
- Integration
- Mobility and loss of constraints
- Dependency on information and communication technology

18 Defined in SFT 21 2035, part II, chapter 2.2.2, note 125.

4.3 The changing face of war

Against the background of these developments in modern societies, constraints on organized violence are lost. This trend is in stark contrast to earlier epochs where, according to Clausewitz, war was regarded as the continuation of state politics by other means. The global public has a conception of the image of war that is rooted in the devastations of the Thirty Years' War, enhanced by images of the Dresden firestorm in the Second World War. This is a notion of war as a "global conflagration, a total war".[19]

"Threat" was therefore defined in the security policy concept of the 19th century as the political determination to employ the military potential of one state or group of states against others with warlike intentions or to convey a credible threat to do so.[20]

The word "war" has generally been understood to refer to a "major military conflict".[21] This conception is based on an understanding of war as a legal status between two states and has historically been supported by the emergence of territorial states. According to this view, only states and their regular armed forces had the right to wage war. After the experience of war in the medieval world, a certain legal framework for war emerged, resulting in codified rules of war under an increasingly differentiated body of laws of war and international law. For example, only the opposing armed forces were counted as legitimate targets of military operations, while the enemy's civilian population was not. Nevertheless, the applicability of this image of war has largely remained limited until today to relations between the European and Atlantic states.[22] It was only after the attacks of 11 September 2001 that the international com-

19 Cora Stephan, 'Krieg ist nicht Apokalypse', *Die Welt*, 13 October 2001, p. 29.

20 Günter F. C. Forstenreicher: *Neue Formen der Bedrohung der internationalen Sicherheit: Terrorismus – Proliferation – Organisierte Kriminalität – Migration. Erscheinungsformen – Bewältigung – Sicherheitspolitische Aspekte*, Sonderbroschüre IAP-Dienst Sicherheitspolitik (Bonn: IAP-Dienst Sicherheitspolitik, 2001), p. 7.

21 Ibid.

22 Martin Hoch, 'Krieg und Politik im 21. Jahrhundert', *Aus Politik und Zeitgeschichte*, supplement to *Das Parlament*, 20 (Berlin: Bundeszentrale für politische Bildung, 2001) <http://www.bpb.bund.de/publikationen/SW12JX,,0,Sicherheitspolitik.html>, accessed 8 August 2007.

munity realized that the image of war is changing at the dawn of the 21st century.

First of all, war is increasingly perceived – under the notion of enforcing national interests, as described above – as a violent perversion of politics.[23] Nearly all states of the world are significantly integrated in economic and political terms, so that outbreaks of inter-state conflicts based on supra-regional dependencies are becoming increasingly unlikely.

Secondly, there is a change in the increasingly outdated conception of war characterized by a clear distinction between states of war and states of peace, and by the absence of a third state apart from these two.

Third, a conception of war is being advanced in qualitative and quantitative terms that has always been present since the end of the Thirty Years' War, but nevertheless has never been at the focus of strategic considerations.[24] This notion is characterized by armed violent conflict between state and non-state actors, but also among non-state actors. This kind of violence – also labeled "small" or "new" war[25] – is not necessarily lesser in terms of intensity, duration, destructive force, or effect than that of "large" inter-state conflicts. Therefore, the term "small" war does not do full justice to the future phenomenon of violence. But one might also question the epithet "new" in the concept of "new war" with equal justification, since a broader historical approach reveals that it is not so new at all.

Participants can be expected to include both state and non-state actors, who will use conventional as well as asymmetric forms of warfare, all of which take place both in real space (land, air, sea, and outer space) and in virtual cyberspace with effects that are felt throughout society.

In this context, Peter Lock identifies three characteristics of such "new" wars: Denationalization and commercialization of violence; asymmetry

23 Erhard Rosenkranz, 'Der Dritte Weltkrieg ist vermieden, nun ist der Weltterror ausgebrochen', *Marineforum*, 11 (2001), p. 2.

24 Hoch, p. 3.

25 Christopher Daase, *Kleine Kriege – Grosse Wirkung* (Baden-Baden: Nomos, 1999); Herfried Münkler, *Die neuen Kriege* (Berlin, 2002); Mary Kaldor, *Neue und alte Kriege: Organisierte Gewalt im Zeitalter der Globalisierung* (Frankfurt am Main: Suhrkamp, 2000).

in the willingness to use violence; and the release of violence from the fetters of integration into the military context.[26]

4.4 Asymmetry of violence

The term "asymmetric war"[27] only makes sense semantically if it is used to describe something other than the qualitative or quantitative disparities between the participating actors in a conflict, since many – if not most – of the past wars would otherwise have to be labeled as "asymmetric". This probably relates to a deeper-seated mechanism reflecting the manifold use of the term in a variety of contexts. The phenomenon of asymmetry in warfare can therefore only be approached if the symmetry of violence is not conceived as being self-evident, but as being rooted in the emergence of the European state order in the early modern age. The European state system, an outgrowth of the Peace of Westphalia (1648) that provided the backdrop for the development of classical theories of war, is based on assumptions about symmetry and sovereign territorial statehood. States, which hold a monopoly on war, are constituted in this system as the only legitimate actors to employ force and resemble one another in that respect. According to this approach, a war is symmetric if the parties to the conflict are regarded as reflections of one another in terms of equality or comparability.[28] The boundary between the parties or the frontline on the battlefield, in a way, marks the axis along which the opposing actors are mirrored. The laws of nations and the laws of war originated as an expression of the symmetric order of states. To this extent, sovereign states acknowledge one another as being fundamentally equal and concede each other the right to wage war (ius ad bellum), while also committing themselves to respect the prin-

26 Sabine Kurtenbach and Peter Lock, *Kriege als (Über)Lebenswelten: Schattenglobalisierung, Kriegsökonomien und Inseln der Zivilität* (Bonn: J.H.W. Dietz, 2004), pp. 20f.

27 Felix Wassermann, *Der Dschungel des asymmetrischen Krieges*, Master's dissertation, Institut für Sozialwissenschaften, Humboldt University (Berlin, 2004); Josef Schröfl and Thomas Pankratz (eds.), *Asymmetrische Kriegsführung – ein neues Phänomen in der internationalen Politik?* (Baden-Baden: Nomos, 2004).

28 Herfried Münkler, 'Angriff als beste Verteidigung? Sicherheitsdoktrinen in der asymmetrischen Konstellation', *Internationale Politik und Gesellschaft*, 3 (2004), pp. 22–37, at pp. 24ff <http://www.fes.de/IPG/arc_04_d/03_04_d/b03_04_1.htm>, accessed 8 August 2007.

ciples of the laws of war (ius in bello). War and peace are distinguished as separate states of law, and the rules governing transgression of these states are given an institutional framework by virtue of formal declarations of law and formal peace treaties.[29]

The reciprocal acknowledgement of opponents and the mutual commitment to adherence to the agreed rules govern proceedings at the negotiation table and on the battlefield. States, in principle, wage war as conventional war, which implies in particular that they limit warfare to the actual battlefield.[30]

The core element of symmetric warfare is therefore the conscious political limitation of the conflict. Conversely, the loss of constraints in politics, in political goals, and therefore in war, can be seen as the cause of asymmetric conflict. Clausewitz identifies politics as the force that prevents war from succumbing to the logic of violence.[31] Where political expediency is taken to its extreme, or where it is replaced by economic or religious goals, violence is released from its fetters and becomes asymmetric. This loss of constraints applies to five aspects in particular:

- Actors
- Goals and purposes
- Methods
- Space
- Time

The trends in the transformation of war as described here will determine, in various permutations, the scenarios for the coming decades.[32]

29 Wassermann, p. 15.

30 Ibid., p. 17.

31 Carl von Clausewitz, *Vom Kriege*, Hinterlassenes Werk des Generals Carl von Clausewitz, complete ed. in one volume (Bonn: Ferd. Dümmlers, 1980), pp. 200ff.

32 Kurtenbach and Lock, p. 21.

The conception of future war is general in nature, describes abstract developments, and serves as a conceptual basis for deducing conclusions. Assuming, as security-policy practitioners do, that the great industrial nations will continue to have a significant interest in securing a (more) violence-free international order in the future, the most important goals of future security policy will be a cooperative multipolar world order and the prevention or containment of war (both inter-state and "small" wars). This implies that the states of the world will develop their military instruments in a way that will allow them to intervene successfully in such conflicts. The ability of armed forces to operate within the United Nations or as part of alliances or ad-hoc coalitions, with combined arms and global force projection, will continue to increase.

Just as an increasing mechanization of land, air, and naval warfare aimed at destroying enemy capabilities could be observed over the past century, the security-policy framework and tactical-operative applications of modern technology create new possibilities for the future. Information technology has a key role to play in this context, since it can support all branches of the military, but will also become a branch of warfare in its own right. The main aspects of the future warfare of industrialized nations that are discernible today include: First, a general conception of warfare and its constitutive elements, geared towards the abovementioned political goals of a cooperative global order and the resulting military tasks; and secondly, orientation towards scientific-technological developments and resulting possible options for tactical-operative concepts that meet the related challenges. The picture emerging from these components implicitly encompasses all relevant development trends.

5 Summary

Strategic future analysis is not an exact science, but makes use of scientific instruments and insight to offer consultancy for political and administrative decision-makers.

It is in itself a tool for methodical and systematic analysis that is expected to support the top level of political and military leadership within the Bundeswehr in the highly complex planning process for the conceptual development of the armed forces.

As far as current insights of previous analyses are concerned, the following emerging changes in the security-relevant environment of the future can be extracted and highlighted:

- All parts of society in the "modern" world are undergoing a process of transformation from industrial to post-industrial societies, the main characteristics of which include an explosion of knowledge and a productive response to this transformation.
- The globally observable asynchronicity of development processes within civilizations is an obstacle to the process of "global governance" as demanded by the political sciences. In terms of security policy, this process confronts the states that have the greatest creative capabilities with the challenge of global responsibility, for which the political entity of the "nation-state" and its orientation towards its national interests is not yet ready.
- In the course of this process towards civilization, forces are unleashed that are reminiscent of the past, but which may also come to dominate the future. The de-nationalization, economization, and ideological justification of organized violence (war) and its admixture with individual and collective social violence that has hitherto been categorized as "crime" represent a new challenge. The international security system has so far been geared towards the prevention of interstate conflicts, but in the future, the containment of the various forms

of non-state violence will have to become an additional focal point of such a system. In the past 50 years, such conflicts constituted about two-thirds of all armed conflicts, and that tendency is increasing. This is a development that, due to the global implications outlined above, requires that security policy already be realigned at this stage.

- Technological innovation, which is taking place at an ever-increasing pace and is market-driven, will continue to be a driving force for the armed forces of the future. On the one hand, it is a contributing factor to the shape of future threats, while on the other hand, it provides the basis for technical systems determining the shape of the armed forces that are expected to respond to them.

These changes demand that the armed forces of post-industrial societies be modernized through a constant process of transformation. Such radical change in the social system must result in constant, but sustainable transformation of the armed forces.

EARLY WARNING AND POLITICAL RISK ANALYSIS IN THE ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE (OSCE)

Erik Falkehed [1]

The strengths, challenges, and opportunities of early warning and political risk analysis in the OSCE are connected to the basic characteristics of the organization. The OSCE is essentially an intergovernmental, co-operative political organization. The implication is that information is gathered from diverse, often informal channels, and that there are no formal indicators by which countries are being monitored. Within the OSCE, early warning can therefore be said to be a mode of operation rather than an abstract goal in itself. Thanks to the OSCE's diverse ways of engaging with its member states and its regional presence, the OSCE is well connected with developments on the ground. The Field Missions are truly the "eyes and ears" of the organization and often the first source of early warning. They stand in regular contact with the Conflict Prevention Centre in the Secretariat, which, in practice, is the heart of the OSCE's institutional early-warning and political analysis function. Currently, however, most OSCE structures individually assess the information that is obtained. While this diversity is one of the strengths of the OSCE, there is a risk that early warning and risk analysis may be improvised and incomplete and have a low impact due to the lack of organization-wide consolidation of information.

1 The views expressed here do not necessarily represent the position of the OSCE.

1 The OSCE approach and capacities

1.1 Principal OSCE characteristics and implications for early-warning capacities and political risk analysis

The capacities of the OSCE in early warning and political risk analysis are shaped by a number of basic characteristics and conditions. The OSCE is recognized as a regional arrangement under Chapter VIII of the UN Charter and has a primary mandate for early warning, conflict prevention, crisis management, and post-conflict rehabilitation.[2] The status of the OSCE is not one of an organization in the strict sense. As mentioned above, the OSCE constitutes a *regional arrangement* under the UN Charter rather than a legal person. This implies that political decisions for (early) action are up to the participating states (i.e., the member states) and the chairman-in-office (CiO)[3]. It also means that parties to disputes address the OSCE as a regional organization first in order to seek advice on methods of peaceful settlement, in line with the UN Charter.[4] Furthermore, the OSCE pursues a *comprehensive concept of security* consisting of a political-military, an economic and environmental, and a human dimension. The deterioration of security in one dimension is understood as reducing security overall. This means that early warning and political risk analysis are conducted in the context of all three dimensions.

2 The mandate of the OSCE to provide early warning can be traced back to the era of the Conference on Security and Co-operation in Europe (CSCE) (Ministerial Council in Prague, 1992). Cf. Second Meeting of the Council, Summary of Conclusions, III. 6: "Representatives to the Follow-up Meeting should, in particular, be guided by [...] the need to strengthen the capacity of the CSCE to contribute, in accordance with CSCE principles, to a peaceful solution of problems involving national minorities which could lead to tensions and conflict – both within and between States – including possibilities for early warning." The OSCE Strategy to Address Threats to Security and Stability in the Twenty-First Century (Ministerial Council in Maastricht, 2003) specifically delegated to the OSCE the task of strengthening the early-warning function of the OSCE, its Secretariat, and its institutions and field operations (para. 22).

3 The chairman-in-office of the OSCE is the foreign minister of the country holding the Chairmanship. As such, he has overall responsibility for executive action. The Chairmanship rotates annually on 1 January of every year.

4 Article 33 requests that the "parties to any dispute, the continuance of which is likely to endanger the maintenance of international peace and security, shall, first of all, seek a solution by negotiation, inquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their choice."

Early warning is one of the key functions of the OSCE. Socio-economic disparities, political instability, autocratic regimes, organized crime, and humanitarian crises or natural disasters are only some of the factors that continue to carry the risk of potential conflict within the OSCE area and that give rise to requests for assistance by the member states. The OSCE is essentially an intergovernmental, co-operative organization of a political nature. The implication for early warning and political risk analysis is that information is gathered from diversified, often informal channels and that there are no formal indicators by which countries are monitored. Within the OSCE, early warning can therefore be said to be a mode of operation rather than an abstract goal in itself.

As political risk analysis is an essential part of early warning, and is frequently indistinguishable from the latter, this paper will generally not deal with them as separate and detached entities. Instead, when we refer to the early-warning process within the OSCE, the reader must keep in mind that political risk analysis is implicitly included, just as it is in the daily work of the organization. However, for clarification, under most definitions, early warning is understood to involve at least three elements:

- Regular monitoring of conflict indicators
- Analysis of security-relevant developments, and
- Preparation of timely and appropriate policy responses.

Concerning all three elements, the OSCE has developed an array of substantial capacities. The main bottleneck for early warning is indeed the reaction time (between the perception of the signals and the outbreak of actual conflict). However, one key advantage is that within the OSCE, various forms of political dialog and informal consultations serve as a source of information as well as a method to determine early action. This and the multilateral character of the organization give the OSCE another standing, often perceived as more neutral than other organizations.

1.2 OSCE institutional capacities and tools

The present shape of the OSCE with its specific institutions, norms, and instruments has been developed mostly to address the issues that emerged after the breakdown of the Soviet Union.

This is true, on the one hand, for the OSCE's *norm-setting function* in areas concerning democracy, human rights, and basic freedoms, minority rights, but also applies to norms concerning the military side, be it with respect to the military relations between states (arms control, military confidence- and security-building), but also the situation of the military within states (democratic control, norms against the misuse of the armed forces, respect for humanitarian international law, etc.). These norms can be seen to serve a dual function: stability through compliance and early warning in the case of non-compliance.

The same applies, on the other hand, to the broad array of *institutional instruments* of the OSCE to cope with crisis-prone situations. Overall, OSCE capacities in early warning demonstrate the diversity of information available within the organization, whether it is obtained on the basis of political dialogue, projects, formal or informal exchanges, or through open information sources. Each OSCE structure individually assesses the information it obtains. While this diversity is a major strength of the OSCE, it also creates a need to better integrate this data in the preparation of policy responses.

Today, the OSCE has a number of tools for conducting its early-warning responsibilities. Of course, many of these tools can also be used for political risk analysis. The extent to which this is actually done in practice (at least in a structured and formalized way) is a matter of debate. It could be argued that, despite all the instruments for early warning that are at the organization's disposal, the actual conduct of structured political (risk) analysis is not commensurate to the amount of early warning signals and indications available. Nevertheless, these tools include:

- Institutions: The Parliamentary Assembly (PA), the Representative on the Freedom of the Media (FOM), the Office for Democratic Institutions and Human Rights (ODHIR), and the High Commissioner on National Minorities (HCNM). All these institutions are involved

in monitoring and following specific situations/activities throughout the OSCE region, and are in a position to provide early warning when necessary.

