OECD Studies in Risk Management

Denmark

ASSESSING SOCIETAL RISKS AND VULNERABILITIES

OECD

OECD STUDIES IN RISK MANAGEMENT

Denmark

ASSESSING SOCIETAL RISKS AND VULNERABILITIES

OECD
ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT

Foreword

The OECD Futures Project on Risk Management Policies aims to assist OECD countries in identifying the challenges of managing risks in the 21st century, and contributing to their reflection on how best to address those challenges. Its focus is placed on the consistency of risk management policies and on their ability to deal with the challenges, present and future, created by systemic risks.

The Project is designed in two phases. In Phase 1, the countries participating in the project propose specific themes as case studies of their risk management policies. For each proposal, the OECD Secretariat prepares an overview of the issue covering both recent international developments of interest and the national policy context. Where relevant, the Secretariat elaborates a tool for self-assessment and review, consisting of one or several questionnaires following the methodological framework of the project. This prepares the ground for Phase 2 in which an in-depth review of the risk management issues will be conducted by a team of experts for those countries that wish it. Self-assessments will be used as the basis of these reviews. At the end of phase 2, a cross-country report will bring together the lessons learned from the project, and identify opportunities for sharing best practices and improving risk management.

In the framework of the Project, the Danish Ministry of Defence asked the OECD Secretariat in October 2004 to prepare a study on risk and vulnerability identification methods. The aim of the study is to contribute to ongoing reflections regarding the need to assess more systematically and effectively the nation's vulnerabilities and exposure to hazards. Its focus is therefore on methodological and implementation issues linked to the creation and execution of nation-wide risk and vulnerability assessments, rather than existing policies.

This study has been prepared by Reza Lahidji and Marit Undseth, from the OECD International Futures Programme. The authors have benefited from the support of Dorthe Juul Munch from the Danish Emergency Management Agency, and from the guidance of the Steering Group to the OECD Futures Project (see the list of Steering Group members in Annex 1). The study is issued under the responsibility of the Secretary General of the OECD.

Table of contents

Introduction

Denmark is currently engaged in a reappraisal of its strategy for managing major risks. The context in which this reappraisal takes place was set by the political agreement of 21 June 2002, which will be valid until 2006. The agreement stated that in the current threat landscape, the Danish preparedness system needs to be reorganised, with a shift of emphasis from traditional defence tasks to peace-time preparedness. It gave more power to municipalities to adapt their preparedness measures according to their own evaluation of risks, and called for a better coordination of preparedness policies at the national, regional and municipal level.

The political agreement furthermore asked the government to carry out a cross-sectoral assessment of the country's major vulnerabilities. A commission was constituted to this aim, started its work in March 2003, and gave its final report in October 2003. The report deemed Denmark's preparedness system satisfactory, but recommended to improve coordination between private and public actors as well as across sectors. One of the commission's key findings was the need for a "systematic, intensive and on-going surveillance and analysis of threats and risks", which would focus on the "collection of intelligence reports on societal threats; sectoral information on developments in the risk landscape, preparedness and other issues which may have impact on the joint level of preparedness; and information on critical infrastructure dependencies."[1]

The responsibility for establishing such a broad picture of the nation's vulnerabilities was subsequently assigned to the Danish Emergency Management Agency (DEMA), as the coordinator of risk and vulnerability assessments elaborated in all relevant sectors of activity. This will entail to develop a generic model of risk and vulnerability assessment, which will apply across sectors regardless of differences in the sources of threat, data availability, experience with risk and vulnerability assessments, and the legal and regulatory framework. In addition, the Agency will need to identify and monitor a number of risk-related trends and issues which might be overlooked in sectoral approaches. The active participation of governmental agencies, businesses and representatives of the civil society will be crucial in this endeavour. Obtaining a realistic view of the risk and vulnerability situation will require a high degree of involvement of sectoral regulatory agencies (e.g. when it comes to detecting possible threats as well as reporting about new practices in the sector), private sector companies (e.g. operators and owners of critical infrastructures), as well as people who are at risk (e.g. regarding questions of risk acceptance).

[1] Udvalget for National Sårbarhedsudredning, 2004, pp. 298-302.

This report raises a number of methodological issues for consideration in DEMA's work. These issues are drawn from the experience of harmful events which have challenged the capacity of governments to protect the population in some OECD countries, and the lessons that these countries have learned in order to better assess risks and vulnerabilities at the level of the nation. The report is divided in three parts. The first part provides a brief overview of risk and vulnerability assessment methods commonly used in various sectors and identifies a number of key components in these methods. The second part proposes a checklist of additional topics of interest for a nation-wide assessment of vulnerabilities. Finally, the third part scrutinises development and implementation questions.

Methodologies for identifying and assessing risks and vulnerabilities

The concepts of risk and (to a lesser extent) vulnerability are nowadays applied to a broad range of issues, from human health to the security of information systems. Inevitably, there are substantial differences in the way risk and vulnerability are defined, understood, analysed and measured in these various sectors. However, a common understanding of the concepts has gradually emerged, thanks notably to harmonisation efforts by institutions such as the International Organization of Standardization (see box 1). This section first introduces common elements of terminology, then reviews some of the most widespread methods of risk and vulnerability assessment, and briefly compares the principal features of those methods in order to derive some general lessons of interest when analysing risks and vulnerabilities at the level of a nation.

Some terminology

Box 1 presents some basic definitions which are accepted in most if not all areas dealing with risk.

Box 1 – Risk and vulnerability terminology

The International Organization of Standardization (ISO) has defined the following standard terminology for risk and risk assessment.

- Hazard: Potential source of harm.
- Risk: Combination of the probability of an event and its consequence. The term "risk" is generally used only when there is at least the possibility of negative consequences.
- Risk assessment: Overall process of risk analysis and risk evaluation.
- Risk analysis: Systematic use of information to identify sources and to estimate the risk. Information can include historical data, theoretical analysis, informed opinions, and the concerns of stakeholders.
- Risk identification: Process to find, list and characterise elements of risk. Elements can include source or hazard, event, consequence and probability.
- Risk estimation: Process used to assign values to the probability and consequences of a risk.
- Risk evaluation: Process of comparing the estimated risk against given risk criteria to determine the significance of the risk. Risk evaluation may be used to assist in the decision to accept or to treat a risk.
- Risk criteria: Terms of reference by which the significance of risk is assessed.

The ISO has also defined vulnerability and the related concept of threat in the context of information systems and information security:

- Vulnerability: A weakness of an asset or a group of assets than can be exploited by one or more threats.
- Threat: A potential cause of an incident that may result in harm to system or organisation.

The concept of vulnerability is also used in social science. A possible definition in that context is the one given by Chambers (1989):

- Vulnerability: The exposure to contingencies and stress, and difficulty in coping with them. Vulnerability thus has two sides: an external side of risks, shocks and stress to which an individual or household is subject; and an internal side which is defencelessness, meaning a lack of means to cope without damaging loss.

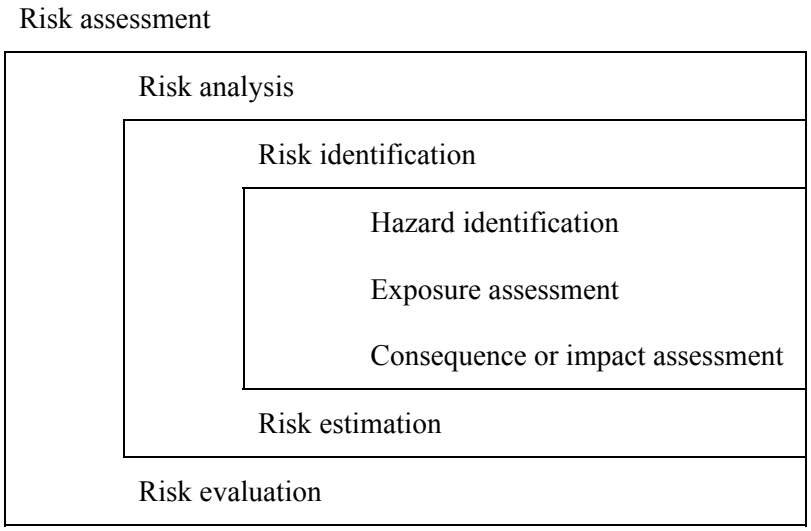
Sources: International Standards Organisation, 1999, 2002 and 2004; Chambers, R., 1989, pp.1–7.

With these definitions in mind, a number of statements can be made as the basis for any risk and vulnerability assessment.

- Risk refers to a hazard which is more or less likely to occur, and to the consequences that its occurrence would have. These consequences can concern individuals or entire populations, assets, ecosystems, and activities, depending on their exposure to the hazard and their vulnerability.

- Risk assessment is the process of gathering information regarding risk before taking any decision relative to its handling. Risk assessment comprises a number of possible steps, but all of these steps are not relevant to all risk sectors (figure 1).

Figure 1 – Possible steps in risk assessment



Source: See in particular National Research Council, 1996.

- Risk can be quantified as the product between the probability of occurrence of the hazard and the value of the damage it would cause, but such quantification is not always possible.

- To make a comprehensive assessment of the consequences of an event, it might be necessary to identify indirect effects such as secondary hazards triggered by the event, and to analyse complex social, economic or environmental developments caused by the hazard.

- All steps of risk assessment can entail uncertainties and limitations. Information about these uncertainties and limitations is an inherent part of risk assessment and a crucial element of decision-making.

- Just as risk refers to a defined hazard and a variety of endpoints (populations and systems which might be affected), vulnerability refers to a single endpoint and various hazards.

- Vulnerability assessment entails to collect information on the extent of damage which might be caused to a population or system. Hazards can be assessed or not. Vulnerability is usually not quantifiable.

Commonly used methodologies

Sophisticated methodologies have been developed in numerous areas exposed to hazards in order to assess risks and vulnerabilities. A brief description is provided here for some of the most well-known tools used in areas such as environmental health (e.g. health effects of exposure to hazardous substances), food safety (e.g. in food processing industries), natural disasters (floods, earthquakes, etc.), complex engineered systems (e.g. airplanes or nuclear power plants), and security (physical security, cyber-security).