- Field Missions and Activities: These are the "eyes and ears" of the OSCE. Field missions fulfill a unique role and as such are a vital tool. Their activities can do much in the area of conflict prevention, crisis management, and post-conflict rehabilitation, but they are also extremely well-placed to give early warning. Field missions (long-term missions, fact-finding missions, and observation and support missions) are a major asset of the OSCE in understanding developments on the ground and engaging with member states constructively. Missions report on a regular basis to the chairman-in-office and the Secretariat (Conflict Prevention Centre, CPC). So-called "spot reports" are delivered in urgent situations. The missions are therefore often the first source of political risk analysis and early warning. Currently, the OSCE maintains 19 field missions which support member states in South Eastern Europe, Eastern Europe, the Southern Caucasus, and in Central Asia consolidating comprehensive security. Some missions have very specific tasks, such as border monitoring (in Albania, Macedonia, and formerly in Georgia), monitoring democratic institutions and practice (Serbia, Croatia), or gathering information (Moldova). The missions are well aware of security developments and the extent to which OSCE norms are applied in practice, e.g., whether the laws they have analyzed and drafted have become general practice.
- Personal Representatives of the Chairman in Office (PRs): PRs are active in a number of regions, particularly in the field of "frozen" conflicts[5] that carry the risk of "reigniting". The involvement of a PR means that specific situations will be monitored in a dedicated and committed fashion, since a PR has the obvious advantage of being in a position to both be aware of and to affect changes in a given situation immediately, should this be necessary.

5 The term "frozen conflicts" generally refers to the cases of South Ossetia, Abkhazia, Nagorno-Karabakh, and Transdniester.

- Delegations: The 56 member states have their own means of monitoring particular situations and are in a position to bring any specific concerns to attention of the Permanent Council at any time. To varying degrees, the delegations do also conduct their own political risk analysis of events and developments in the OSCE region. Through the political dialog in Vienna, the delegations can also be said to fulfill an early-warning capacity through regular information exchange (e.g., in the Permanent Council and in the Forum for Security Cooperation), regular review of commitments, informal exchanges, and feedback from missions and institutions.
- Situation/Communications Room: In the Secretariat in Vienna, there is a Situation/Communications Room that is staffed on a 24/7 basis and tasked, inter alia, with following the news as well as using open-source information (such as the internet) to collect relevant raw data on situations of interest throughout the OSCE region. The Situation/Communications Room is also an important member of the NATO/EU/UNDPKO family of "operation centers", and a variety of unclassified reports are exchanged on a daily basis. Where developing situations of mutual interest occur, there is a regular exchange of information. But most importantly, the OSCE missions are in place to provide updates on events as they occur.
- Analyst: An analyst works in the CPC within the Secretariat. The analyst has a multi-faceted role, but is in a position to make longer-term assessments and reports on events. This analyst is supposed to use the information supplied by the Situation Room/Communications in order to research developing situations and bring them to the notice of the Chairmanship, whenever necessary. However, so far, the organization has only made sporadic use of the position for continuous political risk analysis.
- The Conflict Prevention Centre in the Secretariat (which, among other functions, includes the Mission Program Section, the Situation/Communications Room, and the analyst) is the heart of the OSCE's functions in terms of early warning and political analysis. As

mentioned above, the CPC supports the field operations and functions as a focal point for conflict prevention, crisis management, and post-conflict rehabilitation. Especially activities in the politico-military dimension are supported by the CPC. Since the creation of the Secretariat,[6] the CPC has been providing support to the organization in early warning. Specifically, the Operations Unit within the CPC was given the task of identifying potential crisis areas.[7] As a result, the mandate of the CPC is to serve as the focal point for early warning, and it has capacities and functions in all three aspects of early warning. Consequently, monitoring, analysis, policy and operational preparation are united. This link under a single institutional structure is intended to ensure relevance, timeliness, and adequacy of early warning

To be more precise, the specific early-warning capacities of the CPC extend to the following:

- Monitoring and analysis: E.g., through continuous contact with developments on the ground in mission areas and beyond. This is complemented by frequent contacts with delegations, providing yet another useful perspective in the assessment.
- Facilitating response: The CPC carries out an alert and support service for the chairman-in-office and the secretary general (SG). At the operational level, quick reaction is facilitated in particular through the Operations Unit (liaison, planning, analysis, lessons learned, and input from the Situation/Communications Room).
- Responding to requests for assistance: information obtained through projects especially in the political-military domain provides additional feedback on the political situation and developments that ought to be consolidated with overall early-warning information.

6 Rome Council, 1993.

7 Organization for Security and Co-operation in Europe OSCE, Permanent Council, *Decision No. 364: Strengthening of OSCE Operational Capacities*, PC.DEC/364 (Vienna: OSCE Permanent Council, 29 June 2000).

- Links to other partner organizations and their own early-warning and analysis systems, both at the level of headquarters and on the ground.

2 Overall assessment of OSCE's early-warning and political risk analysis capacities

The strengths, challenges, and opportunities of early warning are connected to the basic characteristics of the OSCE mentioned in the beginning.

Due to the OSCE's diverse ways of engaging with its member states and its regional presence, it is well connected with developments on the ground. Far-reaching instruments such as the HCNM and the field missions give the OSCE a clear advantage in early warning. OSCE decisions, recommendations, and review mechanisms (although not legally binding) help to informally build political pressure.

At the same time, the diversity of information requires that early-warning information be integrated and analyzed more systematically and continuously, which goes against the decentralized nature of the organization and its rotating political leadership. Furthermore, the OSCE needs to consider more extensively those security developments that do not originate in, but affect the OSCE area.

The transparent nature of the organization itself has a confidence-building effect, as all information is shared with member states. Transparency also enables full information-sharing with other international players like the UN, the EU, and NATO, to whom the OSCE may refer cases of emerging crises. Regular staff-level meetings with these organizations have proven a useful format to bring the organization up to date in areas of common concern.

Some concrete examples of OSCE early warning

A clear example of early warning includes the work of the Border Monitoring Mission in Albania (1998), which was set up to monitor the situation in the northern border region area of Albania with Kosovo (and Serbia), including

fighting, the flow of refugees, and the humanitarian situation. Monitors in border field offices provided much-needed data for decision-makers within and beyond the OSCE, e.g., real-time border monitoring reports and observance of aid distribution and implementation.

Also, the "Moscow Mechanism"[8] was invoked several times because of reported attacks on civilians in Croatia and Bosnia-Herzegovina (1992), legislation in Estonia, minority rights in Moldova (1993), and reported human-rights violations in Serbia and Montenegro (1993); in the last case, the OSCE's intervention failed because of the authorities' lack of co-operation. The example of Turkmenistan in 2003 seems to suggest that the mechanism needs to be revised as a more co-operative instrument. In 2003, a fact-finding mission of ODIHR tried to examine concerns regarding the conduct of investigations resulting from the reported attack on President Saparmurat Niazov. Although the mission was unable to travel to the country, its initiative helped to focus the attention of the OSCE and other international actors on the ongoing crisis.

The HCNM has on several occasions raised issues concerning minority rights. For example, in 1998, the start of the crisis in Kosovo had a severe negative effect on the situation in the Former Yugoslav Republic of Macedonia, which had to deal with a considerable number of Albanian refugees from Kosovo. This led the High Commissioner for the first time to issue a formal early warning on 12 May 1999 that unless the international community significantly increased its efforts to provide more assistance, the country could become destabilized.

8 The OSCE has established a number of tools to monitor the implementation of commitments that member states have undertaken in the field of human rights and democracy (the human dimension). One of these tools, the so-called Human Dimension Mechanism, can be invoked on an ad-hoc basis by any individual member state or group of states. It is composed of two instruments: the Vienna Mechanism (established in the Vienna Concluding Document of 1989) and the Moscow Mechanism (established at the last meeting of the Conference on the Human Dimension in Moscow in 1991), the latter partly constituting a further elaboration of the Vienna Mechanism. The Moscow Mechanism builds on this and provides for the additional possibility for member states to establish ad-hoc missions of independent experts to assist in the resolution of a specific human dimension problem either on their own territory or in other participating states of the OSCE. The ODIHR is designated to provide support for the implementation of the Moscow Mechanism, and it maintains a list of experts appointed by some of the member states who are available to carry out such investigations.

Furthermore, the CPC was instrumental in supporting the mediation processes related to the crisis in Ukraine following the contested second round of presidential elections in 2004, and in mediating during the crisis which broke out in Kyrgyzstan following the parliamentary elections in February and March 2005.

3 Challenges and opportunities for improvement

It is usually assumed that within the OSCE, early warning is a mode of operation rather than an abstract goal in itself. The organization has the mandate and the tools. However, it must be pointed out that while a key advantage of the OSCE in early warning is that it can draw on its various forms of political dialog, both as a source of information as well as a method for determining early action, limitations in the institutional nature of the OSCE do make for certain challenges.

Overall, the OSCE's capacities in early warning demonstrate the *diversity of information* available within the organization, be it obtained on the basis of political dialog, projects, formal or informal exchanges, or through open information sources.

However, at present, most OSCE structures individually assess the information they obtain. While this diversity is a major strength of the OSCE, there is also a risk that early warning and political risk analysis may be improvised, incomplete, and lose impact due to the lack of organization-wide consolidation of early-warning information. Unless relevant information is better integrated, it will be difficult to make an adequate assessment of the full web of causalities and potential consequences as security risks evolve, and so prepare a suitable response.

So, while the OSCE has this primary mandate in early warning, when we look to consider OSCE realities, a pragmatic approach is needed that takes into account the political nature of the organization and the diversity of its instruments for political risk analysis and early warning.

Another challenge is the *political sensitivity* of early-warning information, and the reaction anticipated from the member states directly concerned

– but then, no state likes to be told it has a problem. However, if early warning is not delivered, even in the most serious cases, the OSCE will lose credibility significantly.

It must also be kept in mind that security risks affecting the OSCE area go well beyond its *geographical scope*. Due to the reliance on, and importance of, information gathered on the ground, early warning has been largely concentrated to the OSCE's mission areas. This approach does not always properly reflect the areas where security risks, including those identified in the OSCE "Threats Strategy", originate, and neither does it cover those areas with the potential to be "affected". The existing and potential spill-over from the conflict in Afghanistan is the most obvious case-in-point. What is clearly lacking is a regional stability assessment, conducted periodically, which would cover also the non-mission areas (but does not single out a specific state).

As the significance of threats has shifted over the past 15 years, it may also be time to *thematically re-prioritize* ways of anticipating them. Many of the OSCE's existing early-warning capacities (e.g., peaceful settlement of disputes) continue to be a product of the time of their creation. Furthermore, as always, a greater capacity for political analysis is required in order to purposefully link monitoring results, response options (policy, operations), and appropriate response channels.

In conclusion, before ways of strengthening the OSCE's approach to and performance in early warning and political risk analysis are considered, a few general questions ought to be raised and clarified. The questions are as follows:

What purpose and what audience should early warning serve?
The purpose of early warning may vary, ranging from assessing risks, reviewing OSCE activities, using the information obtained as a basis for political dialog, setting critical issues on the agenda of the Permanent Council and/or other organizations, and measuring progress to making technical recommendations concerning OSCE commitments. What kind of action should result from early warning?

Closely connected to this matter is the question of who the information should be directed at – the chairman-in-office, the secretary general,

or the member states directly? Furthermore, to which extent will early warning information be shared, e.g., with other organizations? Based on these fundamental questions, one could define flexible areas of concern to be monitored more regularly.

Early warning of what?

- What kind of threats should be considered? The threats identified in the OSCE Strategy could be used as entry points for analysis. What kinds of adjustments in monitoring, analysis, and policy projection would this require?
- Regional scope: To what extent should threats originating from outside of the OSCE (mission) area be considered in OSCE early warning?
- Role of non-state actors: How can non-state actors be included in early-warning assessments, both as actors in potential conflict and as sources of information?
- Does it make sense to define thresholds for OSCE early warning? In other words, is it sufficient for OSCE commitments to have been violated?
- Should early warning help to identify critical conditions, causes of potential conflict, or developments that may lead to instability? In the latter case specifically, indicating a trend and providing regular updates could be vital elements of early warning. Could an indicator system be a possibility?

What is "early" enough?

How can follow-up be ensured, and what are the factors that could have an impact on the effectiveness of early warning? What stage of urgency should be recorded primarily?

Early warning by whom?

The diversity of information suggests a need for consolidation. Therefore, for the sake of sustainability, a central early-warning capacity would seem most purposeful, and could ensure that early-warning information is integrated and passed on to the main "benefactor" (the secretary general, the

chairman in office, or possibly member states). This would subsequently make a case for further strengthening the analytical capacity in the OSCE Secretariat.

4 Conclusion

While the OSCE has a primary mandate in early warning, when we look to consider OSCE realities, a pragmatic approach is needed that takes into account the political nature of the organization and the diversity of its instruments for political risk analysis and early warning. Within the OSCE, early warning is indeed a mode of operation rather than an abstract goal in itself. However, it must be pointed out that while a key advantage of the OSCE in early warning and political risk analysis is that it can draw on its various forms of political dialog, both as a source of information and as a method for determining early action, limitations in the institutional nature of the OSCE do make for certain challenges. While the diversity of the OSCE is one of its strengths, there is, however, a risk that early warning and political risk analysis may be ad-hoc, incomplete, and low in impact due to the lack of organization-wide consolidation of early-warning information. Even if it goes against the decentralized nature of the organization and its rotating political leadership, the diversity of information requires that early-warning information be integrated and analyzed more systematically and continuously than is currently the case.

FINANCIAL AND INSURANCE BUSINESSES

EARLY DETECTION AND MANAGEMENT OF EMERGING RISKS IN THE FINANCIAL SERVICES INDUSTRY: LESSONS FROM INSURANCE BUSINESSES

Bruno Käslin

Organizations interact with their environment at many different levels. Therefore, surprising events or unanticipated trends in the environment can quickly lead to negative implications for a company's financial outlook. "Emerging risks", which arise from changing environmental conditions, are especially relevant for the insurance industry. We define emerging risks as new or newly occurring risks or issues with an uncertain but high damage potential. The early detection, analysis, and evaluation of emerging risks allows insurers more time to make appropriate decisions concerning the management of these risks. With adequate early-warning systems, insurance companies can react faster and make better-informed decisions in response to trends and developments. This paper describes the character of emerging risks and their implications for the insurance industry. Based on a detailed analysis of four successful implementations of emerging risk management systems in the insurance industry, four dimensions – organization, processes, culture, and information technology – are introduced to describe important strategic implications of emerging risks for the insurance industry. The research presented is a unique study as it is the first examination of emerging risk management procedures in the insurance industry.

1 Introduction

A current survey on the impact of diverse trends and developments on the insurance industry shows that the topic of "emerging risks" is of great significance for insurance managers.[1] In addition, more than 40 per cent of the respondents to a recent CEO survey from PricewaterhouseCoopers stated that the greatest risks to their organization's market value are "unknowns".[2] The discourse on emerging risks has intensified recently and in many insurance firms the topic is of high priority.[3] Many events (e.g., those organized by the Institute of Insurance Economics, Swiss Re, E+S Reinsurance, and Handelsblatt), research programs (e.g., the Chief Risk Officer Forum Emerging Risk Initiative),[4] and journal articles are further evidence of the increasing interest in this topic.

2 Definition and characteristics of emerging risks

In the insurance industry, the term "emerging risks" refers to risks that are new or have not yet been discovered, which have an uncertain damage potential in the near or long-term future and thus could have serious consequences for insurers and reinsurers. According to the major reinsurers and insurers, emerging risks include phenomena such as electromagnetic fields (EMF), gene technology, nanotechnology, pervasive computing, oc-

1 Unpublished survey by the Institute of Insurance Economics at the University of St. Gallen (2005/2006). Survey participants included more than 250 senior management professionals in the insurance industry.

2 PricewaterhouseCoopers, *Uncertainty Tamed? – The Evolution of Risk Management in the Financial Services Industry* (2004), p. 3 <http://www.pwc.com/images/gx/eng/fs/072704eiurisk.pdf>, accessed 8 August 2007.

3 As Munich Re writes in the 2nd Chief Risk Officer Assembly 2006 Conference Report: "Emerging risks are by far the biggest challenge for the insurance industry." Cf. Munich Re, *2nd CRO Assembly 2006 Conference Report* (2007), p.8 <http://www.munichre.com/publications/302-05241_en.pdf>, accessed 8 August 2007.

4 See <http://www.croforum.org/emergingrisc.ecp>.

cupational diseases such as silicosis or asbestos, pandemics, new financial distresses, or reputation risks.[5]

The danger from "traditional" risks is, almost by definition, immediately obvious and includes, for example, risks emanating from cars, bridges, or aviation; emerging risks are very different in this regard. Due to the most distinctive property of emerging risks – their novelty – it is very difficult to assess the extent of potential loss; there is no loss experience to aid an evaluation. Therefore, rating and pricing these risks is highly challenging. It may be that damage from a particular risk is already occurring, but the time delay before its effects are noticeable and measurable is so great that insurers cannot make a proper assessment until years later.

Asbestos is a near-perfect example: the insurance industry did not realize the scope of the risk posed by asbestos soon enough and is now paying a commensurately high price. Emerging risks can also have a potential for loss accumulation and/or serial loss, as well as global and multi-line implications. Therefore, when emerging risks finally do materialize, their effects can be dramatic and may even threaten a company's solvency.

3 Driving forces behind emerging risks

Emerging risks appear with changes in the risk universe. The risk universe is expanding ever faster due to several driving forces, factors, and trends related to developments in the technological, societal, economic, and legal arenas. Among these forces are the following:

- **Technological developments** lead to innovation and create many business opportunities and the possibility of great economic wealth. However, every technology has its downside potential too, which can be triggered, for example, by design and development errors as well as by application errors.

5 Christian Lahnstein, 'Wie gehen Versicherer mit emerging risks um?' *Börsen-Zeitung*, February 2006, p. 1.

- Changes in **social behavior** have consequences for the risk universe. For example, people now generally live longer due to better medicines. This development has consequences for the life insurance industry. Stress at work and at home has increased, leading to greater consumption of fast food and convenience food, which may very well have implications for the health insurance industry.
- Globalization has had a huge effect on **economic development**. Global trade is rapidly expanding, creating increasing risk potential: loss potential becomes very great when people, value, and infrastructure become highly concentrated. The pursuit of economic wealth is accompanied by a higher degree of vulnerability and extreme loss potentials due to the complexity and interconnectedness of the modern economic system.[6]
- The risk universe can also be fundamentally changed by changes in the **legal framework**. New laws, unexpected court decisions, and the changing interpretation of laws can all change a risk from one that was formerly rather well known to one of suddenly alarming proportions. For the insurance industry, especially relevant developments include changes in liability law, damages law, procedural law, and insurance law.[7]

In summary, the risk universe is subject to many forces of change, and everything seems to move faster. This has some real and serious consequences for the risk universe:

- Complexity, uncertainty, and ambiguity increase.
- Conditions change more rapidly.
- Increasing vulnerability with respect to technological, social, and natural risks.

6 Matthias Haller, 'Erübrigt sich angesichts der Globalisierung der Risiko-Dialog?' in Peter Gomez, Günter Müller-Stewens, and Johannes Rüegg-Stürm (eds.), *Entwicklungsperspektiven einer integrierten Managementlehre* (Bern: Haupt, 1999), pp. 99ff.

7 A good overview of liability trends and developments is found in Tom Baker, 'Insuring Liability Risks', *The Geneva Papers on Risk and Insurance*, 29 (January 2004), pp. 87–106.

- Risks are difficult to discover and assess and often manifest themselves before adequate preparations can be made.
- Damage potential is bigger, possibly even catastrophic.
- The risks have linked physical, social, and economic effects.

4 Consequences for the insurance sector

An insurance company's business model generally consists of accumulating money (premiums) by agreeing in advance to pay financial compensation to the policyholder if a pre-specified uncertain event occurs. The fixed payments the insurer agrees to make are often uncertain in their scope and timing.[8] Emerging trends, developments, and changes in the risk universe can have an enormous impact on the insurance business:

- Policies can span decades (e.g., life insurance policies); thus, intervening events or issues can have consequences that were completely unforeseen at the time the policy was written.
- Over time, general trends and developments can become emerging risks and, possibly, actually manifest themselves as risks even later. This process may be very slow and the level of uncertainty very high. Often, it is hard to discover, let alone evaluate, these risks.
- Obviously, insurance companies do not have extensive (or even any) loss statistics for emerging risks. This is a challenge because the traditional method of setting rates is based on statistical data.
- Another problem is that emerging risks are often already covered by the insurance portfolio because, previously, they were not known to be emerging risks or, indeed, any sort of risk at all. Nevertheless, claims associated with these risks have to be paid, even though the premiums paid for them are now known to be inadequate.

8 Swiss Re, *The Risk Landscape of the Future* (2004), p. 7 <http://www.swissre.com>, accessed 8 August 2007.

- For emerging risks, causation, as well as the actual consequences for the insurer, may not be clearly defined. In particular, causal relationships cannot always be verified.
- Even after emerging risks have been identified and evaluated, their actual effect on the insurer is still difficult to ascertain with any degree of certainty. Which of the risks will materialize? Which of the risks will have the most significant consequences for the insurer? What is the probability of occurrence? How quickly will the risk materialize?
- Emerging risks of global scope – such as pandemics – can have extreme consequences for the insurance industry, especially when different geographic regions, many industries, or several insurance lines of businesses are exposed to a single risk. In this situation, one of the fundamental principles of the insurance business – diversification – will be of no use at all and may even aggravate the situation.

To successfully overcome these challenges, insurers need an effective way of dealing with emerging risks. An early-warning system is a good start, and can help insurers avoid risks, reduce surprise, and win a little extra time for planning and implementing appropriate action. An early-warning system starts with the basic premise that in reality, emerging risks are not complete surprises – it is usually possible to detect a "weak signal" of an emerging development. These weak signals need to be anticipated, analyzed, and evaluated so that appropriate communication, mitigation, and product development measures can be taken. In the insurance industry, such early-warning systems are widely used, but are rarely formalized or standardized. A more systematic approach to early detection and the handling of new trends and developments could be of great benefit to insurers:

- It may prevent surprises: anticipation of imminent developments can promote action and solutions in advance, leading to stability and protection of the balance sheet, thus helping to maximize shareholder value.

- It provides more time for strategic maneuvers: an insurer who has had time for thorough planning and implementation of countermeasures against hazardous risks will gain a competitive advantage, because the company will have been able to take advantage of new opportunities in terms of relevant and timely products and services.
- It can lead to more effective, more efficient management. In particular, if a standardized procedure is in place to deal with emerging risks, resources can be used most efficiently; knowledge can be processed and managed, instead of being relegated to a "data dump"; information can be transmitted quickly and appropriately to partners and customers; duplication of effort will be avoided – in short, the firm will be working at peak efficiency to deal with the emerging risk, thus ensuring its survival, possibly even its increased prosperity.

5 Empirical examination of systematic handling of emerging risks in the insurance industry

This study focuses on how the insurance industry deals with emerging risks. The research framework is illustrated in Figure 1 (on p. 162). First, the organizational dimension of handling emerging risks was analyzed. Second, the processes of managing emerging risks were examined, including the identification, analysis, evaluation, and implementation of emerging risks in the insurance business. The third step consisted of looking at the systems, tools, and information technology chosen for managing emerging risks. Last, but not least, the cultural aspects of managing emerging risks were explored.

The empirical analysis is based on a thorough examination of four companies in the insurance industry: two insurance and two reinsurance companies. The analysis was based on expert interviews. Since there is very little literature covering these topics, the analysis is descriptive. The following sections detail results from the data analysis.

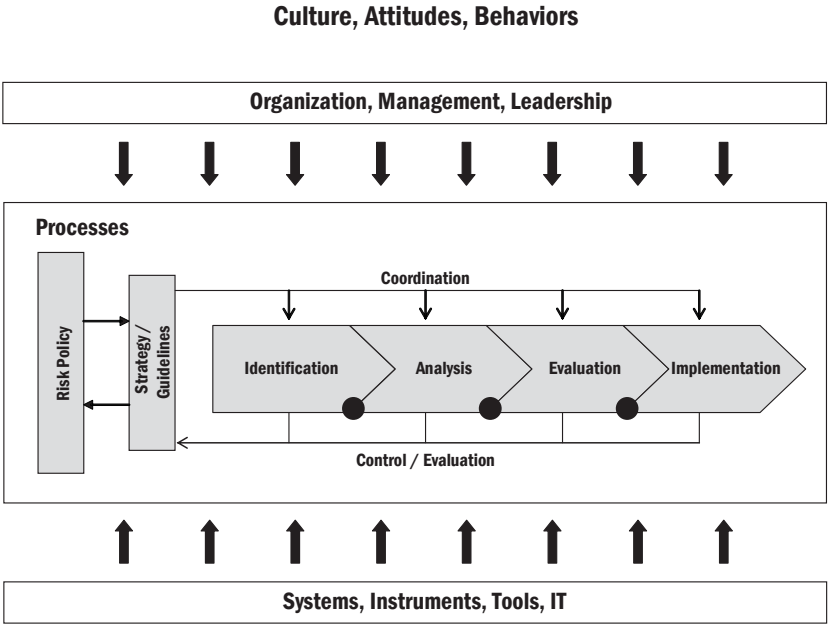


Figure 1: Research framework

5.1 Organization of emerging risk management in the insurance industry

The majority of the examined firms use a structured and coordinated approach. In all four firms, there is a high-ranking committee (e.g., the group risk committee, the group underwriting committee, etc.) or single person (e.g., the chief risk officer, the group chief underwriting officer, etc.) that sets the strategy and issues guidelines for managing emerging risks.

Within the boundaries of the strategy, the units responsible for overall business operations work to detect emerging risk signals early on and implement the insights derived from analysis and evaluation of emerging risks into their business units/countries. The firms' emerging risk management activities are usually coordinated via a centralized project team/department or, alternatively, the responsibility is decentralized through an internal network at the business-unit level.

The majority of the examined firms analyze the implications of emerging risks not only at a business-unit level, but also holistically. They use models to analyze the effects of certain potential threats on the firm's assets and liabilities and implement countermeasures as soon as feasible. The responsibility for those measures is distributed in various ways; sometimes, it lies with the emerging risk management team, sometimes with the department of the chief risk officer, and so forth.

All the project teams responsible for managing emerging risks are interdisciplinary and heterogeneous, thus combining different cultural and functional backgrounds, geographic regions, and expertise, which facilitates a global and holistic view of emerging risks.

Some of the firms have a very structured and formalized process for managing emerging risks. The workflows are defined, every process step is clearly documented, and competencies are specified. There are clear personal/time guidelines and control/reporting procedures that enable top management to view the actual emerging risk landscape at all times. At other firms, the process of managing emerging risks is deliberately less structured, with more leeway allowed in searching for the best organizational solution on a case-by-case basis. The information flows are still structured, but there is room for "customized" solutions. Some insurance firms have no formalized or holistic early-warning systems for detecting emerging risks, but this does not mean that these firms are not concerned with the issue.

In summary, there appears to be a general trend in the insurance industry toward network-based early-detection systems for emerging risks (see Figure 2 on p. 164). All the examined firms use internal and external personal networks to gather information regarding emerging risks. The personal networks converge on a "big radar screen" that covers the entire emerging risk landscape.

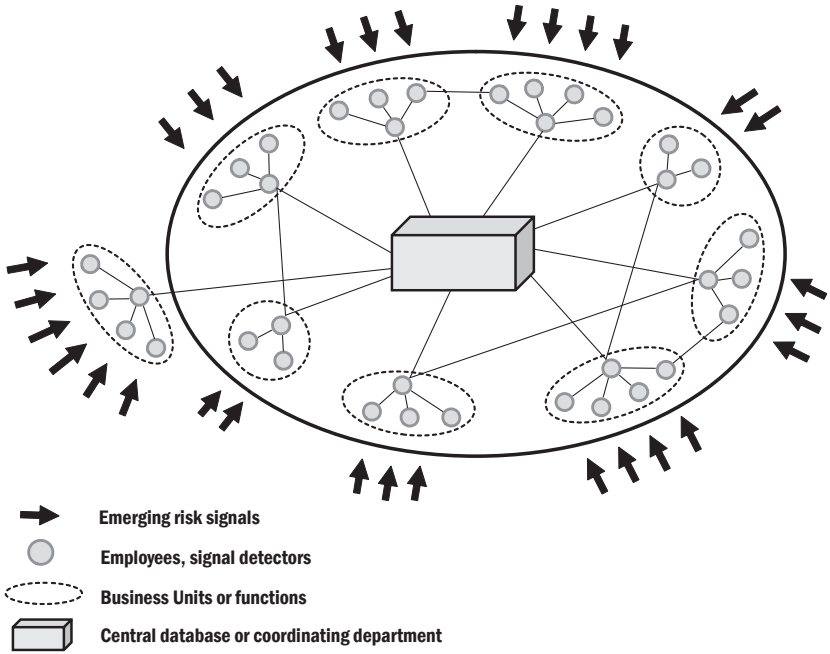


Figure 2: Network-based early-warning system for emerging risks

5.2 Processes of emerging risk management in the insurance industry

Detection and identification of emerging risks

Analysis of the case studies shows very clearly that the identification of emerging risks is based on many inputs from many different sources:

- All the examined firms state that a **broad employee base** is integrated in the process of identifying new risks. These employees are a valuable source of information, as they are generally very experienced in the insurance field and have day-to-day contact with the market and customers, thus putting them on the front line for picking up signals of new risks.
- Some firms deploy **specific groups** for the management of emerging risks, thus centrally coordinating identification activities. The

firm might create an interdisciplinary team for this task consisting of employees from different departments, who, in addition to their "normal" job, are, so to speak, integrated into the group.

- All firms have established specific channels for **involving customers** in the process of identifying emerging risks, e.g., customer feedback possibilities, customer dialog programs, or special events.
- Information regarding future risks is also provided by **industrial bodies** such as the Chief Risk Officer Emerging Risks Initiative.[9]
- It is striking that all firms purchase external knowledge and know-how through **cooperation with external experts**. The extent of this cooperation varies, however.

Analysis of emerging risks

The degree to which insurers are affected by the issues that have been identified varies. Therefore, an assessment of whether the company is likely to be affected by the emerging risk needs to be carried out in an initial **screening process**. The basis of the screening process is often an unevaluated list of all emerging risks.

The companies employ diverse **tools, methods, and aids** in the scientific analysis of emerging risks. Most of the firms examined work with watchlists to which they add all emerging risks to be analyzed. They also constantly update the list with new information. This produces an overview of relevant and less relevant risks. One of the examined firms also links its watchlist to a risk radar, resulting in a graphic representation of all emerging risks.

As the **result of this analytical process,** all the firms create a position paper in which all the information is presented in a condensed form and fully formulated. This paper is usually divided into three parts: a *neutral* section containing scientific background information, a *risk-oriented*

9 This initiative is a good example of an industry-shared early-warning system serving the needs of a number of firms. As part of the initiative, the firms meet periodically and exchange information about newly identified risks, including the presentation of position papers reflecting their current opinions. See <http://www.croforum.org/emergingrisc.ecp>.

section, setting out firm-specific relevance as well as the impact on the industry more generally, and, finally, a *recommendations* section, which makes proposals for the future handling of the emerging risk and serves as the foundation for further decisionmaking. One company additionally records each emerging risk in a progress database, transparently indicating the status of the risk, previous work done, implemented solutions, and expert opinions solicited.

The process of analyzing emerging risks can be very intensive in terms of time and resources used, and the utility of the end results are often uncertain, as no one knows exactly if, when, or how an emerging risk will become a reality. The risks are thus monitored and reevaluated whenever new facts, reactions, or information become available. In some cases, this may stretch over a period of years or even decades, for example, if a new technology emerges that seems very promising, but for which it is not yet known where and how it will be used, what sort of danger it might give rise to, and so forth. However, the analysis of emerging risks is a crucial step toward understanding the nature of the risk, and possibly crucial for the future of the firm, and much depends on the quality of the analysis.

Evaluation and quantification of emerging risks

It is necessary to separate out those emerging risks that represent the greatest and most damaging impact. The basis for this sorting is careful qualitative and, if possible, quantitative assessment. All the companies examined regard this step as very important, since it is the foundation for further measures. Moreover, it focuses complete attention and all resources on a few individual risks.

The assessment of the company's exposure to an emerging risk is a difficult task that is generally made on the basis of expert knowledge, knowledge of the market, long-term professional experience, and gut feeling. Usually, experts from the departments of underwriting, product development, claims management, the legal department, and risk management are consulted.

With regard to **relevance determination**, a large number of criteria are considered. The following is a list of criteria most often considered in emerging risk assessment.

- Driver of the risk (natural hazards; technological, social, political, or economic developments).
- Type of damage (environmental, personal, assets, financial resources).
- Damage potential (of the individual business units and/or the entire portfolio), cumulative damage potential, serial damage potential.
- Probability of occurrence.
- Latency period of the occurrence.
- Affected lines of business, countries, and insurance classes.
- Demonstrability.
- Coverage aspects.
- Potential to be influenced.
- Awareness of the risk by competitors, customers, and society.

Various filter criteria are used at different levels of the organization. At the business-lines level, insurance criteria tend to be applied, whereas at the company level, both insurance and strategic aspects, such as cumulative damage potential, risk to the firm's financial stability, and robustness of the strategy in light of the emerging risk, are considered.

The companies often illustrate the potential threat of a risk by using graphical, symbolic, or mathematical **tools**. In the mathematical system, a figure is assigned to each evaluation criterion. Adding up the figures produces a sum that in itself is not very informative, but when examined in the context of the whole emerging risk portfolio makes possible an objective comparison. Using a traffic-light system to sort the risks (red, orange, or green) provides a simple, yet effective, guide to the urgency of the emerging risk. Another type of risk assessment consists in listing different concepts and grading them according to their level of severity.