- Environmental health: risk assessment for hazardous substances[2]

When a substance is suspected to have adverse effects on human health, the initial steps are usually to determine what kind of toxicity or illness it can cause, and how the incidence of adverse effects evolves with exposure. Once a hazardous substance is identified, its health impacts are usually evaluated according to dose-response relationships built on empirically determined thresholds, such as the No Observed Effect Level (NOEL) or the Lowest Observed Effect Level (LOEL). For carcinogenic substances, response is generally assumed to increase proportionally to the dose absorbed at low levels of exposure (unless a threshold level is observed).

The process necessarily involves elements of uncertainty, including reliability of the test method, differences between laboratory animal species and humans, variability among humans, and longer-term impacts. To account for uncertainties affecting the value of a parameter, the common practice is to determine a conservative upper (or lower) bound for it, often called the safety factor. In some food safety

[2] See United States Environmental Protection Agency, 1998.

regulations in the United States, for instance, a safety factor is applied between the No Observed Effect Level determined from animal study and the Allowable Daily Intake.

Such dose-response relations are the cornerstone of hazard assessment for most issues related to human health, from water contaminants and pesticides to radiation. In order to produce a risk assessment, the outcomes of hazard assessment must further be combined with the results of an exposure assessment, determining the levels of possible exposure. In some cases, an exposure pathway assessment is also performed to explore through which media and in what proportions and time scales populations at risk might be exposed.

- Food safety: Hazard Analysis and Critical Control Point (HACCP) plans[3]

A variety of agents and substances can affect human health through food: micro-organisms such as bacteria, viruses and prions; mycotoxins (fungi), phycotoxins (algae), and other natural toxic substances; and hazardous chemical compounds used in agriculture or in food production, such as pesticides. Some of these hazardous substances or agents can enter the food chain at any of its stages depending on a variety of factors, including the behaviour of the food's consumer.

Hazard Analysis and Critical Control Point (HACCP) plans are safety programmes designed to identify and manage the ensuing risks for human health. HACCP plans, which have become one of the central elements of food safety systems in most OECD countries, are based on a systematic identification and control of risk through the phases of food production, from buying raw materials to delivering the final products. First, the various hazards that may affect food safety are identified. Their likelihood of occurrence is quantified, and the least likely hazards are excluded. Every step of food production and handling where one of the selected hazards could be introduced in the process – and therefore needs to be controlled – is pinpointed as a Critical Control Point. A critical limit is determined for every control parameter, below which the occurrence of hazard can be considered unlikely. Procedures are determined to monitor the CCPs through testing and observation. Corrective actions are planned, in order to be engaged when monitoring shows that a critical limit has been reached. Supplementary tests are also elaborated to verify that the system is working properly, and ran periodically by an unbiased and independent authority. Finally, records are effectively kept in order to document the various HACCP procedures.

- Natural disasters: catastrophe models[4]

[3] See FAO/WHO, 2003.
[4] See Grossi and Kuhnreuter, 2005.

Catastrophe models simulate the occurrence of a natural disaster and estimate its effects, usually through three modules: a hazard simulator, a vulnerability block, and a loss assessment module. Based on historical records and statistical analysis (using hydrologic information for floods, seismic and tectonic information for earthquakes, etc.), a catalogue of events is generated. Each event comprises a source, a magnitude, a duration, and an annual frequency. The area of concern is mapped in detail thanks to (micro)zonation, in order to describe the propagation of the hazard. Exposure is assessed for the main types of property and assets in the area: residential buildings, factories, agricultural land, etc. Buildings can be classified according to their function and architectural structure, and capacity curves and repair/replacement costs estimated for each of these classes. Finally, total casualties, displacements and economic losses are calculated for each event. Average and worst-case losses can also be computed for a given area across the range of events, without consideration for probabilities of occurrence.

Each of the above assessment stages involves various sources of uncertainty. The influence of each of these sources on overall uncertainty can be estimated by varying the corresponding parameters (e.g. frequency of events, building resistance, etc.) and measuring the sensitivity of final results. Once all sources are included, sensitivity analysis often shows that catastrophe loss estimation remains a highly uncertain process.

- Natural disasters: community vulnerability assessment[5]

In the area of natural disasters, vulnerability assessment aims at determining those factors that make a given community more or less susceptible to hazards. Such factors can include density of population, physical vulnerability (e.g. weak soils) and poverty. Here, the focus shifts from the possible consequences of a hazard to the likely causes of damage.

Possible steps of the process include: identification of the most significant hazards; definition of high-risk areas; selection of facilities of particular relevance (e.g. hospitals, schools, or hazardous industrial installations), and conduct of a vulnerability analysis for those; selection of social groups of particular relevance (such as landless farmers in a specific area), and conduct of a vulnerability analysis for those; mapping of the local economy and analysis of possible economic impacts; analysis of direct and indirect impacts (e.g. due to accidents caused by the initial event) on the environment; identification of possible measures to prevent or mitigate hazards and/or to reduce vulnerability.

[5] See for instance United States National Oceanic and Atmospheric Administration, n.a.

Such specific, scale-dependent assessment strategies may eventually be able to isolate an appropriate set of factors, analyse their interactions, and assess their overall influence on elements of vulnerability such as coping reserves and adaptive capacity.[6] One important aspect of vulnerability assessment is to identify the segments of a society that are more susceptible to damage, and by doing so, to focus attention on avoiding dangerous combinations of factors.

- Industrial facilities and other engineered systems: safety assessment methods[7]

Modern safety assessment of complex systems originates from reliability analysis techniques which were developed from the 1930s onwards, in order to accompany technological developments where safety could no longer be based on trial and error (e.g. commercial aeroplanes, large-scale chemical facilities, etc.). It uses a variety of hazard identification and risk assessment tools, such as Hazard and Operability (HAZOP) analyses, Preliminary Hazard Analysis, Fault and Event Trees, and Probabilistic Safety (or Risk) Assessment (PSA/PRA).

HAZOP analysis is a method for identifying all possible deviations from the normal operation of an industrial process, and ensuring that the measures needed to avoid an accident are in place.[8] The analysis is conducted by a multidisciplinary team, which systematically considers potential deviations by combining process conditions (temperature, pressure, etc.) with guide words (such as more, less, etc.). Although some quantification is possible, HAZOPs primarily produce a qualitative analysis of hazards.

Similarly, preliminary hazard analysis (PHA) aims at identifying all potential hazards and accidental events that may lead to accidents, as well as identifying hazard controls and follow-up actions.[9] It is a relatively rapid mapping and classification process of all known hazards, and is conducted by a small expert team which identifies all hazards and potential accidental events, often by use of hazard checklists. Severity and frequency of an event are classified and ranked (by use of quantitative or qualitative methods), something which leads to a final estimation and ranking of risk. It has been noted that this method relies heavily on the expertise of the team conducting the analysis, and on ample information of known hazards, something which make it less suitable for assessing hazards in a system with little operational history, or in an environment where hazards change quickly.[10]

[6] Clark et al., 2000.
[7] An overview of frequently used methods can be found at United States Coast Guard, n.a. (a);or in Rausand and Høyland, 2004.
[8] For more information, see for instance Kletz, Trevor A, 1997.
[9] Rausand, Marvin, n.a.
[10] United States Coast Guard, n.a.(b).

Fault trees and event trees are graphic techniques used to describe systematically the combinations of possible occurrences in a system. Fault trees focus on events which would significantly alter the system's safety – named as top events. A tree is then constructed with the sequences of equipment failures, human errors, or other incidents which could combine to trigger the top event. The tree helps to relate each top event to its possible root causes. Similarly, event trees start with an initiating event and investigate its consequences, which they follow through a series of possible paths. In both cases, each path is assigned a probability of occurrence, and the probability of the various possible outcomes can be calculated.

Methods such as Probabilistic Safety Assessments apply fault and event trees in a comprehensive manner in order to evaluate a system's overall safety. Such methods have gradually emerged as necessary supplements to traditional deterministic studies, compared to which they provide a more balanced and realistic picture of a risk situation. Evaluation of probabilistic distributions for model parameters also helps to identify the various sources of uncertainty involved in the assessment.

In the context of the safety of nuclear power plants, where they have been largely developed, probabilistic assessments are used to identify the potential vulnerabilities of plants seen from a relative point of view (i.e. dominant contributors to risk) and not as bottom-line results. Criteria for backfitting decisions, they constitute analyses preceding deeper investigations.[11] They are gradually being applied to a wider range of risk areas – such as hazardous chemicals, where they can help gauge variability and uncertainty in toxicity and exposure.[12]

- Malevolent acts and security assessment[13]

Malevolent acts such as sabotage, terrorism or cybercrime differ from most other types of risk in ways which make the assessment of security difficult. Usually, risks of malevolent acts cannot be quantified using reliable historical data. Furthermore, they are generated by human behaviour. In other words, their context is one where damage is not caused by an exogenous event such as an earthquake or even an accidental human error, but by the deliberate action of persons resolved to exploit every breach in security. Events such as a large aeroplane colliding with a nuclear power plant, or a lethal bacterium contaminating a food production process, are considered in safety assessment procedures, but very seldom as the results of a deliberate act. In such areas, more methodological work is needed to integrate the risk of malevolent acts into the framework of risk analysis. Various tools have been developed in recent years to this aim.

[11] OECD – NEA, 1992.
[12] OECD, 2001.
[13] See for instance Woo, 2002.

A number of innovative ideas have been put forward for modelling terrorism risks,[14] and recently, several models have been developed. Based on experts' opinions (collected e.g. via Delphi methods) and/or game theory models of behaviour, they evaluate the likelihood that a given location becomes the target of a terrorist attack and the likelihood that the attack succeeds. A loss simulation module then estimates the damage incurred.