Charting the estimated effect thus creates a profile for each emerging risk, which can be compared with other profiles. Classic risk maps, of the type long used in risk management, are also common. So-called cobweb diagrams, where, for example, six criteria are represented, are also used. The concepts are distributed in the diagram and provided with an axis, resulting in different gradations, with the middle corresponding to a low value and the values increasing toward the edges. The emerging risks are then inserted, together with the related points of intersection, creating a surface that indicates a visible exposure trend.

Operational and strategic measures

Transferring the results from the analysis and evaluation of the emerging risks to the operational divisions, to product development, and to risk management is a major step in managing emerging risks.

In the area of **risk control**, specific measures can be taken at two levels: insurance measures at the business-lines level; portfolio/strategy-oriented measures at the whole-company level. The insurance measures that can be implemented are quite similar across all four of the studied firms, and include the following:

- Adjustment of contractual terms taking into account the new risk situation (higher retentions, lower limits for the risk, limitation of the amounts covered, change of the trigger of "loss occurring" to "claims made," specific formulations for exclusions).
- Charging additional premiums for taking on the greater risk.
- Offering repurchase possibilities with conditions that better reflect the risk situation.
- Alteration of the target market or target product strategy; in extreme cases, exit from a market or withdrawal of the product.
- Better risk segmentation of customers.
- Sending out newsletters or bulletins to make the policyholders aware of the risk.

- Improving customer risk management.
- Developing and introducing group-wide best-practice applications and underwriting methods so that the risks are better evaluated and quantified and an appropriate price calculated.

Some of the examined companies look at emerging risks in relation to the whole portfolio and the overall strategy of the company. Reinsurers are especially concerned with protecting themselves against cumulative and latent risks. In this respect, all companies emphasize that they want to avoid unpredictable, ruinous cumulative claims. This is why they all believe that cumulative control is one of the important functions in general risk management.

All the companies stress the importance of **product development** in relation to emerging risks. Only two companies, however, systematically link the risks examined to potential market opportunities. These departments have the responsibility to develop and implement products before their competitors do. However, this is far from easy. Rating – a subject emphasized by all four companies – is a major challenge. As no data, no statistics, and only limited experience exist, the exposure rating must be used as the basis for premium calculation. Calculating the necessary reserve capital for emerging risks is also problematic. A further challenge has to do with uncertain market acceptance. If entry into the market with a new set of products (e.g., exclusion of a risk with the simultaneous possibility of repurchase by means of a new product) occurs too early, there is a high probability that the product will not achieve the desired level of market acceptance. Thus, most insurers emphasize that product development aimed at controlling emerging risks will meet with success only if customers and regulatory bodies are involved in the problem-solving process.

In addition to the insurance measures and those taken at the overall-portfolio level, insurers can also counteract emerging risks through the use of **internal information measures** (e.g., policy guidelines for underwriters, underwriting warnings, distribution of position papers), training measures (integration of the emerging risks in training, hold-

ing workshops, presentations at employee events), and consulting and communication measures (e-mail, person-to-personal, publications, a database, an intranet). All these methods educate employees on how to handle these topics on an everyday basis or explain how they can access more information.

Only two of the companies studied have a system for **systematic controlling/reporting** of the measures being taken in regard to emerging risks. In both firms, the market departments keep a record of the measures taken, and the measures are checked regularly and systematically to gauge effects. On the basis of this, the measures are either retained, abolished, tightened up, or watered down. In one company, the emerging risks are also incorporated into the annual risk report, which lays out the risk landscape for the management board.

A crucial component of successfully introducing new products and new risk management measures is **external communication**. In this context, the companies all emphasize that every effort must be made to maintain a dialog with customers, authorities, regulatory agencies, investors, and other stakeholders. Timely communication is essential to maintaining the risk dialog with stakeholders and actively influencing opinion. This is another area where all four companies have the same goal, but approach it from different avenues. The many methods of external communication employed include: publishing in various formats (academic journals, specialist and other magazines, newspapers, the internet, etc.); presentations at seminars, workshops, meetings, or conferences; workshops and bilateral talks on individual emerging risks; interfacing with the media on topics of concern; and lobbying at the national level.

5.3 Information systems to support the management of emerging risks

Various tools are employed in support of the management of emerging risks and the operations undertaken in response to them. There are also systems for the recording, administration, and communication of such risks.

Two of the studied companies use central databases in an effort to simplify the management of emerging risks. In addition to the database,

the firms maintain pages on their intranets that are devoted to emerging risks. These pages primarily serve information and communication functions. Sophisticated technical research tools that automatically browse the internet for information are not broadly employed yet by the insurance companies we studied.

In short, current technology is not being fully exploited yet, and a great deal of reliance is placed on personal networks. Although this is a workable system, to be effective, a network structure is required within the company, and employees need to know who is responsible for dealing with emerging risks.

5.4 Future-oriented risk culture

The organizational culture is of great significance in the context of emerging risks. All the companies examined emphasize that cultural values within the firm are crucial to the successful operation of an early-warning system for emerging risks. One of the most important determining factors here – according to the companies examined – is an open risk culture within the company and accordingly appropriate treatment of stakeholders. All the companies emphasize that risk is their main business and that, therefore, the proactive and farsighted handling of this "raw material" is of great importance. Handling emerging risks in a professional and efficient manner is seen as an integral part of the business, sometimes even to the extent of determining its sustainability.

Another important factor in firmly embedding the early-warning system within the company is that the system must be promoted as being of high importance. In each of the companies studied here, high-level personnel actively promote emerging risks as an important challenge. The involvement of top-level management in the topic is seen as essential by many of our interviewees. In the absence of such high-level interest, the management of emerging risks is relegated to the periphery, which could lead to a dangerous situation.

Despite the active support of top management, the companies have found it difficult to involve the desired (i.e., the maximum) number of employees in the emerging risk process. Financial incentives have failed

at several firms, and these firms are now exploring other incentives in an attempt to involve as many employees as possible in the process. Some methods being tried include encouraging the recognition of employees' diligence by third parties, involving employees in the production of publications, listing productive employees on the intranet, and so forth. There are some employees who participate in the early-warning process simply out of a personal interest. In the case of decision-makers and those employees closely integrated in the emerging risk process, three of the firms have set out concerns about emerging risks as part of a target agreement process, and participants are evaluated on the basis of performance.

To make sure that information about emerging risks is disseminated across the entire organization, the companies regularly hold internal briefings, dispatch e-mails to interested persons, place information on the intranet, and exchange information personally or via internal brochures. Formal and informal networks are believed to be of great importance in this context. However, once again, the four companies display a wide range of behavior in this regard: one of the firms packs as many topics about emerging risk as possible into workshops, meetings, "knowledge fairs", or further training seminars; other companies do nothing of this nature.

The firms' openness toward new topics is made obvious by the way they distribute information externally. All the companies are extremely open in sharing knowledge they have gained about emerging risks. To this end, they send out publications and provide briefings on their own internet pages. Moreover, they regularly participate in stakeholder dialogs, appear at events, and hold workshops, meetings, and conferences. All the companies have their own methods of presenting research results to the public and engaging in the exchange of opinion. And, as previously mentioned, each of the four companies cooperates in various initiatives, and each is a member of the Chief Risk Officer Forum Emerging Risk Initiative.

From the cultural perspective, however, there are still many hurdles to overcome in dealing with emerging risks. Some representatives of

the insurance sector say that their companies are characterized by adoption of a short-to-medium term view of business; long-term issues are not a priority. A similar phenomenon can be found in the case of non-measurables, a category that certainly includes emerging risk. Senior management often has but one question: "What is the monetary benefit?" However, the greatest achievement of a good early-warning management system is the prevention of as many kinds of damage as possible. Unfortunately, phenomena that have *not* happened are very hard to value in monetary terms. This is why some companies cannot even imagine instituting an emerging risk department – such a department does not bring money *in*, it only(!) prevents money from going *out*. A further obstacle to the institution of a successful early-warning system arises from the "silo" way of thinking that takes place in some companies, meaning that they are reluctant, or unable due to the corporate culture, to share knowledge, either between their own departments, or with "outsiders" (i.e., policyholders). This is a case where short-term security measures can result in long-term vulnerability.

6 Conclusions

Emerging risks may have great damage potential, are hard to observe, and are difficult to manage. A proactive handling of such risks is therefore crucial for insurance companies. In this study, we have examined four firms doing business in the insurance sector. Our main focus was on the organization, the process, the supporting systems, and the cultural aspects of handling emerging risks.

The study revealed that in the insurance industry, emerging risks are increasingly viewed as an integral part of the risk landscape. The fact that all four of the examined firms employ dedicated staff for the management of emerging risks is evidence that insurance companies have changed their attitude toward risk management from one of "wait and see" to an actively future-oriented approach.

The operational management of emerging risks offers many challenges. To be successful, insurance companies need to establish an effective early-warning system to detect, monitor, analyze, and evaluate future risks. Reliance on many risk experts, both inside and outside the company, is necessary. However, it is only when the findings are translated into action – risk control, communication, and product development measures – that danger will be avoided. Risk control measures can often be implemented very quickly, and damage can thus be minimized; taking advantage of opportunities revealed by a new risk situation, and thus profiting in a substantial way from the early-warning system, takes a little more time.

When an early-warning system fails, it is often the case that the fault lies not with "hard factors" such as processes, systems, and structures, but with "soft factors" such as behaviors, attitudes, and other cultural aspects. Transforming employees into effective elements of an early-warning system takes time and effort, and it is essential that top-level managers demonstrate in a very tangible way how important such work is. One step in this direction is to integrate emerging risk topics into as many contexts as possible – internal presentations, trainings, workshops, talks, and so forth – until the very concept of emerging risk becomes an integral part of every employee's functioning. When this occurs, accompanied by appropriate methods of educating and informing stakeholders as well, the company will be viewed as a competent, credible, far-sighted, and caring insurer – all of which can only add to its prosperity.

SWISS RE POLITICAL COUNTRY RISK RATING

Marco Lier

With the presentation of a political country risk rating database, this contribution describes a part of political risk management in a multinational company. This rating is an additional tool for assessing the overall risk quality of transactions, and it has become part of the wider risk assessment that often encompasses other ratings or quantitative parts. The rating is a pragmatic and – despite all its inherent shortcomings and simplifications – a very useful and time-efficient tool supporting daily business decisions, especially for transactions in emerging markets or for specialized business dealing with political risk.

The political country risk rating database is calculated on the basis of 24 outside indicators, most of them compiled by international organizations, think-tanks, or universities. The weighting of the 24 indicators varies according to certain aspects of different business contexts. In an additional step, the indicators are transformed into an "intensity rating". This reflects the fact that a rating in an insurance context should not only rank the countries according to the relative degree of inherent risk (of doing insurance business there), but also allow to compare the risk in a certain country compared to another one, or to give an approximate indication of the probability of an insurance-relevant event occurring.

1 Introduction

This contribution describes political risk analysis in the risk management context of a multinational company. Political risk analysis appears in many forms in this context, and one of them, Swiss Re's proprietary political country risk rating database, will be described more comprehensively in this chapter. The political country risk rating is an additional tool for assessing the overall risk quality of certain transactions, and the rating format is particularly useful for business practitioners (in an insurance context, "underwriters") when they are assessing a transaction and deciding whether to proceed with it or not. Other aspects of transactions are frequently also assessed through a rating or a similar quantitative method.

2 Organizational setup

Swiss Re is the world's largest reinsurance company with about 10'000 employees and nearly 30 billion CHF premiums earned in 2006, and operates on a global basis. Its main markets premium-wise are still OECD countries, although emerging markets are catching up fast. The Political Risk Management unit is part of the risk management function and reports to the chief risk officer, who is a senior member of the executive board. Among its diverse tasks, an important one is the assessment of country risk for certain business transactions with political risk aspects, mainly for business in emerging markets. Swiss Re has developed a political country risk rating database in order to make this assessment more efficient, auditable, and comparable over time. The setup and use of this database will be described in more detail in the following.

3 Rationale of the political country risk rating database

As indicated above, the aim of the country risk assessments and country risk ratings is to give underwriters a short and quantitative assessment of the country risk for a certain transaction. They take the country rating into account as part of a transaction's overall context and as an additional consideration among other aspects, which include, for instance, a transaction's financial viability and pricing, technical (risk management) considerations, the client relationship, and regulatory and compliance constraints. The political country risk input is, of course, much more important in an emerging market context than in stable OECD countries.

The political country risk rating should only map (and possibly also serve as an early-warning system for) country risk aspects that are relevant to the insurance business, and not replicate a general political risk rating. Although several country ratings and rankings are available from international institutions, think-tanks, and universities, all of them focus on certain aspects, and none of them offers a rating tailor-made for our purpose. This is why Swiss Re decided to build a customized rating system that can be adapted for different purposes. In our setup, there is currently one overall rating (which also functions as a repository for all inputs that can be selected for different focuses) and two specialized ratings, which are used for more narrowly defined applications:

- A rating for the specialized line of business "political risk insurance" (PRI), which is a niche market covering such political perils as expropriation, currency inconvertibility, or contract frustration. These are perils related to trade and investment, and as such are not covered by the main insurance lines. The trigger for insurance losses in this case are usually discriminatory government actions affecting a company doing business in a foreign jurisdiction.
- A sustainability-focused rating, which is used for assessing the risk to a company's reputation stemming from business operations in certain countries. The sustainability rating is an important step in the process of identifying such countries for further qualitative assessment.

4 How the rating works

Swiss Re has developed and refined the political country risk rating database according to the following steps:

1. **Selection of 24 indicators:** From the many political rankings and ratings that have sprung up in the past few years and have been released as part of the public domain or for commercial purposes, 24 ratings were selected as outside input for the rating. The selection was made according to different criteria: First, they should rate an important aspect of the political risk landscape that is relevant for doing (insurance) business. Second, they have to cover the majority of countries.[1] Third, the input has to be quantitative and comparable over time and between countries.[2] Fourth, the rating has to be made by a respected and independent institution and be updated regularly in a consistent manner. In practice, these four criteria are not always fulfilled completely and are at times even contradictory; therefore, the selection had to be pragmatic and consider the ratings most useful for the purpose. Most of the selected outside input is compiled by international organizations, think-tanks, or universities, but some is also supplied by private organizations (such as the Corruption Perceptions Index by Transparency International) or private risk consultancies (Control Risks Group). The selected input is grouped together for aspects such as stability and security or governance issues, and covers aspects such as a government's regulatory quality, the UN's Human Development Index, civil liberties, or expropriation risk.
2. **Conversion into a single scaling system:** As the outside indicators come in very different forms (e.g., in a rating scale from A to E, or from 0–100, or from -2.5 to +2.5), the indicator value has to be converted into a single scale of 1–10.

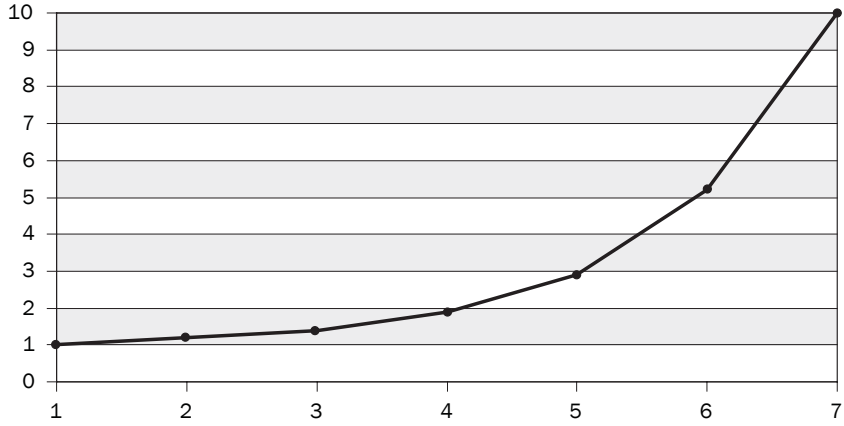
1 Some ratings and assessments would give good insights for some aspects, e.g. the Bertelsmann Transformation Index, but have not been comprehensive enough for the rating which should cover as many countries as possible.

2 Reports on the human right situation of countries by Human Rights Watch or Amnesty International for instance might be very valuable and comprehensive but they cannot be translated easy enough into a quantitative rating.