Processes have also been designed to analyse threats and vulnerabilities, both for physical and information systems. For this, the first step is to designate the important components or assets of the system, and to evaluate their criticality, replacement options, recovery time and value. The next step is to identify, for each important asset, the significant threats and modes of operation of malevolent actors, and to assess the asset's vulnerability. Risks can then be evaluated by relating the likelihood of threats and vulnerabilities with the value of the asset. The final step is to map and rank undesired outcomes.

A comparison of assessment methods

Analysing in detail the merits and limits of the risk assessment methods reviewed above is beyond the scope of this study. However, even a rapid comparison of their main elements can provide some interesting insights into the challenges of risk and vulnerability assessment. Table 1 below summarises the principal features of some of these risk assessment tools. In addition to the traditional steps of risk assessment (identification, estimation, evaluation), a number of other questions have been considered in order to differentiate the methods: Are secondary risks considered? Are broad social, economic and environmental impacts analysed? How are uncertainties evaluated? Finally, is there an input to decision-making in terms of prioritisation of risks or choice of counter-measures (prevention, mitigation, risk transfer, etc.)?

In the first place, such a comparison shows that risk assessment methods can be quite comprehensive for theoretically well-structured systems, where only a limited number of interactions with the external environment need to be considered. Inside such "closed" systems, assessment can aim at identifying all possible chains of events leading to the realisation of a hazard, and all possible chains of consequences (even though those possibilities that are estimated too unlikely often are subsequently excluded). As the scope broadens to less "controllable" environments, systematically identifying and quantifying risk becomes considerably more complex. Efforts then need to be focused on specific issues such as:

- the particular risk conditions of certain systems or populations, due to their critical role in a larger context, their high value, or their relatively higher exposure or vulnerability

[14] Major, 2002; Woo, 2002

- the channels through which hazards can propagate, and the factors that aggravate or attenuate risks (e.g. secondary risks) when hazards are difficult to identify and monitor;

- understanding and controlling risk at its source (e.g. emission of a pollutant) and endpoint (e.g. safety of food) when the transmission mechanisms are too complex;

Secondly, some risk assessment issues appear to be well understood, thanks to reliable data and scientific knowledge, while others involve large uncertainties. The larger the uncertainties and the complexity of the risk issue at hand, the less risk assessment can be considered as a technical discipline which leads to a policy decision with no need for further inputs. An important issue, then, is to identify whether uncertainty is "due to inherent randomness or to lack of knowledge; and whether it is recognised and quantifiable, recognised and indeterminate, or unrecognised",[15] and decide how to treat the information. For quantitative elements of the analysis it means to carefully evaluate the quality and relevance of the data used, and to clearly identify the different sources of uncertainty. In qualitative analysis, there may be quantitative components, with the same problems of uncertainty as listed above. Perhaps the most challenging task is to account for unrecognised risk. This may be better picked up by scenario-building methods than traditional risk and vulnerability assessments. In addition, formal uncertainty analyses can be used to identify major gaps of knowledge where additional research may be necessary.[16]

This shows that in all cases, but particularly when risks are complex and partly unknown, or when risk conditions are changing:

- Uncertainty needs to be explicitly described, and if possible measured, when communicating the results of an assessment.

- Risk assessment needs to be designed as a open and inclusive process.

The two following sections of the report illustrate and further explore some of these lessons.

[15] National Research Council, 1996, p.116.
[16] ibid., pp. 109-111.

Table 1 – Comparison of various risk and vulnerability assessment methods

Sector	Method	Risk identification	Risk estimation	Risk evaluation	Secondary hazard identification	Environmental analysis	Socio-economic analysis	Uncertainty analysis	Prioritisation and choice of counter-measures
Environmental health	Hazardous product risk assessment (*)	Hazardous substance identification (toxicology, epidemiology)	Empirical evaluation of dose-response relationship, and exposure assessment	Calculation of toxicity thresholds (e.g. No Observed Effect Level)				Safety factors established as a conservative upper or lower bound for every uncertain parameter	Maximum admissible levels (e.g. allowable daily intakes)
Food safety	HACCP	Hazard analysis and identification of critical control points (where food processing can be affected)		Critical limits are determined for each critical control point				Safety factors established as a conservative upper or lower bound for every uncertain parameter	Preventive and corrective actions are proposed in cases where a critical limit is reached
Natural disasters	Catastrophe models (floods, earthquakes)	Historical data, statistical analysis, topographic analysis, scale models, mathe-matical models	Evaluation of impacts through zonation, hazard propagation models, and damage estimation for each type of asset	In some cases, hazard frequency thresholds (e.g. once-a-century floods)				Sensitivity analysis (e.g. Monte Carlo simulations)	
	Community vulne-rability assessment	Identification of high risk areas based on historical data, population density and other factors as deemed appropriate by the assessment team			Identification of critical facilities in high-risk areas and assessment of their vulnerability	Possible secondary impacts on the environment (e.g. hazardous industrial sites affected by the natural disaster)	Mapping and vulnerability assessment of centres of economic activity and areas of particular social interest		Choice of priority risk areas and hazard mitigation options

Complex systems	PSA/PRA	Possible failures of the system are identified, e.g. through a Fault Tree Analysis	Possible consequences of each failure are determined, e.g. through an Event Tree Analysis	Risk figures can be compared to quantitative thresholds	The risk of fires, accidents, and induced health effects of an accident can be considered	External consequences can be evaluated through a Probabilistic Consequence Assessment (e.g. in level 3 PSAs for nuclear power plants)		Sensitivity analysis (e.g. Monte Carlo simulations)	Contribution of each failure to total risk calculated to determine the major sources of vulnerability in the system
	Preliminary hazard assessment	Preliminary identification of hazards based on historical data and other information	Consequences and frequency of each hazard are estimated, and classified according to severity classes						Risk is ranked in a risk matrix and corrective measures are suggested if necessary. Use of ALARP.
Security	System risk and vulnerability analysis	Identification of the key components of the system, and of potential threats against one or several of those	Identification of weaknesses in protection / mitigation capacities. Qualitative evaluation of probability and consequences		Consideration of cascading effects				Description of possible prevention, mitigation and recovery measures
	Terrorism risk assessment	Historical data and expert opinions	Probability estimation: event trees, expert opinions, game theory models. Probabilistic loss distribution						
	Information security risk assessment	Identification of valuable assets, and identification of threats and vulnerabilities for those assets	Valuation of the assets. Assessment of the likelihood of occurrence of threats and vulnerabilities	Determination of acceptable risk levels for the organisation					Ranking of incidents by measured risk, or separation in acceptable and non-acceptable risks

(*) Specifically, non-carcinogenic hazardous substances.

Critical elements of a nation-wide assessment of vulnerabilities

On various occasions in recent years, harmful events of both natural and man-made origin have overwhelmed the response capacities of OECD societies. These accidents and disasters shed light on a series of environmental, demographic, socio-economic and technological trends which seem to have altered the risk landscape of OECD countries. In order to better prevent, mitigate and respond to such events, the mechanisms at work need to be better understood – a task that governments have just started to undertake.

Based on these experiences, this section raises five issues which should receive particular attention when evaluating a nation's vulnerabilities:[17] the identification of critical infrastructures and interdependencies among them; a specific focus on the protection of vulnerable regions or groups of population; a future-oriented approach pinpointing changes in risk patterns; the magnitude of risk in locations with a high density of people, activities and assets; and the need to monitor hazard propagation mechanisms. For each of these, the section reviews one or several events which are particularly illustrative, analyses the issue in general terms, and describes some policy initiatives of interest in OECD countries.

(1) The identification of critical infrastructures and interdependencies among them

The ice storm that hit Canada and the United States in January 1998 was unprecedented in its geographic extension, intensity of freezing rain, and duration. The storm lasted for seven days, and caused the death of 47 persons and generated USD 1.2 billion insured losses. It led in particular to severe interruptions to electric power supply in Canada, destroying 120 000 km of power lines and telephone cables, 130 major transmission towers and 30 000 wooden utility poles. The water supply was also disrupted.[18] 3 million people lost electricity, and in some areas it took 3 ½ weeks to restore power. In the evaluation that followed the disaster, the reporting commission for Québec pointed out the inadequacies of emergency preparedness in the Québec government in the face of such disruption in a critical infrastructure.[19]

The 2003 power outage in Eastern Denmark and Sweden illustrates in particular the problem of cross-border interdependencies between infrastructures. Following two unrelated errors in the Swedish power grid, power failed in Southern Sweden. The failure rapidly spread to Eastern Denmark, as the two regions are so closely linked that they practically make up one area for alternating current (while the links between

[17] See also OECD, 2003.
[18] Klaassen and Cheng, 2003, p. 8.
[19] Nicolet Commission, 1999.

Western and Eastern Denmark are much more limited). Nearly five million persons were affected, for a time period of up to 6.5 hours. Although Sweden and Denmark both had experienced serious power outage incidents before, a breakdown of such magnitude proved difficult to manage.

Emergency plans were not always operational and designed to handle an incident of this size. Some communication networks, such as radio support to the Swedish police and the Danish fire and emergency services failed.[20] Furthermore, both the Danish National Rail Administration and the Danish Energy Authority had problems communicating with underlying suppliers and customers due to absence of emergency power. [21] The Danish National Rail Administration could no longer make use of its train monitoring system, which meant that it could not locate trains on its network.[22] Cost estimates on Swedish side amount to SEK 500 million,[23] a level of impact which is well under that of other major power disruptions (see table 2). This is in part due to favourable weather conditions and relatively short duration of the outage. It was considered that several sectors, especially the portable phone network, would have rapidly reached critical thresholds of functionality had the outage lasted longer.[24]

Table 2 – The cost of power outages in the year 2003 in OECD countries

Incident	Date and duration	Affected population	Estimated cost
Canada and the United States	14-17 August	50 million	USD 100-300 million insured losses USD 6.76 billion total damage
London	28 August - 30 minutes during rush hours	London commuters (disruption in the underground traffic)	-
Denmark and Sweden	23 September	Almost 5 million	Sweden: SEK 500 million
Italy	28-29 September	55 million	5 dead EUR 120 million total damage

Sources: Munich Re, 2004(a); Swiss Re, 2004.

These disasters have highlighted the significance of certain infrastructures for maintaining vital societal functions, and also the strong interdependencies between such 'critical' infrastructures. Definitions of critical infrastructures usually include the sectors of energy supply, communications, water supply, health, transport, and sometimes food supply and finance. Many of these concerned sectors have experienced important changes in their ownership structure and in their regulatory framework in recent years in most OECD countries. Utilities are nowadays often owned and managed by the private sector. In a context

[20] Ekström, Anna Hedin, 2004.
[21] Beredskabsstyrelsen, 2003. No estimate was found for Denmark.
[22] Ekström, op.cit.
[23] Ibid.

where economic efficiency pressures have considerably increased, safety and security issues in these sectors need to receive renewed attention from regulatory bodies. Privatisation increases the number of actors involved in preparedness or emergency operations, and makes it more difficult for the government agencies to arrange sharing of information and obtain data for vulnerability assessments or simulations. In the disasters reviewed above, there was no or little preparation for dealing with the cascading effects of such events on other infrastructures.

In response to this, several countries have made efforts to map and identify interdependencies in critical infrastructures. One example is the work of the Canadian commission to identify critical infrastructures and interdependencies, and organise contingencies accordingly. Netherlands and Germany have also done work in this area. The Netherlands have established a detailed mapping of critical infrastructure interdependencies in the country, in close cooperation with the private sector. Germany has developed a specific methodology aimed at better analysing and understanding critical processes at a relatively detailed business level. The main line of argument is that business processes that are vital for the continued existence of an enterprise are 'business-critical'. If the existence of an enterprise is vital for the functioning of a sector, the business process also becomes 'sector-critical', although this is generally restricted to situations of oligopoly (i.e. only a few market actors). Finally, it is presumed that society-critical and sector-critical processes coincide. Box 2 provides a more detailed description of the methods used by the three countries.

Box 2 – Methods used for identifying critical infrastructure interdependencies

The Netherlands: 'Quick Scan', 2002-2004

The project was launched by sending a questionnaire, developed by the Netherlands Organisation of Applied Scientific Research, TNO, to the ministries to carry out an initial inventory of Dutch critical infrastructures (including products and services). Both the ministries and private companies in critical sectors replied to the questionnaire.

Following the questionnaire, a working conference took place with participation from both the public and private sector, which underlined the importance of continuing the joint effort.

17 workshops were then created to elaborate on the initial inventory of critical infrastructures, where 125 different organisations participated. At the same time, risk experts met to assess the direct consequences of breakdown or disruption of critical business processes.

Germany: 'Analysis of Critical Infrastructures', 2004

The methodology follows five steps: The first step involves gaining an overview of the sector; identify and describe important functions, influencing parameters, general importance of the sector and the major actors. It is important to break the sector down into practicable units of analysis (at segment, service or product level). In the second and third steps, the business processes in the different units must be identified and defined and then assessed for their

[24] Beredskabsstyrelsen, op.cit, p. 22.

criticality, *i.e.* importance at enterprise, sector and society level (see above), including a qualitative assessment of probability of breakdown of the process. This analysis will normally depend on academic and sectoral experts. The same multi-rating scale for effect and failure probability should be used for all business segments and sectors, in order to enable inter- and cross-sectoral comparisons. In the fourth step is investigated how the process depends on IT [or other critical infrastructures could be imagined, electricity, for instance]. In order to save work, focus should only be on those processes with significant or high criticality for society. In the fifth step, measures of control and correction are taken. This includes taking into account already existing protective and preventive mechanisms in the sector, as well as taking the criticality evaluations of national experts with a pinch of salt and try to compare with conclusions in other countries or sectors, as what is considered 'disruptive' for society may differ from one individual to another or from one society to another.

Canada: Mapping of critical infrastructures, 1998-2000

Two commissions have contributed to the mapping of critical infrastructures in Canada: the Nicolet Commission after the ice storm disaster in 1998 and the National Contingency Planning Group (NCPG), which was established to prepare the country for Year 2000.

The Nicolet Commission was mandated by the Canadian government to "analyse the circumstances in which the safety of individuals and property and the smooth operation of social and economic activities were maintained" during the 1998 ice storm. The Commission should furthermore find ways to improve or strengthen the management and coordination of actions during the disaster. Finally, the Commission should analyse the measures planned or considered to reduce the number of power outages to make them shorter or to lessen the impact on the population and economic activities.

The Commission based its approach on three components:

- A broad consultation of the population was held by means of public hearings. The Commission consulted 22 municipalities and 14 regional county municipalities (Montérégie MRCs) that were touched by the disaster. All in all, there were 44 public hearings and 20 citizens' fora, something which enabled over 150 persons and 300 organisations to submit their analyses. The hearings were divided into two phases. During the first phase, the Commission received briefs and recommendations from individuals and organisations. During the second phase, each participant received a list of questions based on predetermined subjects to answer before the public hearings.

- Specific mandates were commissioned to about 60 experts from various disciplines. 20 task forces were formed with specifically determined duties and activities. The work produced by these experts was then analysed and discussed, and were appropriate, modified by the commissioners.

- Finally, the Commission consulted a number of organisations directly – federal and local authorities, NGOs and utility companies.

The Commission was appointed in January 1998 and submitted its final report in April 1999.

In the preparatory work toward Year 2000, Canada established a group to coordinate the development of national contingency plans in 1998, the National Contingency Planning Group (NCPG). The group was *ad hoc*, and consisted of officials on assignments from various ministries and agencies. Its tasks were to identify major critical national infrastructures and asses the risks of their potential Year 2000 failure and to prepare a national validation exercise.

The work started with the development of a national infrastructure risk assessment (NIRA), in order to give a 'snapshot' of the actual situation. Questionnaires were addressed to federal and local governments and the private sector which focused on the criticality of the infrastructure as well as the probability of compliance, failure or other incidents. The sector-wise information was then applied against other infrastructures by the NCPG.

In the second phase of the work, the NCPG developed Y2K scenarios based on the collected information and ensuing assessments, which were widely shared with stakeholders both in the public and private sector, so that they could integrate this information into their contingency planning. By the end of 1999, six NIRAs were carried out.

In the third and final phase, a large-scale exercise was carried out to validate and test the national contingency plan, which involved all concerned government agencies with voluntary participation from other organisations.

Sources: Netherlands Ministry of the Interior and Kingdom Relations, 2003; BSI, 2004; Auditor General of Canada, 1999; OCIPEP, 1999; ETH, 2004; Nicolet Commission, 1999.

(2) A specific focus on the protection of vulnerable regions or groups of population

Disasters do not affect all persons in the same manner: certain groups of the population are more exposed than others to certain hazards, or have lower coping capacities during and after the disaster. Low income, for instance, is a vulnerability–enhancing factor, which may affect both a group's exposure to hazards and its coping capacity: low income groups in urban areas often live in geographically exposed areas (to floods, landslides, etc.); in addition, they often live in low-quality housing, which risk to collapse or get seriously damaged when exposed to hazard; furthermore, their capacity to recover may be impeded by lacking financial resources (no or incomplete insurance) or lack of preparatory measures; finally, low-income groups may also lack the means to evacuate (no car, not enough money to stay in a hotel, etc.).

Income is just one of many factors that may affect a person's vulnerability to hazards. Age can be another one – especially as old age is often related to poverty, especially among women. Elderly people may also have reduced coping capacities physically (reduced capacity of hearing, reading warnings and signs and overcoming physical obstacles in a chaotic evacuation situation, in addition to illness and disability) or in terms of cognition (incapacity to use of technology and communication tools).

Other groups which may be particularly exposed to disruption and harm during disasters may be tourists and migrants, who lack the fundamental experience and tools to interpret danger signals, speak the language and take refuge.

The need for a better understanding of vulnerability and protection of vulnerable groups was tragically illustrated by the heat wave that affected Western European countries (France, Spain, UK, Portugal, Italy) in the summer 2003 and made more than 22 000 fatalities in only three weeks, essentially among the elderly (in the light of Italy's recent re-evaluation of the number of victims, fatalities are probably closer to 30 000). Excess death rates, *i.e.* compared to average fatality rates in the same population group in the same period of year, varied from 16 percent (in the U.K.) to 60 percent (in France).[25] In France, it was found that the emerging disaster was registered too late at the Ministry of Health and that subsequent communication efforts were useless since the true scale of the disaster was detected only after the event

[25] Kovats, Sari et al., 2004.

was over. The level of preparedness of the authorities was deemed inadequate, and it was estimated that lessons from two previous episodes of heat in 1976 and 1983 (albeit with less extreme temperatures and shorter durations) had not been learned. More importantly, the surveillance system proved inapt to detecting early warning signals from a particularly fragile segment of the population.

The elderly were also particularly exposed during and after the 1995 Kobe earthquake in Japan. More than half of the fatalities occurred in the population aged 60 or more, which represented 18 percent of the population in the 1990 census.[26] In addition, the scale of the catastrophe made it difficult to provide for the needs of this group in the days, weeks, and even months following the quake, during which numerous cases of unnoticed deaths due to 'shelter pneumonia' in temporary housing and of suicide occurred.[27] Health and social workers were occupied elsewhere with crisis management and the elderly without family were separated from the local community which could have offered some supplementary help and protection.

These catastrophes show that it is necessary to identify vulnerabilities and vulnerable population groups, find ways to monitor and reach these groups and integrate the data into risk and vulnerability assessments.

Regarding identification and monitoring, evaluation reports in France after the heat wave in 2003 have pointed out the need for some kind of 'inventory' of elderly persons, while indicating that this may be difficult to implement due to privacy issues.