3. **The big difference to other ratings:** the "intensity value". As the first application of the political country risk rating was intended for political risk insurance (PRI), a specialized line of business rooted in commerce-related credit insurance, we tried to replicate the notion of credit risk ratings, which indicate the probability of default for a rated company (or country in the case of sovereign risk ratings). In analogy to a credit risk rating, our rating should indicate the probability of a PRI-relevant incident happening (e.g., expropriation, currency inconvertibility, contract frustration) – and additionally, it should not only indicate in which country the risk of doing a specified business is higher than in another one (i.e., establish a ranking), but also to give an indication of the degree of how much higher the risk is in a certain country compared to another one. This additional aspect is important for calculating the probability of an incident or insurance loss happening, and thus for setting the risk appetite and underwriting capacity per country. However, this notion of relative propensity to risk has not been considered by any of the outside political ratings, which give no indication as to how much the probability increases from one risk bracket[3] to the next higher one. Thus, in the further construction of our political country risk rating, we used an analogy based on credit risk rating: in the best case, political ratings have a sample of only about 200 countries stretching back for 10–20 years. Credit ratings, on the other hand, have been used and refined since about 100 years, and they have a sample experience of several millions of data entries. Therefore, they can quantify relatively accurately how much higher the default risk of a company is compared to other companies. In other words, country ratings can give an exact probability of an incident happening for every rating bracket. This can be plotted on to an exponential graph of the rated companies' default probability, meaning that the probability of an incident increases in

3 A risk bracket is a group of countries with a similar risk rating: e.g., a rating from 0 to 100 can be divided into ten brackets, with every rating between 20 and 29.9 falling into the same bracket.

much bigger increments from rating bracket to rating bracket than a linear increase, which is implicitly used in most other ratings.



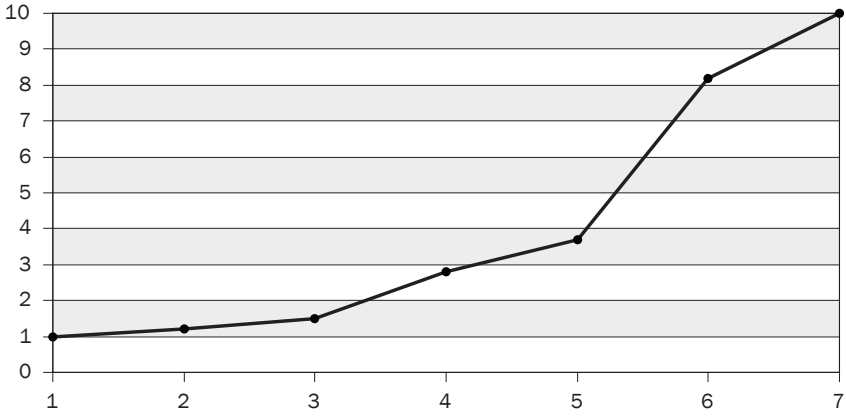
Graph 1: exponential curve as used in credit risk rating, translated into the rating scale of the political country risk rating

x-axis: 7 rating brackets of the input rating

y-axis: 10 rating brackets of the final rating

In order to reach a comparable statement for our political country risk rating, we tried to emulate this experience and setup of the credit rating with an "intensity approach". In this step, we drew curves, based on analogy and our expert judgment, for every single indicator. We took the country rankings of the 24 indicators and created seven rating brackets for each indicator,[4] then decided on where to draw the line between different groups of countries and estimated how big the difference between these groups was, focusing on the probability of an event occurring. This assessment resulted in different shapes of the graphs for the 24 indicators: most of these were not exponential, unlike the credit risk rating model, but they were clearly shaped differently than a simple linear increase of the probability, which is the implicit norm in most other rating systems.

4 The scale of seven is quite often used and offers good accuracy without pretending to deliver results with a degree of exactness that does not reflect reality.



Graph 2: example of the intensity graph created for one of the outside indicators

first row and x-axis: indicator value

second row and y-axis: intensity value

third row: increase from the value of one rating bracket to the next

Through this step, we received for every indicator value (1–7) a related "intensity value" from 1–10, which is used for the further calculating of the rating.[5]

4. **Weighting of the indicators:** In order to measure different aspects in different ratings, the weight of the 24 indicators can be changed accordingly. Indicators not used for a certain rating are assigned a value of 0. Currently, three different ratings for different purposes have been established. According to the selected weighting of the indicators, the database calculates the final rating; the result always lies between 1 and 10.

5. **Conversion into a letter rating:** The numerical rating between 1 and 10 is then converted again into a simplified letter rating with ten equally distributed steps – in analogy to the rating used by Standard

5 The scale has to begin at 1, and not 0, in order to indicate the increase in percentage from one rating bucket to the next or the relation of a country's susceptibility to political risk compared to another one.

& Poor's credit risk rating – in order to underline the similarity to credit risk and for comparability with other ratings used by business practitioners.

PCR2 and Sustainability		
Intensity		Rating
from	to	
1	1.9	AAA
1.91	2.8	AA
2.81	3.7	A
3.71	4.6	BBB
4.61	5.5	BB
5.51	6.4	B
6.41	7.3	CCC
7.31	8.2	CC
8.21	9.1	C
9.11	10	D

Table 1: Mapping of intensity ratings to letter ratings

5 Impact on decision-making

This political country risk rating database has a pragmatic setup. At the same time, it is accurate and comprehensive enough to capture important aspects of political risk in about 220 countries and non-sovereign entities. Its application in daily business is time-efficient, the database is updated every quarter and offers the possibility to include a manual override (i.e., to upgrade or downgrade a country) based on expert judgment, e.g., when the outside indicators do not yet reflect recent events and developments or when original input data is not comprehensive enough.

The political country risk rating database is more of a risk management tool than a way of detecting emerging (political) risks. As far as

emerging *political* risks in a narrow sense are concerned, the Political Risk Management unit deals with them in another process (which cannot be described in this contribution in more detail). Emerging risks in a *broader sense,* which could have an impact on Swiss Re or insurance operations in general (e.g., risks associated with nanotechnology or electromagnetic fields), are treated by a neighboring team. Based on a network with representatives from all risk areas throughout the company, this unit coordinates the systematic identification, assessment, and evaluation of emerging risks at the company level as well as the translation of findings into business practices (e.g., exposure management through adjusted underwriting guidelines, product development, and communication).

The political country risk rating is primarily used for PRI business, where it is established as a binding risk management tool and relevant for setting capacities per country. In many other lines of business, the rating represents one among several factors to be taken into account by an underwriter considering a transaction. The rating's impact on daily business decisions is stronger for transactions in emerging markets or when it comes to specialized lines of business with very specific requests, and less pronounced in routine business. Nevertheless, it is a clear improvement for risk management compared to the tools available several years ago, when awareness of political risk was less widespread and political risk was only dealt with in a haphazard, less consistent way. In this sense, Swiss Re's risk management has been broadened and deepened by the application of the political country risk rating.

FINANCIAL AND INSURANCE BUSINESSES

POLITICAL RISK AND PUBLIC POLICY MANAGEMENT AT CREDIT SUISSE

René P. Buholzer and Manuel Rybach

Using the example of public policy management at Credit Suisse, a globally active financial services company based in Switzerland, the authors argue that there is a dual rationale – based on regulation and reputation – for a professional, specialized in-house political risk and public policy management function at internationally active firms. The article then lays out the issue management process at Credit Suisse. In analogy to commonly used risk management terminology, according to which risk management is divided into the three steps of risk identification, risk analysis, and risk response, Credit Suisse uses a three-level process, distinguishing between the phases of monitoring, assessment, and lobbying, to deal with political risk and public policy issues likely to impact the firm. There is also a formal Reputational Risk Review Process to manage and mitigate reputational risk. The authors conclude by touching upon critical success factors of effective public policy management, such as the need for firm representatives to speak with one voice on major policy matters globally.

1 Introduction

In the spring of 2005, a group of environmental activists positioned big, inflatable whales in front of the Credit Suisse global headquarters building at Paradeplatz in Zurich, the bank's US headquarters on Madison Avenue in New York, and the representative office in Moscow. Attracting considerable media attention, the activists used the whales – together with signboards and leaflets handed out to passers-by – to protest against the fact that Credit Suisse served as financial advisor to Sakhalin Energy (SEIC), the world's largest integrated oil and gas project. Environmentalists criticized that the project endangers the habitat of the last western grey whales off Sakhalin Island off the eastern coast of Russia.

This example of non-governmental organization (NGO) activism highlights some of the issues that will be discussed in this article. The protest graphically illustrates that the terms of the debate on political risk and public policy issues have changed dramatically in recent years.[1] Firstly, the political decisionmaking process is becoming increasingly heterogeneous, exposed to a constantly changing environment of different networks. Consequently, the management of political issues is no longer restricted to the executive and legislative branches of government. Rather, a growing number of non-governmental intermediaries and groups demand attention as well. Secondly, the expanding nature of the state in providing regulation and social welfare increases the number of individuals and companies that are affected by political decisions – positively, through the entitlement of benefits, or negatively, through redistribution and restrictions of their freedom. Thirdly, the world today is characterized by growing specialization and division of labor. The resulting complexity renders a sound judgment of political risks more difficult. Finally, the increasing internationalization of all actors (states, firms, and NGOs, as well as individuals) improves cross-

1 Concerning terminology, reference is made not only to "political risk" and "political risk management", but also "public policy issues" and "issue management" as well as "public policy management". As understood in this article, these terms basically refer to the same concepts, and they will often be used interchangeably.

border cooperation and means that political decisions are integrated into a multi-level decisionmaking system.[2]

In this context, large and internationally active financial institutions, in particular those with a broad private and/or retail banking client base, face a dual challenge: on the one hand, they have to respond to traditional public policy challenges, such as anticipating, analyzing, and, if needed, effecting changes in their regulatory environment or mitigating their impact, which is eminently important in a highly regulated industry such as banking. On the other hand, banks with international operations are increasingly in the spotlight of a critical public and the media, and must ultimately protect and enhance their reputation in order to secure their operating license.

Against this background, this article uses the example of public policy management at Credit Suisse, a globally active financial services company based in Switzerland,[3] to, firstly, argue that there is a two-pronged rationale – based on both regulation and reputation – for a professional, specialized in-house political risk and public policy management function at large, internationally active financial services providers. The second part of the article outlines the three-level issue and public policy management process at Credit Suisse, distinguishing between the phases of

2 Buholzer, René P., 'Herausforderungen und Lösungsansätze der politischen Unternehmenskommunikation im internationalisierten Umfeld', in Otfried Jarren, Dominik Lachenmeier, and Adrian Steiner (eds.), *Entgrenzte Demokratie? Herausforderungen für die politische Interessenvermittlung* (Baden-Baden: Nomos, 2007), p. 203.

3 Credit Suisse Group is a leading global financial services company headquartered in Zurich, Switzerland. As an integrated global bank, Credit Suisse provides its clients with investment banking, private banking, and asset management services worldwide. Founded in 1856, Credit Suisse is active in over 50 countries and employs approximately 47'000 people from over 100 different nationalities. Credit Suisse Group's registered shares are listed in Switzerland and, in the form of American Depositary Shares, in New York.

monitoring, assessment, and lobbying.[4] Thirdly, critical success factors of effective public policy management are identified in the form of concluding remarks.

2 Regulation and reputation: the two-pronged rationale for political risk and public policy management in international banking

2.1 Regulation

As an important financial market participant, Credit Suisse has a keen interest in ensuring that the economic policy framework in the bank's key markets is sound. A fundamental objective of Credit Suisse's activities in the area of political risk and public policy management is therefore to contribute to a competitive, pro-business policy environment that is conducive to economic growth, vibrant capital markets, and a proportionate regulatory framework for financial services providers.[5]

As regards the regulatory environment, there are several challenges for globally active banks today. A prosperous financial market that functions well requires sound regulation as well as competent, effective, and efficient supervision. Both firms and supervisors have a strong, shared interest in developing and maintaining an effective set of relationships that support

4 This article addresses neither "classical" risk management issues at banks as they relate to, e.g., market, credit, operational, or liquidity risks, nor corporate communication-related crisis management. A treatment of emerging market and country risk analysis functions is also beyond the scope of this article. On political and country risks in international banking, see, e.g., Fight, Andrew, *Understanding International Bank Risk* (Chichester: John Wiley and Sons, 2004), chapter 6; Moran, Theodore H., *Managing International Political Risk* (Malden: Blackwell Publishers, 1998). On political risks in banking more generally, see, e.g., Denk, Christoph L., *Politische Risiken für Banken: Charakter, Typologie, Management* (Berne: Haupt, 2003). On political risk analysis more generally, see, e.g., Ruloff, Dieter and Daniel Frei, *Handbuch der weltpolitischen Analyse: Methoden für Praxis, Beratung und Forschung* (Chur: Rüegger, 1984).

5 The need for business-friendly operating conditions goes beyond banking regulation and supervision and covers policy areas such as social, taxation, competition, infrastructure, and foreign trade policy. As this is the case for all corporations, this section focuses on issues that are of specific relevance to banks.

a growing and competitive economy, ensure financial system stability and security, and serve customers' best interests. The fundamental requirement for a certain amount of regulation, therefore, cannot be denied, as highlighted by the benefits brought about by a solid framework of regulation and supervision of financial institutions and markets. Also, there is no doubt that security and stability are fundamental prerequisites for the sound operation of any top-level financial center.

The other side of the coin, however, is the cost at which these benefits should be acquired.[6] Indeed, getting the priorities right in regulation and supervision is a topic that is right at the top of the agenda for financial services providers in every major market. To that end, bankers and their regulators and supervisors should engage in a proactive regulatory dialog and should ideally be guided by principles that foster a meaningful and proportionate regulatory framework. Recently, much thought has been given to such principles of "better regulation".[7] Such guidelines, which are observed by an increasing number of regulatory bodies worldwide,[8]

6 An example: According to a study by the Swiss Banking Institute of the University of Zurich, the total cost of regulation to banks in Switzerland amounted to an average of 4.5 per cent of all expenditures, which equates to close to 13'000 Swiss francs per employee. The number of full-time jobs in the compliance area of Swiss banks has, on average, more than tripled in the period 1998 to 2002. See Geiger, Hans and Ivo Hubli, *Regulatory Burden: Die Kosten der Regulierung von Vermögensverwaltungsbanken in der Schweiz*, Swiss Banking Institute of the University of Zurich, Working Paper No. 37 (Zurich, 2004) <http://www.isb.uzh.ch/publikationen/workingpapers.php>, accessed 4 September 2007.

7 See, e.g., International Council of Securities Associations, ICSA, *Principles for Better Regulation* (New York, 2006); Swiss Federal Finance Administration, Swiss Federal Banking Commission, and Swiss Federal Office of Private Insurance, *Guidelines for Financial Market Regulation: The Requirements for a Reasonable, Cost-Conscious and Effective Regulation of the Financial Market* (Berne: SFBL, 2005).

8 In the European Union (EU), promising developments are taking place under the heading of the EU's "better regulation" initiative. In March 2005, the European Commission proposed a better regulation package, which aims at cutting red tape by amending or withdrawing altogether EU laws which prove to be excessive. Also, the important role that impact assessments can play in limiting the cost of regulation has been acknowledged. In the area of financial services, the change of regulatory culture brought about mainly by Internal Market Commissioner Charlie McCreevy has put greater emphasis not only on impact assessments, but also on extended consultation, which is performed in line with the so-called Lamfalussy Process. In addition, the Commission is trying to prevent member states from "gold plating" when they implement EU directives into national law and to ensure consistent, coherent, and timely implementation and application of European rules.

stipulate that regulation should be envisaged only in case of market failure, require that cost-benefit analyses be performed, and demand that regulation and supervision be proportionate and differentiated. In addition, regulation should be enshrined in principles that allow for flexibility to adapt to the rapidly changing nature of financial markets and products rather than in strict and overly prescriptive rules. The "better regulation" philosophy also leaves enough room for self-regulation, where appropriate, and calls for prior consultation with the recipients of the regulation (i.e. the financial services industry), an open and active dialog throughout the whole process, and realistic implementation deadlines.

Regulatory issues, which already constitute a demanding task at the national level, become even more challenging at the cross-border and international levels. As a result of the rapid globalization and evolution of the financial sector, the complexity of the regulatory landscape has increased dramatically over the last decades. Internationally active banks are subject to countless different – and at times diverging – rules and regulations and have to meet reporting requirements stipulated not only by their home supervisor, but also additional host supervisors. For global financial institutions, internationally consistent rules are of paramount importance.[9] Much work needs to be done in this area, and the global banking industry is actively looking for solutions.[10] The coherence and consistency of international regulation, often lacking, has to be promoted through the more widespread application of the principle of mutual recognition of equivalent rules and regulatory dialogs among the major jurisdictions, including, but not limited to, the US, the EU, Japan, and Switzerland as well as key emerging markets such as the BRIC countries (Brazil, Russia, India, and China). Finally, cooperation is needed not only among the various rule-setting bodies, but also among

9 See, e.g., on the issue of varying national implementation strategies of the international capital adequacy standard Basel II, Bischofberger, Alois and Manuel Rybach, 'Basel II: Bedenken sind erlaubt', *Neue Zürcher Zeitung*, 29 July 2003, p. 23.

10 See, e.g., Institute of International Finance, IFF, *Proposal for a Strategic Dialogue on Effective Regulation* (Washington, D.C., 2006).

the authorities supervising the same financial institution if it operates in several jurisdictions.[11]

2.2 Reputation

Prompted by growing – real or alleged – corporate misbehavior across the past years, stakeholder opinion of corporations has declined and mistrust has become more widespread. Examples of such corporate misbehavior include financial and executive malfeasance as well as operational failure and errors in personal judgments – underscoring that threats to corporate reputation can come from virtually anywhere and can affect any type of company or industry.