An example of an existing, well-functioning scheme is in Denmark, where municipalities have a legal obligation to organise home visits to all persons aged 75 or more at least twice a year. In a 1999 evaluation of this practice, 80 percent of the responding municipalities reported that the scheme had helped them reach groups of 'vulnerable' elderly, which they had not formerly known.[28] Pilot projects have also been carried out in Sweden concerning outreach to the elderly. Finally, there are examples of social data (integration of population 65+) being integrated in preparedness planning among municipalities (special wards) in Tokyo.[29] After the experiences made in Kobe, Japanese authorities have re-evaluated their disaster prevention plans in later years, where specific policies concerning the elderly are spelled out. This includes measures to protect areas with a high percentage of elderly against floods or sediment-related disasters.[30]

[26] Tanida, Noritoshi, 1996, pp. 133-1135.
[27] Ibid.
[28] Den Sociale Ankestyrelse, 1999, p. 25.
[29] Uitto, Juha I., 1998, p. 13.
[30] Japanese Cabinet Office of the Prime Minister, 2004, p. 9.

Data on vulnerable populations and factors of vulnerability can be brought together in models and maps in order to facilitate preparedness and emergency response. The Energy and Resources Institute (an independent research organisation in India) in cooperation with several international partners[31] has for instance created maps that identify vulnerability levels of Indian farmers to climate change (vulnerability=monsoon dependence and dryness) and globalisation (defined as trade liberalisation – vulnerability=port distance and import-sensitive crops). The resulting maps combine regional indicators of biophysical and social vulnerability which is overlaid with indexes of climate and trade sensitivity.[32]

(3) A future-oriented approach pinpointing changes in risk patterns

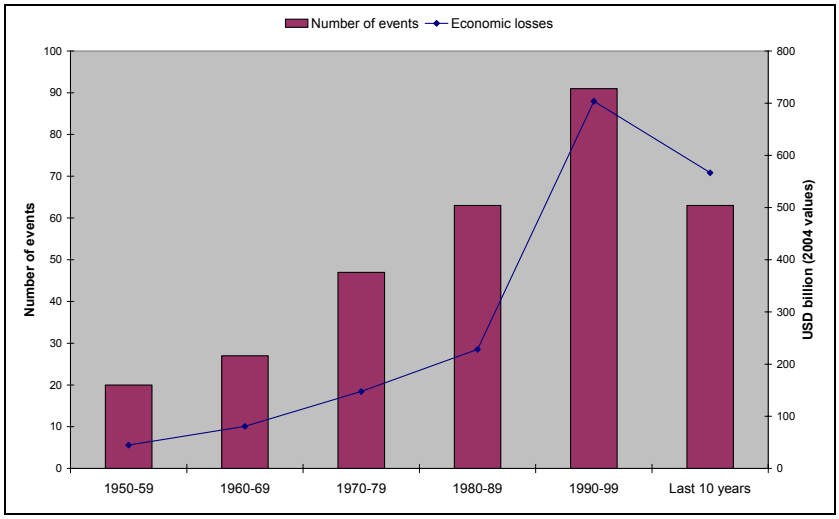
One of the most visible trends of changing risk patterns is global climate change. There has been a marked change in weather patterns during recent decades. In the past ten years, the climate has been the warmest since modern measuring began (nine of the ten last years have been the warmest since 1861[33]). Climatic phenomena such as heavy rains in parts of the northern hemisphere, warm episodes of the El Niño Southern Oscillation over the tropics, and droughts in some regions of Asia and Africa have gained in intensity and frequency.[34]

In 1992, Hurricane Andrew, the most costly natural disaster to date, hit the US coast (Florida and Louisiana) and the Bahamas. 46 persons died, and insured losses amounted to USD 21 billion (2004 value). The hurricane is reported to have destroyed 25 000 homes and damaged 100 000 others in Florida alone.[35] Good preparedness and evacuation routines probably contributed to minimise the loss of life – about 2 million people evacuated in Florida, Louisiana and Texas.[36] In the ten years following Hurricane Andrews, wind storm activity has remained high, with high accumulated insured losses in several OECD countries. In 2004, USA was exceptionally hit by four hurricanes, and Japan was hit by ten typhoons.

More frequent and intense climate-related hazards are one of the key factors behind the trend increase in losses due to natural disasters (see figure 2).

[31] Centre for International Climate and Environmental Research in Oslo (CICERO), Geography Department – Rutgers University and the International Institute for Sustainable Developments, Canada.
[32] Obrien Karen et al., n.a.
[33] Intergovernmental Panel on Climate Change, 2001, p. 3.
[34] Ibid.
[35] Rappaport, Ed, 1993.
[36] Ibid.

Figure 2 – Major natural catastrophes and economic losses, 1950-2004



Source: Munich Re, 2005.

According to the scenarios reported by the Intergovernmental Panel on Climate Change (IPCC), the global average temperature is expected to increase by an additional 1.4 to 5.8°C by 2100, causing more intense precipitation and a rise of 0.1 to 0.9 meters in the sea level. It is therefore considered likely that climatic accidents such as droughts, heavy rainfall, floods and tropical cyclones will become more frequent in the coming decades in many parts of the world. This would represent an immense challenge for unprepared policy-makers, insurers, and societies at large. For instance, increases in wind storm force may cause considerable damage to infrastructures and buildings which have been constructed to endure a lower storm category.

As demonstrated by this example, risk patterns can change in a way that makes risk management extremely difficult if prevention and preparedness strategies have not been adapted with long lead times. These changes therefore need to be tracked and gradually integrated into risk management.

Some methodologies are better than others when it comes to picking up new trends (see box 3). The 'futures' approach is increasingly used by both public and private organisations, and is often applied in the field of science and technology. In the UK, futures planning is used in public services (such as the Foresight Directorate of the Office of Science and Technology, and the Department for Environment, Food and Rural Affairs). The Foresight Directorate has among other things just finished a study on Flood and Coastal Defences, which looked at possible developments of flooding over the next 100 years in Britain, in particular in relation with climate change scenarios. The project was divided into three parts. The first part saw the elaboration of trends, drivers and scenarios for the chosen timeframe. Four different scenarios were developed, situated along two main axes of economic liberalisation and political autonomy. In the second

part, the impacts of the different scenarios on floods and coastal defences were identified, whereas the third part looked at possible responses to forestall the different developments described in the scenarios. More than 80 experts and stakeholders were consulted in the course of the project, which went over 2 years, and the main report was written by two academic experts. The project finally involved a series of mid-term reports, working papers and scientific consultation papers.

Box 3 – Methodologies for futures studies

Future planning may be closely related to risk and vulnerability assessments, as risk and vulnerability assessments with a long timeframe may have to depend on such techniques. This exercise has different names, be it 'foresight', 'futures' or 'horizon scanning', but all terms imply the systematic scanning of opportunities and threats 5, 10, 20 years ahead in time. The aim is to identify 'robust' policy options that may survive a wide range of political, economic and environmental eventualities, and try to take account for changes that are not known to us today, and which would not be identified in trend projections or extrapolations. Some techniques also make use of future 'wild cards'. Typical futures-tools such as quantitative and qualitative trend studies, Delphi surveys and scenarios are briefly described below:

Quantitative and qualitative trend analysis

The advantage of quantitative trend analysis is the objective and relatively neutral process, and its capacity to provide rapid results which can give an overview of the future situation for several issues. However, it is important to take the output for what it is – an extrapolation or projection of existing trends.

Where there is less data available (for instance sociological, cultural and political trends) qualitative trend analysis may be used. The Performance and Innovation Unit of the UK Cabinet Office proposes the following methodology:

1) Develop at conceptual framework of the forces at play.

2) Identify what is known and unknown about these forces with support of theoretical frameworks (if existing), and seek out any relevant information.

3) Derive an alternative future.

Delphi surveys

Delphi surveys are carried out inside a panel of experts, by which a questionnaire is circulated anonymously, each expert sees the reply of the others and has the chance to modify his/her response. Thus the questionnaire is circulated several times. The method is for instance used in technological forecasting.

Scenarios

Identify key concerns. Create different scenarios according to key concerns and uncertainties identified for a certain time span. Try to make the scenarios as internally coherent and plausible as possible, while covering a large span of eventualities. This will be the *possibility space.* Analyse the impact of the different scenarios on the key concerns and analyse the implications for policy. It is important to try to be creative, and remember that the exercise is more about testing the robustness of policies under a wide range of different conditions, than predicting the future.

Source: UK Cabinet Office Performance and Innovation Unit, 2001.

(4) The magnitude of risks in locations with a high density of people, activities and assets

In various occasions over recent years, natural and man-made hazards, some of a new kind and some traditional, have caused large-scale disasters. The most notable example is the terrorist attacks against New York and Washington on 11 September 2001, which took more than 3 000 lives and caused economic losses of about USD 90 billion (2001 value), of which 30 billion were insured.[37] The effects of the attacks were staggering both in terms of local societal impact (business interruption, infrastructure breakdowns in transport and communications) as well as the impact on international capital markets.

The Kobe earthquake of 17 January 1995 is another mega-event, which was even more devastating in terms of human losses (more than 6 000) and with estimated economic losses exceeding USD 100 billion (1995 value).[38] For the first time in history, an earthquake took place directly underneath the centre of a densely populated urban area. The geographically isolated location of Kobe made the relief efforts difficult, and local rescue and medical services were overwhelmed by the amount of persons who needed medical attention and provisional shelter, while at the same time carrying out rescue operations. It took a week to restore electricity, while water services were not fully restored until the end of March.[39]

In cases such as these, the impact of natural and man-made disasters has been amplified by the concentration of people, activities and assets which has accompanied the urbanisation process in OECD countries – and increasingly in the developing countries. In 2006, the global urban population will for the first time in the world's history surpass the rural population. Whereas there was only one city with more than 10 million inhabitants in 1950 (New York), there were seven with more than 15 million inhabitants in 2000, and seven cities are projected to have more than 20 million inhabitants in 2015.[40]

The 2005 tsunami in the Indian Ocean provided another perspective on the issue of large-scale disasters. It is among the most devastating natural catastrophes in terms of human losses in the past 50 years with more than 280 000 fatalities. The ensuing rescue operation was a great challenge both for local authorities and for the administrations who tried to manage the operation from abroad, many of which were completely unprepared for an event of such a magnitude. While the tsunami represented a major catastrophe for the countries that it affected, it also shed light on a new challenge for OECD countries: these countries discovered that thousands of their nationals can be concerned by a threat at the other side of the planet, where the governments have very limited intervention capacities – hence a complete discrepancy between needs and means.

[37] Swiss Re, 2002, p. 3, and OECD, 2005.
[38] Munich Re, 2005, p. 24.

The large-scale disasters of the recent years emphasise the need to confront risks of an unprecedented scale in areas with a high density of people and wealth. This has at least two sets of practical consequences for risk management:

1. In addition to the huge direct damage, one of the distinctive features of such 'mega-risks' is the magnitude of secondary effects on infrastructures, economic activities, trade, etc. Risk assessment and the design of prevention and mitigation measures need to consider more consistently the possibility of hazards with low probability and very high impacts.

2. Such events can easily overwhelm the coping and response capacities of a region or even a country. They call for creating or enhancing platforms of cooperation at the regional and international level.

The World Conference on Disaster Reduction has suggested a series of measures to strengthening local resilience to disasters and to improve international relief efforts. In the Action Plan 2005-2015 there is particular emphasis on ensuring that disaster risk reduction is a local priority; identification, assessment and monitoring of disaster risks; building a culture of safety and resilience; reduction of underlying risk factors; and strengthening disaster preparedness. Regional and international cooperation is encouraged, especially when it comes to monitoring trans-boundary hazards, information exchange and early warning. In some cases this will lead to the creation of new monitoring schemes, as is planned with tsunami warnings in the Indian Ocean.

Regarding risk-sharing and the insurance of mega-risks, a major challenge is the heightened risk of large-scale terrorist attacks, which in addition to their devastating consequences, are very difficult to anticipate. The OECD has initiated work in this field, with a special Task Force established by the Pensions and Insurance committee, which was requested in 2002 by OECD governments to carry out "policy analysis and recommendations on how to define and cover terrorism risks and to assess the respective roles of the insurance industry, financial markets and governments, including for the coverage of 'mega-terrorism risks'."[41] In its recommendations, the Task Force puts forward as a possibility the creation of a regional risk-sharing scheme with participation of both private and public actors, but also notes that there is considerable resistance to this among several OECD governments. One such proposal by the *Comité*

[39] City of Kobe, n.a.
[40] Munich Re, 2004 (b), p. 10.
[41] OECD, 2005, op. cit., foreword.

Européen des Assurances (CEA) to set up a multi-layered public-private partnership scheme at the European level was rejected in November 2001.[42]

(5) The need to monitor hazard propagation mechanisms

The last decade saw the renewed threat of communicable diseases, with SARS as the most prominent example. In seven months, between November 2002 and May 2003, SARS had spread to 30 countries on six continents and caused about 8 000 probable cases and 663 deaths.[43] The impact of SARS on Asian economies has been estimated to constitute 0.4 percentage points reduction in annual GDP for East Asia, and 0.5 percentage point reduction for Southeast Asia.[44] The World Health Organisation loosely mentions an economic loss of USD 30 billion.[45]

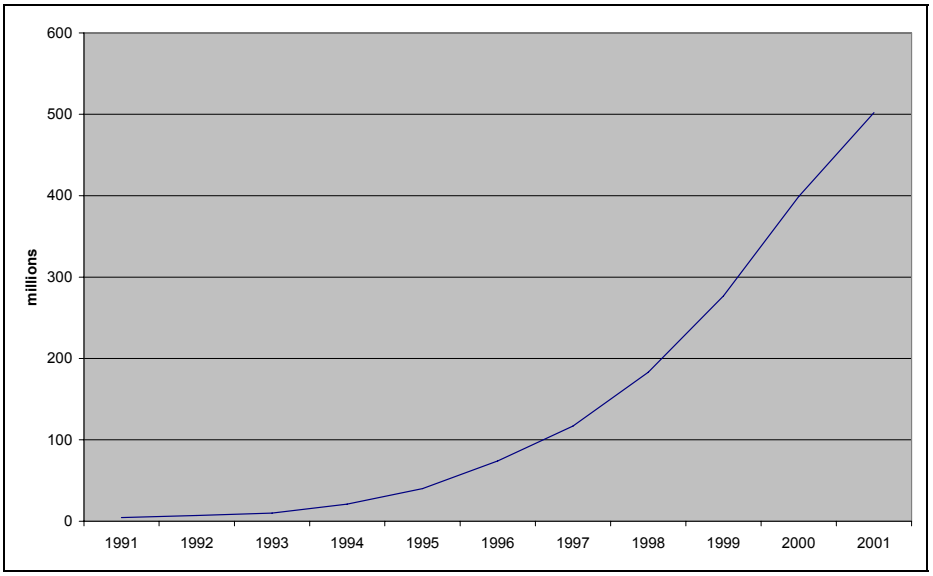
Previously, animal epidemics such as Europe's Bovine Spongiform Encephalopathy ('mad cow disease') crisis of the 1990s and British Food and Mouth Disease outbreak in 2001 had also caused considerable economic damage. These episodes demonstrate that controlling the spreading of communicable diseases can become extremely challenging in a context of free movement of people and goods.

Computer worms and viruses give a new dimension to the problem of global propagation of a local event. The explosive growth of information technologies throughout the world and the ubiquity of home computers and increasingly rapid Internet connections have created new vulnerabilities to malicious activity. For example, the Code Red and Nimda viruses propagated to a point of global saturation in less than 18 hours. Code Red reportedly reached a spreading rate of more than 50 000 computers per hour.[46] The cost estimates of such virus attacks are notoriously unreliable, but according to two different information security consultant firms, Code Red caused between USD 2.62 and 2.75 billion of damage.[47]

Technological developments and in particular the rapid digitalisation of societies play an important role both in protecting against hazards and well as creating new vulnerabilities. Computer penetration in Western countries has more than quadrupled between 1990 and 2001, if measured by households' access to a home computer. The global spread of the Internet is even more impressive (see figure 3). The number of Internet users in the world rose from 4.4 million in 1991 to 502 million in 2001. The use of broadband and mobile telephones are examples of other technologies that have spread rapidly.

[42] Ibid., p. 90.
[43] World Health Organisation, 2003, p. 2.
[44] Fan, Emma Xiaoqin, 2003.
[45] World Health Organisation, op.cit., p. 2.
[46] NSA, 2003.
[47] US Congressional Research Service, 2004, p. 12

Figure 3 – Global Internet users, 1991-2001



Source: International Telecommunications Union, 2001.

One of the reasons why local events can spread so rapidly at the international level is the lack of international tools to monitor events and to police malicious activity, a gap that various efforts at national and international levels have tried to close.

International strategies to combat infectious diseases have undergone important changes. The long-standing traditional approaches to containing outbreaks were essentially defensive in nature (brick wall methods) which tried to secure borders against invasion by emerging infectious diseases. More innovative approaches are now in use; these consist of early warning surveillance systems, plans for epidemic preparedness, stockpiles of vital medicines and materials, and communication and sharing of information through networks. Under the framework of the International Health Regulations, for example, WHO – together with its partners – is committed to the systematic collection of epidemic intelligence, rapid verification and the co-ordination of international response. It is in daily contact with its 191 member states, and every year around 200 outbreaks of potential international importance (e.g. cholera, meningitis, haemorrhagic fevers, anthrax) are actively verified.

When it comes to IT security, most governments and many private organisations have established so-called CERTs (Computer Emergency Response Teams) which have a crucial role both when it comes to detecting and responding to incidents. Many CERTs are linked together in an international network, FIRST (Forum of Incident Response and Security Teams), which has both public and private members, for information

exchange. The Cyber Convention of the Council of Europe also aims at supporting law enforcement at the international level.

Development and implementation issues

The way the process of risk and vulnerability analysis is handled is at least as critical as methodological considerations for the accuracy and relevance of the final outcome. Analyses must be kept updated and effectively integrated in policy-making, close links must be created with the private sector to obtain a complete picture of existing risks and vulnerabilities, and the issue of risk acceptance needs to be thoroughly discussed with all societal stakeholders. This section explores the ensuing challenges for elaborating vulnerability assessments.

(1) Vulnerability assessment as an ongoing process, embedded in risk reduction strategies

The previous section has shown how it is necessary to monitor evolutions in the risk landscape regularly, and to re-assess the consequences in terms of risk and vulnerability. How can this be carried out practically? Which structures are necessary and how can interest and cooperation be ensured at a decentralised level? How to ensure a governmental 'uptake' of the assessment, *i.e.* that the process leads to actual measures, implementation of change and, if need be, re-allocation of responsibilities and resources among government actors?

In recent years, and particularly in the aftermath of the 11 September 2001 events, many OECD countries have engaged broad reflections on the changing risk landscape and their vulnerabilities in that context. Canada, Denmark, the Netherlands, Norway, Sweden and the United States are prominent examples.

These reflections have often led to changes in the countries' risk management strategies, with an increased focus on the detection and assessment of hazards and vulnerabilities. One example is the Netherlands, where an initial project on Critical Infrastructure Protection emphasised the importance of continuous attention, and processes were set to continue in the ministries after the end of the project in June 2004.[48]

Some countries have placed a strong emphasis on developing the capacity to evaluate and analyse past experiences and draw lessons for policy-making In Sweden, the NCO in the Swedish Rescue Services Agency holds such a function.

The Norwegian cross-ministerial report 'A vulnerable society' (*Sårbarhetsutredningen*) is an interesting case in point. The launch of the report in 2000 triggered a number of investigations (including a governmental White Paper) and policy reforms in areas such as Critical Infrastructure Protection, and also

[48] Netherlands Ministry of the Interior and Kingdom relations, 2004, p. 5.

led to institutional change – although not entirely following the recommendations of the report regarding the creation of an overarching ministerial department dedicated to emergency preparedness, similar to the American Department of Homeland Security. Instead, main coordinative responsibility was given to the Ministry of Justice and the Police, and the Directorate of Civil Protection and Emergency Preparedness was established. In the field of information security, for instance, the government introduced important changes in the institutional framework with the creation of a National Information Security Coordination Council (KIS), of a Digital Warning Infrastructure (VDI), and a Centre for Information Assurance (SIS). However, these changes, as well as the government's overall strategy for information security, are reappraised on a regular basis, in the light of rapidly-changing conditions in the area of information security.[49]

In a different but related area, the UK government launched in 1999 the second round of the Foresight Programme, aimed at identifying opportunities for the economy or society from new science and technologies, or evaluating how future science and technologies could address key future challenges for society. However, the programme, which came directly after a five-year first, round, led to a certain foresight 'fatigue' among government agencies.[50] The first two rounds had consisted of several panels and task forces, and especially the second round had a very wide scope investigating innovation in science and technology and the implications for education, skills and training and sustainable development.[51] It was found that there was too much focus on process – networking and high meeting activity – with short and not very informative written outputs.[52] In response to the critique, the third and fourth current rounds have returned to the original focus on technology, and overlapping projects have been chosen over standing panels.