One key implication of this credibility deficit has been intensified scrutiny from stakeholders. Several factors are contributing to this trend. Media attention has increased significantly in the past few years. At the same time, regulations are opening companies up to a level of scrutiny that would not have been possible some years ago. Finally, the internet has brought about a quantum leap in the speed at which news is spread across the globe. The amount of information available on company misdeeds is sensitizing stakeholders to corporate misconduct, and their sensitivity

11 In the case of Credit Suisse, the Swiss Federal Banking Commission (EBK) serves as home supervisor and has been practicing a supervisory approach to prudential supervision similar to the so-called lead supervisor regime advocated by industry groups such as the European Financial Services Round Table (EFR). This has been carried out by implementing, on a trilateral basis, a "college of supervisors" with the US Federal Reserve and the UK Financial Services Authority (FSA), given the significance of Credit Suisse's operations in these two foreign jurisdictions in relation to its overall operations. This is a good example of international supervisory coordination, but much more could and should be done.

is causing them to seek more information (and subsequently become more disgruntled). A vicious cycle is under way.[12]

It should come as no surprise, therefore, that most practitioners of risk and public policy management at financial institutions agree that protecting the integrity of a firm's reputation is of paramount importance.

Empirical research by the Reputation Institute has identified seven key drivers influencing a firm's reputation. While some of these drivers are more closely related to the business activity as such (innovation, products/services, leadership, performance), others deal with broader aspects of corporate behavior (workplace, governance, citizenship).[13] All drivers have in common that they both have the potential to enhance or damage the reputation of a company.

Therefore, structures and procedures need to be in place to, firstly, manage reputational risks, and, secondly, to communicate a firm's efforts and achievements and to reach out to the relevant stakeholders (see figure 1 on p. 193). For this dialog to be sustainable, it has to avoid exaggerated promises and must provide a consistent and objective picture.

12 Dissatisfied stakeholders of all types – customers, business partners, employees, communities – can certainly dampen corporate success, but the stakeholder group that draws corporate attention most quickly is the financial community. A review of the frequency of "stock shocks" in the US – defined as a 30 per cent drop in a firm's weekly share price relative to the S&P 500 index – underscores this point. The number of companies that have experienced such shocks has increased fivefold in the last five years, according to research of the Corporate Executive Board. Of course, only a portion of these share shocks were related to the reputation of the companies in question. Still, it should be noted that the financial community today punishes companies more severely – and more permanently – than in the past. In short, scrutiny is up, credibility is down, and financial punishment is increasingly severe. Corporate Executive Board, *Refocusing Reputational Management* (London / Washington, D.C., 2005), pp. 4ff.

13 See also Fombrun, Charles J. and Cees B.M. Van Riel, *Fame and Fortune: How Successful Companies Build Winning Reputations* (Upper Saddle River: Financial Times Prentice Hall, 2004). On reputation management in the context of corporate communications, including best practice examples, see also Van Riel, Cees B.M and Charles J. Fombrun, *Essentials of Corporate Communication* (New York: Routledge, 2007).

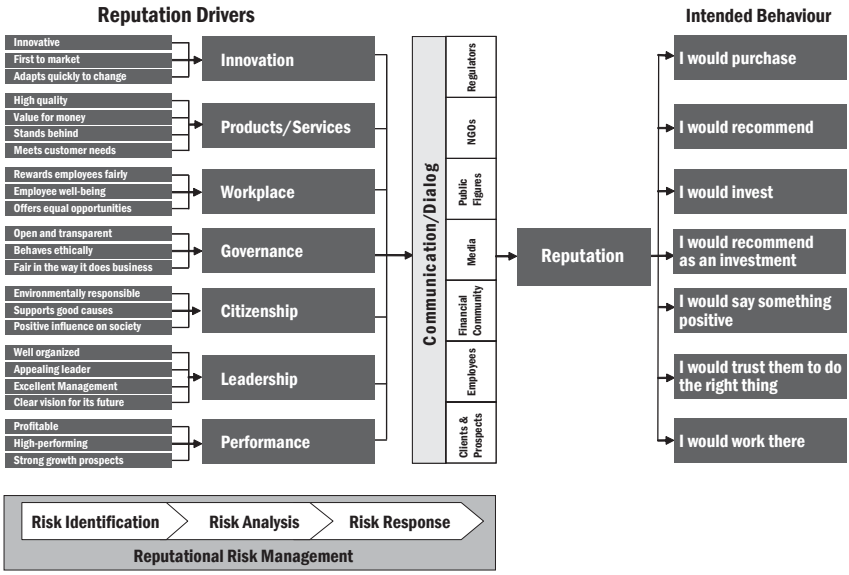


Figure 1: Reputation: drivers, management, dialog

Source: Buholzer/Rybach adapted from Reputation Institute 2007

The benefits of a good reputation are tangible for financial services providers by enhancing client goodwill, helping to recruit, motivate and thus retain key employees, creating a favorable perception by supervisors and supporting a good rating agency status. By contrast, years of client goodwill can be lost through a single bad event that is widely reported. Consequently, protecting and enhancing the reputation of the bank is one of the three main guiding principles of Credit Suisse, the other two being client centricity and teamwork.

As regards the protection of its reputation, Credit Suisse faces three challenges, in particular. Firstly, as a bank with a large private and retail banking client base, the bank is more vulnerable, for example, to orchestrated NGO campaigns that call for client boycotts than a brokerage boutique catering to a few wealthy clients only. Secondly, as a globally active bank that constantly strives to reduce its cost base, it is susceptible to criticism concerning outsourcing and offshoring efforts. Indeed,

similar to other global players and contrary to domestic firms, Credit Suisse may have to weather the "popular backlash against globalization", which is caused by increasing concern – if not outright hostility – over the liberalization and integration of world markets.[14] NGOs, growing in numbers and importance, are both drivers and products of this backlash. As witnessed by the coordinated efforts in the context of Sakhalin briefly referred to at the beginning of this article, NGOs increasingly operate on a global basis, using international networks for their progressively professional campaigns. Thirdly, companies, including banks, are increasingly held responsible by a critical public for the compliance of their suppliers as well as clients with human rights, environmental, and other sustainability-related matters, a trend which could be referred to as "up- and downstream corporate responsibility".

3 Monitoring – assessment – lobbying: three-level process of issue and public policy management

With regulation and reputation identified as the two main challenges for public policy management for globally active banks, the next section of this article briefly outlines the process according to which issue management is handled at Credit Suisse.[15] In analogy to commonly used risk management terminology, according to which risk management is divided into the three steps of risk identification, risk analysis, and risk response, Credit Suisse, in its issue management, uses a three-level process, distinguishing between

14 For a discussion of this popular backlash against globalization, in particular in the trade policy context, see Rybach, Manuel, *Linking Labor Rights and Trade: Assessing the Clinton Administration's Policy in Multilateral Fora* (Bamberg: Difo, 2001), chapter 4.2.

15 For a practicable definition of issue(s) management, see, e.g., Cutlip, Scott M., Allen H. Center, and Glen M. Broom, *Effective Public Relations* (Englewood Cliffs: Prentice Hall, 1994), p. 16, as cited in Bentele, Günter and Daniela Rutsch, 'Issues Management in Unternehmen', in Ulrike Röttger (ed.), *Issues Management: Theoretische Konzepte und Praktische Umsetzung. Eine Bestandsaufnahme* (Wiesbaden: Westdeutscher Verlag, 2001), p. 146: "Issues management is the proactive process of anticipating, identifying, evaluating and responding to public policy issues that affect organisations and their publics."

the phases of monitoring, assessment, and lobbying to deal with political risk and public policy issues that are likely to impact the firm.[16]
The Public Policy department, which handles issue management at the bank globally, has teams in all four regions of the world in which the bank operates: Switzerland, the bank's home market, the Americas, Asia-Pacific, and Europe/Middle East/Africa (EMEA). This ensures global coverage of issues, an invaluable advantage given the increasing significance of the bank's international activities.

3.1 Monitoring

Any political risk and public policy issue management must be grounded in the continuous observation of politically relevant developments and their background. The scope of the responsibilities of a public policy or issue management unit determines the breadth of issues that need to be covered. In the case of Public Policy at Credit Suisse, coverage includes a broad range of issues, including societal, political, legislative, regulatory, and sustainability-related trends and developments, with the geographical focus lying on the bank's key markets.

A wide range of methods such as environmental scanning (both with methods developed in-house and by using specialized external providers supplying state-of-the-art reputational risk assessment tools, for example) and sources should be used during this stage. Possible sources include general and industry-specific publications and newsletters as well as issue-specific websites, in particular those run by NGOs. Information and analysis is also available from trade associations, specialized political risk analysis or public policy consultancies, peers, the executive and legislative branches of governments, political parties, embassy and foreign service personnel, international organizations, academic experts and think tanks, and NGOs. It is fair to say that valuable information can be gathered in the monitoring stage from all (political) stakeholders who may be the target of lobbying efforts later in the process. The

16 For a more detailed treatment of such a three level approach, see Buholzer, René P., *Legislatives Lobbying in der Europäischen Union: Ein Konzept für Interessengruppen* (Berne/Stuttgart/Vienna: Haupt, 1998), pp. 42–9.

value added by the public policy function at this stage in the process stems from its ability to screen, verify, and prioritize the large amount of information gathered and to determine its relevance for the bank by checking it against the bank's strategy and activities.

3.2 Assessment

Once identified, political risk management and public policy issues are assessed by both qualitative (structured and unstructured) and, to a lesser degree, quantitative methods. Examples of methods used include brainstorming, scenario and SWOT analysis, and the use of expert judgment (including from external sources, such as think tanks and consultancies, where appropriate).

Importantly, the assessment phase culminates in structured issue reporting in the form of standardized "Public Policy Issue Reporting Sheets". These documents are widely used internally by other shared services functions such as corporate communications as well as business departments and top management. They succinctly describe key facts of a given social, political, legislative, regulatory, or sustainability-related issue or development, point out its relevance to the bank, and, most importantly, lay out the official Credit Suisse policy position on the issue. This position has been elaborated by Public Policy, working together with other internal experts from departments such as, e.g., legal and compliance, tax, economic research, and the relevant representatives of Credit Suisse business departments. Issues of greater significance – or cases where different business entities within the bank may have diverging views – are presented to top management for sign-off or for a final decision.

While the process outlined above relates to "classical" political risk or public policy issues, for example emanating from legislative or regulatory initiatives, the assessment phase looks different in the case of reputation

risk.[17] Here, Credit Suisse has established a formal Reputational Risk Review Process (RRRP), underscoring the great importance of this risk category for the bank. The process functions both as a bottom-up process (all employees must follow the corresponding internal Reputational Risk Policy and raise issues as they encounter them, which should ensure wide transaction capture) and in a top-down manner (senior reputational risk approvers, independent of the business/front offices, located in all four regions and covering all divisions of the bank, ensure a consistent approach, which is ultimately ensured by Executive Board oversight). While the RRRP is inherently – and inevitably – judgmental, it still represents a serious, systematic, and consistent approach that can help manage and mitigate reputational risk at a globally active bank. The process is not just about rejecting unsuitable transactions. Rather, in many cases transactions can be approved if modified and improved, e.g., through additional disclosure. Such a differentiated approach, complemented by training efforts, raises internal awareness of reputational risk and ultimately increases the quality of the bank's business judgment. The growing number of transactions/cases fed into the process reflects rising levels of awareness. It should also be noted that these internal rules on reputational risk, which apply to all transactions and are complemented by sector-specific guidelines for particularly sensitive industries such as forestry, are in addition to legal constraints, as stipulated by laws and regulations. The ultimate objective of this approach is to embed reputational risk management considerations in the decision-making processes of line/business management, enabled by experts departments such as Public Policy. Such an approach further aligns line behavior with the firm's strategy of dealing with, inter alia, political risks.

17 Reputational risk can be caused by actions or transactions that could involve controversial clients (e.g., politically exposed persons, PEP) and/or business activities, conflicts of interest, tax, accounting or regulatory implications, and adverse environmental or sustainability implications. Other potential sources of reputational risk relate to more business-driven aspects, e.g., the quality/performance and appropriateness of a financial product, the quality of advice, or fees.

3.3 Lobbying

Once a unified position that is applicable across all divisions and regions of the bank has been defined, lobbying efforts can be undertaken, if deemed necessary and appropriate. Credit Suisse is engaged in a regular, ongoing dialog with various public policy stakeholders (such as parliamentarians, political party staff, government and administration officials, NGOs, ambassadors, international organizations, etc.). The Public Policy department, which is responsible for managing this dialog as well as for the administration of key institutional memberships of the bank, e.g., in think tanks, can thus resort to a solid network of contacts to relevant stakeholders and decision-makers that has already been established before a given issue calls for advocacy efforts. In the case of NGOs, this pro-active dialog also helps to understand civil society priorities and emerging trends in NGO activism, which in turn serves as an important early-warning mechanism. The same holds true for the dialog with political parties.

More often than not, direct lobbying activities are complemented by political advocacy efforts through trade associations and similar institutionalized avenues of influence, which serve as multipliers and a means to reinforce the message that has to be delivered to political decision-makers. In this context, consistency is crucial. In order to highlight the importance of Credit Suisse speaking with one voice across trade associations globally, Public Policy has conceived an annual global town hall meeting of key trade association representatives of the bank.[18] Credit Suisse is represented in the boards of several trade associations. In the bank's home market, this holds true, most notably, for the Swiss Bankers Association, the Swiss Business Federation (economiesuisse), and the Confederation of Swiss Employers. Internationally, Credit Suisse is represented, inter alia, at the European Financial Services Round Table, Businesseurope,

18 In addition to the bank's trade association mandate holders, Public Policy also supports the more than 250 employees of Credit Suisse in Switzerland who have been publicly elected to office and hold a political mandate – a peculiarity of the Swiss "militia" political system, whereby politicians hold their office on an extra-official basis. Even though these mandate holders exercise their mandate independently and without any instruction from Credit Suisse, they are "political ambassadors" of the bank and are thus supported by Public Policy in various ways, including by an annual meeting, which serves as a capacity-building and networking platform.

the American Chamber of Commerce to the European Union, the Securities Industry and Financial Markets Association, the Institute of International Finance, the Business and Industry Advisory Committee to the OECD, and the International Chamber of Commerce. Moreover, the bank's specialists are actively contributing to the work of numerous trade association committees and working groups and participate in the consultative process for new legislation. Credit Suisse also actively cooperates with international business organizations such as the World Economic Forum (WEF), of which the bank is a strategic partner.

In terms of the subject-matter of advocacy, the substance as well as the depth and sophistication of the information used obviously depends on the issue at hand and varies greatly from stakeholder to stakeholder. However, there are some key messages that inform all of Credit Suisse's interactions in the arena of public policy:

1. **Free markets:** supporting the objective of open capital markets that allow and foster competitiveness and supporting the principle of non-discriminatory access to markets
2. **Better regulation:** advocating the adoption of "better regulation" principles, as outlined above, stressing, in particular, the need for international coordination and consistency
3. **Privacy:** underscoring that privacy, including in financial matters, is a basic right and a hallmark of free societies
4. **Competition:** insisting that competition will increase efficiency, including in fiscal matters.

In addition, when interacting with political stakeholders, Credit Suisse regularly notes its manifold contributions to society, particularly pronounced in the Swiss home market, as a financial intermediary (benefiting consumers, companies and investors by increasing innovation and choice), employer, provider of education (apprenticeships, in-firm education), tax payer and buyer of goods and services, sponsor of cultural activities and sports and with philanthropic and volunteering activities. Furthermore, in an effort to improve the quality of regulation, the bank's expertise is frequently sought

by policy makers on a broad range of issues relating to banking, financial products, sales and trading, and taxation, to name but a few.

4 Concluding remarks: success factors for effective public policy management

The world is becoming flat. Different values, cultures, and perceptions are intersecting. In this increasingly heterogenous environment, a professional handling of political risks and a specialized issue management function are critical success factors for businesses, allowing companies to react adequately to the rapidly changing developments in their political and regulatory environment.

At Credit Suisse, Public Policy supports the business objectives of the bank by professionalizing and effectively managing the bank's interface with the political realm, broadly conceived. Public Policy actively engages in a pro-active and honest dialog with all key political stakeholders, e.g. parliamentarians, government and administration officials, international organizations, NGOs, and business, in particular the financial community, both via trade associations and directly. This enables the bank to contribute to the policy debates that shape its regulatory environment and to protect and foster its reputation among key stakeholders. Public Policy further ensures that Credit Suisse has a unified position on key public policy issues and that its representatives speak with one voice on major policy matters globally. Policy positions and important policy developments are reported regularly to top management and to key internal stakeholders.

In turn, effective public policy management on a global scale requires efficient cooperation and a spirit of teamwork between public policy experts with specialist know-how of their respective markets and regions. Also, coordination of message delivery to a growing number of actors and across all avenues of influence has to be ensured. To that effect, solid, long-term relationships based on mutual respect, trust, honesty, and reliability with all relevant partners and stakeholders need to be established.

Finally, close alignment of public policy efforts with the firm's strategy as well as an active involvement of top management is essential for the good performance of a Public Policy function. By focusing not only on risk, but also on opportunities (such as, in the case of banks, financial products relating to socially responsible investment, climate change, and microfinance, for example), Public Policy, if managed properly, provides not only important monitoring, analysis, and lobbying services, but can also contribute to the company's success.