These experiences yield two important messages regarding the implementation of a risk and vulnerability assessment capacity within the government, irrespective of the institutional context in which this occurs (creation of new structures, etc.). First, strong expertise needs to be developed at the central level, and implemented at a decentralised level in a consistent manner. Consultancy and auditing responsibilities can be assigned for this.

Second, the process needs to give decentralised services the opportunity to provide feedback, so that assessments are oriented according to the needs and the observations of "field" managers.

[49] Norwegian Government of Defence et al., 2003.
[50] Joint Research Centre, 2002, p. 29.
[51] Information from www.foresight.gov.uk
[52] Joint Research Centre, 2002, op. cit., p. 29.

(2) Cooperation with the private sector

There is a wider set of problems related to involving the private sector. National vulnerability is to a great extent determined by the preparedness level of the national critical infrastructure, which is to a varying but steadily increasing degree privately owned or operated. In the United States, about 80-90 percent of the critical infrastructure is owned or operated by private businesses.[53] The increasing share of private infrastructure ownership and operation poses a number of challenges to national vulnerability assessments.

A prominent problem is information-sharing between private operators and governmental agencies. For various reasons, infrastructure owners may have incentives to withhold information about safety and security breaches, from the protection of trade secrets and other sensitive data to the possible consequences for their image and reputation. Coming from infrastructure sectors which are increasingly linked and interdependent, such a bias might represent a serious issue for national risk management. In areas such as finance or information security, publicised failures may dampen consumer confidence and be used by competitors. In American computer crime surveys, about half of all respondents are found not to report breaches to authorities or legal councils, with more than 50 percent explaining that this would hurt their image.[54]

As emphasised in the previous section, the sharing of tasks between government and the private sector in the protection of critical infrastructures is an important element of the vulnerability picture which needs to be thoroughly analysed and assessed. The issue also has important implications regarding the process of elaborating a national vulnerability assessment. Private companies, and in particular owners and operators of critical infrastructures, have access to data which are highly relevant to an evaluation of the potential threats a nation is exposed to, and its vulnerabilities. The collection and sharing of that data is paramount to conducting useful analyses and obtaining an as complete overview of risk and vulnerability as possible. This requires the establishment of cooperation structures with the private sector and formal routines for how to handle and use shared information.

Information Sharing and Analysis Centres (ISACs) have become common in many countries in order to create trust, both within private sectors and between private and public actors, and to facilitate flows of information. Still, the survey conducted by Computer Week showed that less than 10 percent of the respondents reported breaches to their ISAC.[55] An evaluation conducted by the US General Accounting Office (GAO) in 2001 proposed measures to improve and facilitate information-sharing. This included in

[53] US surface transportation ISAC, n.a.
[54] CSI/FBI, 2004, p. 14.
[55] Hulme, George, 2002.

particular the establishment of agreements on what to do with the information (standards of protection and dissemination, establishment of secure communication mechanisms) as well as ensuring that the information flow is not one-way, but that there is a real exchange.[56] The fact that government agencies perform poorly in vulnerability detection themselves can discourage private disclosure of incidents.[57] The carrying out of vulnerability analyses among public agencies may therefore have as positive side-effect to act as incentive for the private sector to share information.

A second major issue is how to encourage private infrastructure owners and operators to maintain high levels of preparedness and conduct vulnerability analyses themselves. This is particularly problematic when taking into account the fact that safety and security are long-term investments which might not be justified on the basis of short-term costs and benefits, and which in addition involve positive externalities (i.e. the costs of security investment are private, whereas the benefits in terms of increased level of security are partly captured by society).

One way to approach this problem is to improve the access to data on the costs of inadequate preparedness, in order to persuade by economic means the benefits of protection. This is one of the anticipated positive effects of improved information-sharing among critical infrastructure operators and owners with the public sector. The carrying out of risk and vulnerability analyses can also be imposed by regulation. An additional response might be for the government to subsidise certain security expenses which are beneficial to society as a whole. The challenge in this case is to determine the level of security that a private operator should assure as part of its normal business ('due diligence') and additional reductions in risk that the government might finance in order to meet specific national needs.

(3) The necessity of a dialogue with society

The final outcome of an assessment of risks and vulnerabilities should be management decisions regarding the reduction or acceptance of those risks and vulnerabilities, and the sharing of related costs. The fundamental issue, here, is the level of risk that society is willing to face, i.e. risk acceptance.

The variety of persons who are concerned by risk decisions – public officials, experts in risk analysis, interested and affected parties, and possibly the public at large – may be exposed to a range of possible consequences. Sometimes, the impacts on social, ethical, or ecological values are at least as important as those to health and safety. The analysis serving as the basis for a risk management decision therefore must pay adequate attention to all significant facets of risk. To ensure that all relevant facets of risks are

[56] US General Accounting Office, 2001, p. 18.

considered, all concerned parties need to be directly involved in formulating the problem to be analysed and reviewing the available management options.

The literature on the behavioural and societal dimensions of risk shows that in this regard, it is crucial to have a two-sided communication process: scientific and technical expertise is used to clarify the known facts about risks; but at the same time, the uncertainties and value-laden assumptions are clearly identified, so that all stakeholders can bring their contribution to a balanced evaluation of risk. In the words of the United States' National Research Council: such a process builds equally on analysis and deliberation.[58] Analysis uses rigorous methods developed by experts to arrive at answers to factual questions. Deliberation uses processes such as discussion, reflection and persuasion to communicate, raise and collectively consider issues, increase understanding, and arrive at substantive decisions. Analysis brings new information into the process; deliberation brings new insights, questions, and problem formulations. The process of bringing analysis and deliberation together and presenting the results to policy-makers is often referred to as risk characterisation, which is defined by the National Research Council as "a synthesis and summary of information about a hazard that addresses the needs and interests of decision makers and of interested and affected parties."[59]

Examples of consultations with a broad range of stakeholders abound in areas such as the siting of hazardous industrial installations or waste disposals. The consultation procedures were mainly developed in the nuclear sector, for instance concerning the clean-up after the Three Mile Island accident in 1979.The Governor of Pennsylvania then consulted two environmental organisations about planned measures, and a local mayor proposed involving local citizens in the design and operation of a radiation monitoring plan.[60] A variety of procedures have been developed since, and applied to a broader range of issues: citizen juries, panels, planning cells, consensus-building conferences, surveys, public hearings, etc.[61]

The first important step in this process is to identify the relevant stakeholders, which may prove challenging, as stakeholders are not always aware of their relevance to the assessment, or are not necessarily organised. Although there is no silver bullet to address the representation issue, a widening of the consultation process to all sectors of society and non-traditional partners of government, such as smaller NGOs and community groups can reduce the chances of excluding important stakeholders.

---

[57] Rak, Adam, 2002, p. 55.
[58] National Research Council, 1996.
[59] Ibid, p. 216.
[60] National Research Council, 1996, op. cit., p. 81.
[61] Stewart, 1995; 1997.

Second, considering that the subsequent risk characterisation process includes a wide range of stakeholders with very differing levels of experience of public consultation, it is important for the fairness of the process to provide guidance to all participants.[62]

Third and finally, the process must be designed in such a way as to provide useful input to policy-making. This means first and foremost that the assessment needs to take into account the existing policy environment and, secondly that the risk assessment process itself is firmly embedded in a decision-making process (see point (1) above).

Recognising interested and directly concerned citizens as legitimate partners in the exercise of risk assessment is no short-term panacea for the problems of risk management. But serious attention to participation and process issues may, in the long run, lead to more satisfying and successful management methods. It seems important that the government agency responsible for vulnerability analyses at the national level develop strong methodological and communication skills for doing so, and offer guidance to other government agencies and even to the private sector on this matter. Consultation processes could in particular be organised in the area of critical infrastructure protection, bringing together regulators, operators, researchers, users and other stakeholders in order to discuss the accepted level and allocation of risk in the sector, touching on issues such as minimum security levels ensured by operators and coverage of potential costs ensuing from investments to raise the level of security. A systematic and coherent consultation of all known stakeholders could supplement more traditional methods of policy-making and contribute to making risk and vulnerability assessment processes more flexible, inclusive and proactive.

[62] National Research, Council, 1996, op. cit., pp. 5-6.

Conclusion

It is increasingly acknowledged that governments are facing a series of new challenges in their duty to protect society against major natural and man-made risks. These challenges include the emergence of new hazards and fast and unpredictable changes in old threats, which blunt traditional patterns of response. In this new landscape, risk and vulnerability assessments play a considerable role. Preventing future disasters rests even more than before on an accurate evaluation of threats to society and their possible impacts. This, in turn, entails to monitor a number of key developments, to share information with all relevant sources in society, and to effectively adapt response policies to the results of the assessment.

This report indicated several elements which appear to be crucial for understanding a nation's exposure and vulnerability to hazards, at the light of the recent experience of OECD countries. Assessments must be systematic and thorough. They need to identify sectors deemed critical to the nation's safety, and integrate in their scope all national and international developments of relevance for those sectors. They must furthermore be based on sound science, with careful attention to uncertainties and other methodological issues. They must integrate a mechanism for using their outcome as inputs for day-to-day policy-making and decisions.