CONCLUSIONS

CURRENT PRACTICES AND FUTURE CHALLENGES OF RISK ANALYSIS AND MANAGEMENT

Beat Habegger

The articles presented in this volume provided insights into a variety of professional practices related to risk analysis and management. They explored a broad diversity of topical issues and conceptual approaches, and convincingly demonstrated that the increasing complexity and rapid change in the world have brought the notion of risk to the center of many debates in public policy and the corporate world. Some of the discussed problems or challenges are particular to a specific institutional context. Others, however, cut across conventional sectoral or functional boundaries and provide evidence that risk is a conceptual tool that powerfully connects issues and institutions hitherto perceived as being quite distant from one another. The early identification, adequate assessment, and appropriate mitigation of risks have apparently become decisive requirements for effective and successful policymaking in public and private governance.

This concluding chapter begins by highlighting some key aspects that are mentioned in most articles and are therefore of special relevance when assessing current practices of risk analysis and management. The first section refers to the changed international environment that forces institutions and analysts to adapt adequately to altered circumstances when thinking

about, planning for, and coping with emerging risks and threats. The second section restates the central premise of risk management and outlines selected issues drawn from the contributions in this volume with regard to risk identification, assessment, and mitigation. The text then adopts a more future-oriented perspective by showing in the third section what strategies different actors in politics and business have developed for addressing emerging risks. The fourth and final section focuses on the individual analyst by emphasizing six central tasks that may lead to better tailored and more effective strategic responses to risk governance challenges. It concludes with a short summary.

1 A changing international environment

A common strand in all articles is the diagnosis that the international environment is changing. The increasing use of the risk concept in the domain of security policy, for instance, is due to the altered security situation after the end of the Cold War when it became increasingly difficult to identify hostile actors, their intentions, and the damage they can potentially inflict upon others. Because the threats are diffuse and the shape and evolution of security challenges are near-unpredictable, the concept of risk is well-suited as a tool for explaining the state and dynamic of a radically transformed security landscape.[1] This insight apparently necessitated new approaches to public policy management. It is thus not surprising that the civil defense organizations of Germany, Sweden, and Switzerland have all profoundly changed over the last decade by shifting their focus in terms of which risks are important and imminent and by adapting their doctrine, concept, and organization.

This adjustment process and the related debate about emerging political risks and public policy issues took place simulataneously in such diverse

1 For an overview, see Bailes, Alyson J.K., 'Introduction: A World of Risk', in Stockholm International Peace Research Institute, *SIPRI Yearbook 2007: Armaments, Disarmament and International Security* (Stockholm: SIPRI, 2007), pp. 1–20; Coker, Christopher, *Globalisation and Insecurity in the Twenty-first Century: NATO and the Management of Risk, Adelphi Paper 345* (Oxford: Oxford University Press, 2002).

areas as financial businesses or the armed forces. An important aspect in this regard is the increasing internationalization of policy-making that forced all actors to abandon an exclusively national perspective and to consider their strengths, weaknesses, opportunities, and threats in view of international trends and developments. It is evident that the emergence of systemic risks, which are often global in origin and have an impact that transcends national borders, demand more international cooperation and better coordination among all actors involved, within and across territorial boundaries, in order to effectively counter arising threats.

2 Key issues in risk analysis and management

The central premise of risk management remains the same throughout all articles: the need for early detection and adequate assessment of upcoming issues 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 more reactive sense, it intends to prevent surprises that may negatively affect envisaged (institutional) objectives; in a rather proactive sense, it aims to preserve and enhance the margin for strategic maneuvers in order to better realize envisaged objectives. Beyond the affirmation of this overall objective of risk analysis and management as outlined in the introduction, the different chapters point to a number of aspects that are specific to the three key phases of an ideal risk management process.

In terms of *risk identification*, institutions perceive risks differently, not necessarily because they face different risks, but due to their varying vulnerability assessments. While it is evident that institutions and actors are confronted with the same basic risk landscape, 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 perceives itself as being affected by it. This vulnerability assessment, 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 states and societies from aggression 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. As a result, it is obvious that the vulnerability assessments and thus the risk management perspective of public policy institutions differ from those of private companies.

In the context of *risk assessment*, the focus is on risk prioritization in particular. Insurance companies specifically target unpredictable, ruinous cumulative claims and therefore focus on risks with a high cumulation potential that may lead to ruinous damages. Such a clear setting of priorities might be easier to implement for private companies than for public actors, 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, conversely, more stakeholders are usually involved, all of whom have specific expectations and insist on covering "their" risks: 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 refering to an often vaguely defined public duty, even if the costs for mitigation vastly exceed the potential benefits.

With regard to *risk mitigation*, an intriguing result is that public policy institutions often resort to issuing new laws or regulations when they design preventative or precautionary measures, 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 government-induced regulatory changes in order 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. Such outcomes, apart from once again illustrating the importance of adequately assessing who is affected by what risks to what extent, also underline that risk mitigation measures may not have the intended effect or they may even unfold

unexpected consequences – including the opposite of those desired – in areas or sectors that were not targeted by the measures.

3 Strategic responses in business and politics

The increased attention to risk management and the development of long-term, forward-thinking strategies underline the efforts of many actors in politics and business to adapt to a changing risk landscape over the last decade. In business, the scope of actively managed risks has been broadened significantly from a quite narrow view of operational, financial, or credit risks to a large spectrum of risks – including social, political, or environmental risks – that may all have an impact on business activities. In 1993, for instance, GE Capital, a global financial services firm, was the first to create the position of a "Chief Risk Officer" (CRO) in order to analyze and manage the risks the company faces in a more comprehensive way. Today, the position of CRO is an institutionalized position in many companies across a large variety of business sectors.

At the governmental level, three reports serve to illustrate the trend towards more emphasis on foresight and risk management: the US National Intelligence Council in 2004 published a report entitled "Mapping the Global Future" that takes a long-term view of how global trends might develop and influence the world by the year 2020.[2] The Development, Concepts and Doctrine Centre within the British Ministry of Defence published a (regularly updated) similar study in 2006 in the form of an independent assessment of the strategic context until 2036.[3] Similarly, the Finnish Ministry of Defence in 2006 issued an assessment of the long-term

2 US National Intelligence Council, *Mapping the Global Future: Report of the National Intelligence Council's 2020 Project* (Pittsburgh: Government Printing Office, 2004) <http://www.dni.gov/nic/NIC_2020_project.html>, accessed 15 November 2007.

3 UK Development, Concept and Doctrine Centre, *The DCDC Global Strategic Trends Programme 2007–2036* (Swindon: DCDC, 2006) <http://www.dcdc-strategictrends.org.uk/viewdoc.aspx?doc=1>, accessed 15 November 2007.

developments future strategic challenges in Finland's security environment up to the year 2025.[4]

At the global level, government agencies and non-governmental organizations alike have also contributed to this growing trend: the Organisation for Economic Co-Operation and Development (OECD) released a study on "Emerging Risks in the 21st Century" in 2003,[5] which identified the most pressing challenges in public risk management and was followed by an OECD Futures Project on Risk Management Policies.[6] The World Economic Forum (WEF) in 2004 founded a "Global Risk Network" in response to the concerns of the global (business) community about difficulties in responding adequately to a changing risk situation.[7] In 2003, finally, the International Risk Governance Council (IRGC) was established as an independent organization of risk experts from government, industry, and academia with the aim of improving the anticipation and governance of global systemic risks that affect human health and safety, the environment, the economy, and society at large.[8]

4 The way forward: six central tasks for risk analysts

The changing state of risk apparently evokes the need for a more future-oriented, strategic approach in public and private governance, and the chapters collected in this volume strongly underline this argument. However, the question remains what needs to be done in the future in order to make better use of the full potential of knowledge and expertise of risk analysts – of

4 Finnish Ministry of Defence, *Securely into the Future: Ministry of Defence Strategy 2025* (Helsinki: Ministry of Defence, 2006) <http://defmin.fi/index.phtml?l=en&s=318>, accessed 15 November 2007.

5 OECD, *Emerging Systemic Risks in the 21st Century: An Agenda for Action* (Paris: OECD, 2003).

6 For more information, see the website of the OECD Futures Project on Risk Management Policies <http://www.oecd.org/department/0,3355,en_2649_35014780_1_1_1_1_1,00.html>, accessed 15 November 2007.

7 For more information, see the website of the World Economic Forum's Global Risk Network <http://www.weforum.org/en/initiatives/globalrisk/index.htm>, accessed 15 November 2007.

8 For more information, see the website of the International Risk Governance Council <http://www.irgc.org>, accessed 15 November 2007.

which this book provides strong evidence – and to support decision-makers even more effectively in adequately coping with emerging risks. In the following, six central tasks of risk analysts are identified as propositions for the possible future shape of risk analysis and management.

The *first task* of risk analysts is to develop a nuanced understanding of risks, of the risk landscape, and of the risk management process as such. To begin with, they should understand the essential elements of the risk concept as well as the various concrete risks that are relevant to a particular institution. Furthermore, they should 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.

The *second task* of risk analysts is to recognize that dealing with risks means dealing with the future and to acknowledge that there is always a variety of possible futures. This insight implies that analysts and decision-makers alike must learn to think in terms of alternatives, or more precisely, in terms of alternative futures. Risk experts are not assigned to predict the future, because no one can know it, and it is misleading to pretend to. The job of risk experts is rather to imagine a multiplicity of futures in order to "help policy-makers think about the future" and to "deal with heightened uncertainty by presenting alternative scenarios".[9] They must confront decision-makers with the reality of complexity and uncertainty, while aiming at reducing both to a degree that allows the formulation of meaningful policy recommendations.

The *third task* consequently is to discern uncertainty as a matter of degree. Unfortunately, uncertainty is often perceived in a binary way: the world is either assumed to be certain and its future course open to precise prediction, or it is seen as uncertain and therefore completely unpredictable. Both views are wrong and fatal for risk management: underestimat-

9 Nye, Jr., Joseph S., 'Peering into the Future', *Foreign Affairs*, 73/4 (1994), pp. 82–93, at pp. 88 and 93. Cf. also Minx, Eckard and Ewald Böhlke, 'Denken in alternativen Zukünften', *Internationale Politik* (December 2006), pp. 14–22.

ing uncertainty leads to strategies that do not defend against probable threats, while assuming unpredictability leads decision-makers to abandon analytical rigor, to rely on their "gut instinct", and to forego effective risk management.[10] 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.[11] A certain amount of "residual uncertainty", which corresponds to the "residual risk" as described in the introductory chapter on risk mitigation, may remain, though, even if the best analysis is done.

The *fourth task* of risk analysts, then, is to use a sophisticated understanding of different levels of uncertainty in order to propose appropriate strategic responses and to tailor the methodological tools adequately. We can distinguish at least four levels of uncertainty, for which different strategic and methodological choices can be derived (see Figure 1 on p. 211):[12]

- *A clear-enough future:* the future can be predicted to a degree that is sufficiently clear to allow straightforward strategic answers. A prominent example would be the forecast of demographic trends. Traditional tools like trend analyses, which forecast future outcomes based on historical results, may lead to reliable results.
- *Alternate futures:* a few clearly distinguishable alternate outcomes or discrete scenarios can be observed. We know that one of these will occur, but we do not know which one. Often it is possible to assign probabilities to the different possible outcomes. A classic example is a presidential election: we know that one candidate will win, but it is uncertain which one. In this case, tools for decision analysis (for example, in the form of decision trees) or the development of scenarios for different outcomes may be helpful.

10 Courtney, Hugh, Jane Kirkland, and Patrick Viguerie, 'Strategy under Uncertainty', *Harvard Business Review* (November–December 1997), pp. 67–97, at pp. 68f.

11 Courtney, Kirkland, and Viguerie, 'Strategy under Uncertainty', pp. 68f.

12 For the following, cf. ibid., pp. 69–73.

- *A range of futures:* a multiplicity of potential futures exists, but no concrete final outcomes can be depicted. The range is defined by a few variables, but the actual outcome may lie anywhere along a continuum bounded by that range. An example is the design of future laws and regulations. In terms of methods, analysts need to develop a number of scenarios, focusing on trigger events and offering a broad and distinct risk picture. The set of scenarios should account for the probable, not the entire possible range of outcomes.
- *True ambiguity:* uncertainty in all dimensions creates an environment that is virtually impossible to predict. Neither definite final outcomes nor even ranges of possible outcomes can be identified. So much uncertainty is rare, and experience shows that it tends to drift to another level over time. True ambiguity can be typical for major historical turning points such as the end of the Cold War. The best that analysts can do is to look very hard for variables that may give hints as to future developments.

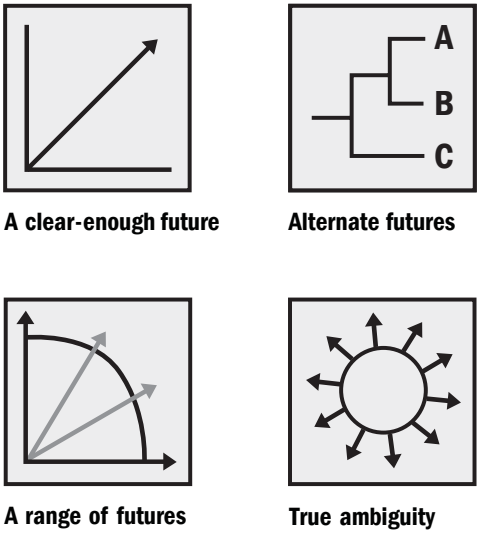


Figure 1: Levels of uncertainty[13]

13 Cf. Courtney, Kirkland, and Viguerie, 'Strategy under Uncertainty', pp. 70f.

The *fifth task* of risk analysts is to facilitate the sharing of knowledge across territorial and sectoral borders. When future challenges become global and their impact transcends boundaries, there is a growing need for risk analysts to engage with 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, resort heavily 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, firstly, engage in the establishment of various forms of platforms for the exchange of ideas and best practices in risk management, and, secondly, they should tailor their specialized advice to the respective institutional needs.[14]

The *sixth task* of risk analysts is to recognize that although risk perception largely depends on individually held values, worldviews, goals, and interests, risk identification and assessment requires 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 a crucial requirement for cultivating open, enlightened, and future-oriented communication about risks and threats.

14 The Crisis and Risk Network (CRN) at the Center for Security Studies, ETH Zurich, is an example of such a platform for sharing experiences among risk experts: <http://www.crn.ethz.ch>, accessed 15 November 2007.

5 Conclusion

Analysts and decision-makers in public adminstrations, armed forces, international organizations, or business corporations have discovered risk as a preferred tool for analyzing and managing trends and developments in an interconnected, complex, and uncertain environment. The notion of risk reveals some of the basic characteristics of the contemporary world by constantly reminding decision-makers of the difficult task of striking a sensible balance between opportunities and threats in dealing with uncertain future events. It has been the aim of this "International Handbook on Risk Analysis and Management" to provide insights into the current practices and future challenges of risk analysis and management from practitioners in a broad range of professional contexts. Indeed, the collected contributions bear witness to a great deal of experience and profound knowledge within and across professional communities. We hope that this volume offers a starting point for even more in-depth research, stimulating reflections, lively debates, and profound discussons about risks and threats today and tomorrow.

ANNEX

ANNEX

GLOSSARY OF METHODS OF RISK ANALYSIS

Affinity Diagram
The affinity diagram is an analytical tool that allows a group of people to systematically generate a large volume of ideas, opinions, or input about a problem or issue and organize these into meaningful categories. It helps participants to break old patterns of thought, discover new patterns, and generate more creative ways of thinking.

Agent-Based Simulation Modeling
Agent-based simulation modeling, sometimes referred to as multi-agent modeling, covers several rather different types of modeling. What they all have in common is that they develop a simulated history out of the interactions of individual agents with one another and/or their environment. Agents typically have the following properties: autonomy (operating without others controlling their actions and internal states), social ability (interacting with other agents), reactivity (perceiving their environment and reacting to it), and proactivity (engaging in goal-directed behavior).

Analogy
An analogy is useful for understanding new and unknown situations in terms of what is already known. Historical analogies are used to explain or make a prediction about a current or future event based on past events.

The past event is used as a source, while the present or future situation is the target of the analogy.

Bayesian Analysis
Bayesian analysis is a statistical inference in which probabilities are interpreted not as frequencies or proportions or the like, but rather as degrees of belief. Bayesian inference provides a logical, quantitative framework for the process of integrating accumulating information. It is applied in a multitude of scientific, technological, and policy settings.

Brainstorming
Brainstorming is an idea-gathering and creativity technique that can be used to identify risks, ideas, or solutions to issues by using a group of team members or subject-matter experts. Typically, a brainstorming session proceeds in a structured manner. Preferably, each participant's ideas are recorded for later analysis.

Cause-Effect Analysis
Cause-effect analysis is a predictive or diagnostic analytical tool used to explore the root causes or factors that contribute to positive or negative effects or outcomes. It is a very useful method for identifying potential risks. Its most typical form is the Ishikawa-Diagram, named after Kaoro Ishikawa, who introduced cause-effect diagrams, and is also known as the "fishbone diagram".

Cognitive Mapping
Cognitive maps try to capture the key factors that drive an issue, and the inter-relationships and feedbacks between them. They can be applied to either the prospects for countries or regions, or to the strategic decisions that companies, governments, or organizations face.

Cost-Effectiveness Analysis (CEA)
CEA is a method for comparing alternative ways of achieving an already specified target so as to achieve this target at the lowest possible cost. In contrast to the CBA (see below), the benefits are constant, and the aim of the analysis is to minimize the costs associated with achieving a specific objective.

Cost-Benefit Analysis (CBA)

CBA is a method for evaluating potential projects and for facilitating decision-making by weighing the costs of a project against its potential benefits. It considers all the net benefits of a project received over time. Therefore, the net benefits must be made comparable and the present value of all future net benefits needs to be computed.

Cross-Impact Analysis

Cross-Impact Analysis is a way of systematically examining potential future events or developments and their interactions. This method is concerned with the identification of potential outcomes rather than with the understanding of what is or what was. It takes into consideration interdependencies between events and developments, and has the potential to produce more consistent and accurate forecasts.

Decision Conferencing

Decision conferencing is a series of intensive working meetings attended by groups of people who are concerned about some complex issues facing their organization. There are no prepared presentations or fixed agenda; the meetings are conducted as live, working sessions lasting from one to three days.

Decision Tree Analysis

The decision tree is a diagram that describes a decision awaiting resolution and the implications of choosing one or another of the available alternatives. It is used when some future scenarios or outcomes of actions are uncertain. It incorporates probabilities and the costs or rewards of each logical path of events and future decisions. It may also use expected monetary value analysis to help the organization identify the relative values of alternate actions.

Delphi Technique

This is an information-gathering technique used as a way to reach a consensus of experts on a subject. Experts on the subject participate in this technique anonymously. A facilitator uses a questionnaire to solicit ideas about the important points related to the subject. The responses are summarized and then recirculated to the experts for further comment. Consensus

may be reached in several rounds. The Delphi technique helps to reduce bias in data and prevents any one person from having undue influence on the outcome.

Environmental Scanning
Environmental scanning (also called environmental assessment) is the acquisition and use of information about events, trends, and relationships in an institution's external environment. Information is collected from many different sources, such as newspapers, magazines, reports, conferences, etc.

Event Tree Analysis (ETA)
ETA is based on a binary logic, in which an event either has or has not happened or a component has or has not failed. It is valuable in analyzing the consequences arising from a failure or undesired event. An event tree begins with an initiating event. The consequences of the event are then traced through a series of possible paths. Each path is assigned a probability of occurrence, and the probabilities of the various possible outcomes can be calculated.

Expected Monetary Value Analysis (EMV)
EMV is a statistical technique that calculates the average outcome when the future includes scenarios that may or may not happen. A common use of this technique is within decision tree analysis.

Expert Judgment
Expert judgment is judgment based upon expertise in an application area, knowledge area, discipline, industry, etc., as required for the activity being performed. Such expertise may be provided by any group or person with specialized education, knowledge, skill, experience, or training, and is available from many sources, including scientists, consultants, stakeholders, professional associations, industry groups, etc.

Extrapolation
See Trend Analysis.

Extreme Event Analysis

In the case of extreme events (the tail end of the probability distribution function), historical, statistical, or experimental data is often sparse. The statistics of extremes is a body of statistical theory that attempts to overcome this shortcoming by classifying most probability distributions into different families on the basis of how fast their tails decay to zero.

Failure Mode and Effect Analysis (FMEA)

FMEA is an analytical procedure where each potential failure mode in every component of a system is analyzed to determine its effect on the reliability of that component and, by itself or in combination with other possible failure modes, on the reliability of the system and on the required function of the component. For each potential failure, an estimate is made of its effect and its impact on the total system. In addition, the action planned to minimize the probability of failure and to minimize its effects are reviewed.

Fault Tree Analysis (FTA)

FTA is a technique that provides a systematic description of the combination of possible occurrences in a system, which can result in an undesirable outcome. This method can combine hardware failures and human failures. The most serious outcome is selected as the top-level event. A fault tree is then constructed by relating the sequences of events that, individually or in combination, could lead to the top-level event. The tree is constructed by deducing the preconditions for the top-level event and then successively for the next levels of events, until the basic causes are identified.

Focus Groups

Focus groups are a form of group interview, consisting of an open-ended, structured discussion with a representative group. One or more interviews with a small group of participants are conducted. While group interviews are often used to collect data from several people simultaneously, focus groups explicitly use group interaction as part of the method. People are encouraged to talk to one another, asking questions, exchanging anecdotes, and commenting on each others' experiences and points of view.

Forecasts
Forecasts are estimates or predictions of conditions and events in the future, based on information and knowledge available at the time of the forecast. Forecasts are updated and reissued based on the provision of new information. The information is based on the past experience and the expected future.

Hazard and Operability Studies (HAZOP)
HAZOPs are structured critical examinations of processes undertaken by an experienced team in order to identify all possible deviations from an intended design, along with the consequent undesirable effects concerning safety, operability, and the environment. The possible deviations are generated by rigorous questioning, prompted by a series of standard "guidewords" applied to the intended design.

Hierarchical Holographic Modeling (HHM)
HHM is a systemic approach for risk identification. The HHM methodology is grounded on the premise that in the process of modeling large-scale and complex systems, more than one mathematical or conceptual model is likely to emerge. Each of these models may adopt a specific view. Through HHM, multiple models can be developed and coordinated to capture the essence of the many dimensions, visions, and perspectives of infrastructure systems.

Horizon Scanning
See Environmental Scanning.

Human Reliability Analysis (HRA)
HRA estimates the likelihood that certain human actions, which may prevent hazardous events, will not be taken when needed, and also assesses other human actions that may cause hazardous events. Both types of action are commonly called "human errors" in HRA, implying that an action was omitted or taken with adverse effects on safety. Results of HRAs are often used as inputs to PRAs (see below).

Influence Diagram
An influence diagram, also called a relevance diagram, is a visual representation of a decision problem. It offers an intuitive way to identify and display the essential elements of a decision problem, including decisions, uncertainties, and objectives, and how they influence each other.

Monte-Carlo Simulation
Monte-Carlo simulation is a type of "what-if" simulation that uses random numbers to measure the effects of uncertainty on decision-making processes. While traditional "what-if" simulations reveal what is possible, a Monte-Carlo simulation reveals what is probable.

Morphological Analysis
This is a method for exploring all the possible solutions to a multi-dimensional, non-quantified problem complex.

Pairwise Comparisons
Pairwise analysis is a method for comparing and choosing the most appropriate solution or option. Options are compared against each other on a number of criteria (e.g., performance objectives) to determine their relative order (ranking). The comparisons can be qualitative or quantitative, and different weightings can be applied for each individual objective.

PESTE-analysis
PESTE is an analytical tool used to systematically scan the environment of an institution and to structure identified environmental factors along specified analytical categories. The PESTE framework uses five different categories of environmental factors that may affect the institution under consideration: Political, Economic, Societal, Technological, and Environmental/Ecological factors.

Plus-Minus Implications (PMI)
PMI is an improvement of the simple "weighing pros and cons" technique. All the positive results, negative effects, and possible implications of taking a specific action are written down; subsequently, each of the points is assigned a positive or a negative score.

Preliminary Hazard Analysis (PHA)
PHA is a semi-quantitative analysis that is performed in order to identify all potential hazards and accidental events that may lead to an accident. It ranks the identified accidental events according to their severity and identifies the required hazard controls and follow-up actions.

Probabilistic Risk Assessment (PRA)
PRA, also called Quantitative Risk Assessment (QRA), is a systematic methodology for evaluating the risks associated with every aspect of a complex (engineered technological) entity. It asks what can go wrong with the entity under consideration, or what the initiators or initiating events are, what and how severe the potential detrimental effects or consequences of the occurrence of the initiator are, and how likely these undesirable consequences are or what the probability or frequency of their occurrence is.

Probability and Impact Matrix
See Risk Matrix.

Quantitative Risk Assessment (QRA)
See Probabilistic Risk Assessment (PRA).

Relevance Diagram
See influence diagram.

Risk Matrix
A risk matrix is a way of determining whether a risk is considered low, moderate, or high by combining the two dimensions of the classical risk definition – namely, the risk's probability of occurrence and its damage potential in the case of occurrence.

Risk Radial Chart
Drawing on a thorough risk assessment, a risk radial chart is a simple tool for graphically illustrating a set of identified risks. It serves to analyze the relative importance of risks and to further prioritize them in case of ambiguities.

Scenario
Scenarios attempt to analyze possible future events by considering alternative possible outcomes. They lead to improved decision-making by allowing a more complete consideration of a variety of different possible outcomes and their implications.

Sensitivity Analysis
Sensitivity analysis is a quantitative risk analysis technique that helps to determine which risks potentially have the most impact. It examines the extent to which the uncertainty of each element affects the object under consideration when all other uncertain elements are held at their baseline values. The typical display of results is in the form of a tornado diagram.

Simulation
A simulation uses a model that translates the uncertainties specified at a detailed level into their potential impact on expressed objectives. Simulations usually use computer models and estimates of risk.

Strengths, Weaknesses, Opportunities, Threats (SWOT)
A SWOT assessment structures information and generates strategic planning alternatives by analyzing internal and external factors influencing an institution. The internal factors are **s**trengths and **w**eaknesses, while the external factors are **o**pportunities and **t**hreats.

Trend Analysis
Trend analysis is an analytical technique that forecasts future outcomes based on historical results. It is a method for determining the variance from a baseline parameter by using data collected from earlier periods. It projects how much a parameter might diverge from the baseline at some future point if no changes are made. It often assumes that the underlying patterns of the past will continue to exist in the future.

ANNEX

AUTHORS

Gregory Baudin-O'Hayon
is a strategic criminal intelligence analyst with the Criminal Intelligence Service of Canada (CISC). He is the senior analyst responsible for the development and implementation of a strategic early-warning system for organized and serious crime in Canada. Before joining CISC in 2003, he completed a doctorate in Strategic and International Affairs at the Graduate School of Public and International Affairs at the University of Pittsburgh.

Stefan Brem
joined the Swiss Federal Office for Civil Protection in March 2007, where he leads a unit on Risk Analysis and Research Coordination. Previously, he served with the Centre for International Security Policy of the Federal Department of Foreign Affairs, where he was responsible, inter alia, for critical infrastructure protection, border security, and private security companies. He completed his dissertation in Political Science at the University of Zurich in 2003.

René P. Buholzer
is head of public policy at Credit Suisse, based in Zurich. Previously, he worked at the Swiss Business Federation (economiesuisse) in Zurich, where he was a member of the executive board. He also worked as a management consultant in Prague. Mr. Buholzer holds a doctorate degree from the University of St. Gallen (HSG) and was a research fellow at the European Parliament and the Centre for European Policy Studies (CEPS) in Brussels and in Luxembourg. Dr. Buholzer is a lecturer at the University of St. Gallen (HSG) and at the Universities of Applied Sciences Winterthur (ZHW) and Zurich (HWZ).

Erik Falkehed
works as an analyst and research officer in the Operations Service of the OSCE Conflict Prevention Centre. He is from Stockholm, Sweden, where he worked as an analyst of Security Policy and International Affairs at the Swedish Armed Forces Headquarters and the Swedish Defence Wargaming Centre. He holds a Masters of Arts (M.A.) in International Relations from Johns Hopkins University, School of Advanced Internationals Studies (SAIS), in Washington D.C. and a Bachelor of Social Science (B.A.) in Political Science and Economics from Stockholm University, Sweden.

Giulio Gullotta
holds a diploma in Political Science from the Bundeswehr University, Hamburg. After joining the core preparation group for the German crisis management exercise "LÜKEX" in 2004, he transitioned from active duty in the German armed forces to the civilian Federal Office of Civil Protection and Disaster Assistance. In 2005, he chaired the interdisciplinary Bund-Länder working group for hazard estimation. Currently, he is an assistant section chief in the Centre for Emergency Planning and International Affairs and is responsible for work in the area of risk analysis methodology.

Beat Habegger
is a senior researcher with the Crisis and Risk Network (CRN) of the Center for Security Studies (CSS) at ETH Zurich and a lecturer in Political Science at the University of St. Gallen (HSG). Prior to joining the CSS, he held various posts in academic research and public policy analysis at universities, international organizations, and a private consultancy. He studied at the University of Berne, the Institut d'Etudes Politiques de Paris (Sciences Po) and the University of St. Gallen (HSG), where he obtained a doctoral degree in 2005.

Bruno Käslin
graduated in 2003 from the University of St. Gallen, Switzerland, with a Master's degree in Economics, specializing in risk and insurance management. After his studies, he worked from 2003–2005 as a senior researcher and account manager at the Mobile and Ubiquitous Computing Lab (M-Lab), responsible for the research group on smart applications in the insurance industry. Today, he is a project manager at the Institute of Insurance Management at the University of St. Gallen and is in charge of several research, consulting, and teaching projects. He is also engaged in writing a Ph.D. dissertation about the systematic detection and management of emerging risks.

Roland Kaestner
has served as a commanding officer and as a staff officer. He participated in the 30th General Staff training course at the Bundeswehr Academy from 1987–89, and was a Military Fellow at the IFSH from 1989–91. He served as a battalion commander of the 252nd Paratroop Battalion from 1992–94 and worked in the headquarters staff of the German Army (Heer) from 1994–95 as a technical officer in charge of the Army/Special Forces air mobility concept. In 1995 and 1997, he was an instructor in military policy at the Bundeswehr Academy. In 1998, he worked in the German parliament as an academic consultant, and from 1999–2000, he supported the parliamentary faction of the German Green Party in security and defense policy issues. Since 2001, he has headed the strategic future analysis department at the Bundeswehr Transformation Center. In 2005, he became a lecturer in strategy at the Bundeswehr Academy.

Matthias Klopfstein
graduated in German Studies and Comparative Political Science from Berne University. During and after his studies, he worked as a journalist and editor for "Der Bund", a major Swiss daily. He was also a freelance copywriter, working, among other things, for the Museum of Communication in Bern. After joining the Federal Service for Analysis and Prevention (SAP), a unit with the Federal Office of Police, some years ago, he worked as a political analyst. He is currently enrolled in religious studies classes at Berne University, while continuing his work at SAP.

Marco Lier
studied History, Political Science, and Middle Eastern Studies in Zurich and Paris. After graduation, he worked as a political editor for a Swiss newspaper. He joined Swiss Re in 2003 as political risk adviser in the Political & Sustainability Risk Management department, where he developed the political country risk rating database together with colleagues from other departments.

François D. Maridor
joined the Swiss Federal Office for Civil Protection in January 2005. Since the early 1990s, he has been involved with and in charge of several projects relating to risk and vulnerability analysis with the former Central Office for General Defence and then with the Directorate for Security Policy, within the Federal Department for Defence, Civil Protection, and Sports.

Daniel R. Morris
is a doctoral candidate at the Department of War Studies, King's College London (KCL), specializing in the study of surprise and warning for counter-terrorism intelligence. He is completing his Ph.D. in London on leave from the Royal Canadian Mounted Police, where he serves as a civilian member. Prior to taking up his fully-funded KCL studentship in 2006, he worked for the Criminal Intelligence Service of Canada (CISC), where he co-developed the CISC's strategic early-warning system.

Sara Myrdal
is a principal analyst within the executive staff at the Swedish Emergency Management Agency (SEMA). She has also worked at the Swedish Institute of International Affairs (SIIA), heading a research project on crisis management in the European Union. Her publications include "The EU as a Civilian Crisis Manager" (EU som Civil Krishanterare) (Utrikespolitiska Institutet, 2002) and "Nordic Responses" in *Europe Confronts Terrorism* by Karin von Hippel (ed.) (Palgrave Macmillan, 2005).

Manuel Rybach
is head of governmental affairs at Credit Suisse Public Policy, currently based in Singapore. Previously, he worked at the Credit Suisse Government Affairs office in Washington, D.C. and was a senior economist at Credit Suisse Economic Research in Zurich. Mr. Rybach studied at the University of St. Gallen (HSG), from where he holds a doctorate degree, and he also studied at the Institut d'Etudes Politiques de Paris (Science Po). He was a visiting scholar at Columbia University Law School in New York and Georgetown University Law Center, and worked at the Center for Strategic and International Studies (CSIS), both in Washington, D.C. Dr. Rybach is a lecturer at the University of St. Gallen (HSG) and a guest lecturer at the University of Lugano (USI).

CSS
ETH Zurich

The Center for Security Studies at ETH Zurich was founded in 1986 and specializes in the fields of international relations and security policy. The Center coordinates and develops the Crisis and Risk Network (CRN), a Swiss-Swedish initiative for international dialog on risks and vulnerabilities that is aimed at enhancing knowledge of the complex causes, interactions, probabilities, and costs of risks in modern societies.

The International Handbook on Risk Analysis and Management gives insight into professional practices and methodical approaches of risk analysis and management. It shows how risk analysts and decision-makers in different professional contexts deal with risk and uncertainty by identifying upcoming issues, assessing future threats, and implementing successful mitigation policies.