Most importantly, reflecting on a nation's exposure and vulnerabilities to hazards is a unique opportunity for bringing a highly technical knowledge to the citizens, and in turn for feeding policy-making and research with people's views and issues. Risk and vulnerability assessments have to be elaborated through a political process of consultation involving all important actors of society – including policy-makers, critical infrastructure operators, private businesses, representatives from the civil society, and the public. Such a process can prove a major step for building a culture of safety in society.

Bibliography

Auditor General of Canada (1999): *Chapter 25: Preparedness for Year 2000,* Ottawa.

Beredskabsstyrelsen (2003): *Endelig statusrapport om årsag, konsekvenser og tværsektorielle virkninger af strømafbrydelsen den 23. September 2003 m.v.*

BSI (2004): *Analysis of Critical Infrastructures – The ACIS methodology*, briefing document, Bonn.

Chambers, R. (1989): "Vulnerability, coping and policy", in IDS Bulletin, 20(2).

City of Kobe, information available at http://www.city.kobe.jp/cityoffice/15/020/quake/saiken/uk/chapter1.html, accessed 12 July 2005.

City of Kobe, information available at http://www.city.kobe.jp/cityoffice/15/020/quake/saiken/uk/chapter1.html, accessed 12 July 2005.

Clark W.C. et al. (2000): *Assessing Vulnerability to Global Environmental Risks*, Cambridge: Belfer Center for Science and International Affairs, Harvard University.

CSI/FBI (2004): *Computer Crime and Security Survey 2004*, San Francisco, p. 14.

Den Sociale Ankestyrelse (1999): *Rapport om kommunernes praksis ved forebyggende hjemmebesøg*, Copenhagen.

Dutch Ministry of the Interior and Kingdom Relations (2003): *Critical Infrastructure in the Netherlands*, The Hague.

Dutch Ministry of the Interior and Kingdom relations (2004): Critical *Infrastructure Protection in the Netherlands: The Dutch approach on CIP*, The Hague.

Ekström, Anna Hedin (2004): *Power Failure in Southern Sweden and Denmark, September 23, 2003*, briefing document, Crismart, Swedish National Defence College.

Fan, Emma Xiaoqin (2003): "SARS: Economic Impacts and Implications", Economic and Research Department Series, No. 15, Asian Development Bank, Manila.

FAO/WHO (2003): *Recommended international code of practice: General principles of food hygiene*, Codex Alimentarius 1 B: basic texts, CAC/RCP 1-1969, Rev.4- 2003.

Grossi and Kuhnreuter (2005): *Catastrophe Modelling: A New Approach to Managing Risk,* Springer.

Hulme, George (2002): "With friends like this", Information Week, 8 July 2002, available at http://www.informationweek.com/story/IWK20020705S0017, accessed 26 May 2005.

Intergovernmental Panel on Climate Change (2001), *Climate Change 2001: The Scientific Basis*, Contribution of IPCC Working Group 1 to IPCC Third Assessment Report.

International Organization for Standardization (1999): "Safety Aspects: Guidelines for Their Inclusion in Standards", ISO/IEC Guide 51, Geneva.

International Organization for Standardization (2002): “”Risk Management- Vocabulary – Guide for use in standards”, ISO guide 73:2002, Geneva.

International Organization for Standardization (2004): “Management of information and communications technology security Part 1: Concepts and models for information and communications technology security management”, ISO/IEC 13555-1:2004, Geneva.

International Telecommunications Union (2001): *Key Global Telecom Indicators for the World Telecommunications Service Sector*, Geneva.

Japanese Cabinet Office of the Prime Minister (2004): *Annual Report on the Aging Society: 2004*, available at http://www.cao.go.jp/whitepaper-e.html, accessed 11 July 2005.

Joint Research Centre (2002): *A Trans-National Analysis of Results and Implications of Industrially-oriented Technology Foresight Studies*.

Klaassen and Cheng (2003): *Estimation of Severe Ice Storm Risks for South-Central Canada,* p. 8Office of Critical infrastructure Protection and Emergency Preparedness, Ottawa.

Kletz, Trevor A. (1997): “Hazop – past and future”, in *Reliability Engineering and System Safety,* Vol. 55..

Kovats, Sari et al. (2004): “Heatwave of August 2003 in Europe: provisional estimates of the impact on mortality”, Eurosurveillance, Volume 8/Issue 11.

Major, J.A. (2002): “Advanced Techniques for Modeling Terrorism Risk”, in Journal of Risk Finance, Fall.

Munich Re (2004(a)): *Topics GEO 2003*, Munich.

Munich Re (2004(b)): *Megacities – Megarisks: Trends and challenges for insurance and risk management*, Munich.

Munich Re (2005): *Topics GEO* 2004, Munich.

National Research Council (1996), *Understanding Risk: Informing Decisions in a Democratic Society*, Washington, D.C.: National Academy Press.

Nicolet Commission, 1999, summary available at www.msp.gouv.qc.ca\secivile\dossiers\verglas\.

Norwegian Government of Defence et al. (2003): *National Strategy for Information Security: Challenges, Priorities and Measures*, Oslo.

Obrien Karen et al. (n.a.): “Vulnerability of Indian Agriculture to Climate Change and Economic Changes”, in Dharmaji, Bhujangarao et al. (eds.): *Mainstreaming Biodiversity and Climate Change*, The World Conservation Union (IUCN), Sri Lanka.

OCIPEP (1999): “National Planning for Y2K”, in *Emergency Planning Digest,* Volume April-June.

OECD – NEA (1992): “The Role of Quantitative PSA Results in NPP Safety Decision-Making”, Statement by Principal Working Group 5 on Risk Assessment, Committee of the Safety of Nuclear Installations, Paris.

OECD (2001): "Hazard/Risk Assessment for Agricultural Pesticides: Probabilistic Risk Assessment", Working Group on Pesticides, Joint Meeting of the Chemicals Committee and the Working Party on Chemicals, Pesticides and Biotechnology, Paris.

OECD (2003): *Emerging Systemic Risks: An Agenda for Action*, OECD, Paris.

OECD (2005): *Policy Issues in Insurance No. 9: Terrorism Risk Insurance in OECD Countries*, OECD, Paris.

Rak, Adam (2002): "Information Sharing in the Cyber Age: A Key to Critical Infrastructure Protection, Information Security Technical Report, Vol. 7, No. 2.

Rappaport, Ed (1993): *Preliminary Report: Hurricane Andrew, 16-28 August, 1992*, National Hurricane Center.

Rausand and Høyland (2004): System Reliability Theory: Models, Statistical Methods, and Applications, Wyler.

Rausand, Marvin (n.a.): "What is preliminary hazard analysis?" supplement to Rausand and Høyland, 2004, available at http://www.ntnu.no/ross/srt/slides/pha.pdf, accessed 14 December 2005.

Stewart, J. (1995): *Innovation in Democratic Practice,* Birmingham: INLOGOV.

Stewart, J. (1997): *Further Innovation in Democratic Practice,* School of Public Policy, University of Birmingham.

Swiss Re (2002): "Terrorism – dealing with the new spectre", Swiss Re Focus Report, Zurich, p. 3

Swiss Re (2004): Sigma, 1/2004, Zurich.

Tanida, Noritoshi (1996): "What happened to elderly people in the great Hanshin earthquake", British Medical Journal, 313, pp. 133-1135.

Udvalget for National Sårbarhedsudredning, (2004): *National Sårbarhedsudredning*, Birkerød.

Uitto, Juha I. (1998): "The geography of disaster vulnerability in megacities", in *Applied Geography, Vol. 18, No. 1*.

UK Cabinet Office Performance and Innovation Unit (2001): *A Futurist's Toolbox: Methodologies in Futures Work*, London.

United States Coast Guard (n.a.(a)): An overview of frequently used methods can be found at http://www.uscg.mil/hq/g-m/risk/e-guidelines/rbdm.htm, accessed 14 December 2005.

United States Coast Guard (n.a.(b)): Risk-based Decision-making Guidelines, Volume 3, available at http://www.uscg.mil/hq/g-m/risk/e-guidelines/RBDM/html/vol3/12/v3-12-cont.htm, accessed 2 December 2005.

United States Environmental Protection Agency (1998): *Guidelines for Ecological Risk Assessment,* Washington D.C.

United States National Oceanic and Atmospheric Administration (n.a.): information on community vulnerability assessments, available at www.csc.noaa.gov/products, accessed 15 December 2005.

United States National Security Agency (2003): Statement by Wolf, D.G director of information assurance, NSA, statement before Congress, Hearing on Cybersecurity – "Getting it right". July 22, 2003.

US Congressional Research Service (2004): *The Cost of Cyber Attacks*, Washington D.C.

US General Accounting Office (2001): Information Sharing: Practices That Can Benefit Critical Infrastructure Protection, Washington.

US surface transportation ISAC (n.a.): www.surfacetransportationisac.org, accessed 24 May 2005.

Woo (2002): *Quantifying Insurance Terrorism Risk*, prepared for the National Bureau of Economic Research meeting, Cambridge, Massachusetts, 1 February.

World Health Organisation (2003): *Severe acute respiratory syndrome (SARS): Status of the outbreak and lessons for the immediate future*, Geneva.

Annex 1: Members of the Steering Group

DENMARK:
Niels JACOBSEN
Head of Section
Danish Emergency Management Agency

Niels MADSEN
Senior Advisor
Danish Emergency Management Agency

Dorte JUUL MUNCH
Head of Section
Civil Sector Preparedness Division
Danish Emergency Management Agency

Henrik Grosen NIELSEN
Head of Division
Emergency Management Division
Ministry of the Interior and Health

Signe RYBORG
Head of Unit
Ministry of the Interior and Health

FRANCE:
Geneviève BAUMONT
Secrétaire du Comité de la Prévention et de la Précaution
Direction des études économiques et de l'évaluation environnementale
Ministère de l'Ecologie et du Développement Durable

Antoine BOISSON
Bureau de l'évaluation des normes et de la sécurité environnementale
Direction des études économiques et de l'évaluation environnementale
Ministère de l'Ecologie et du Développement Durable

Annie ERHARD-CASSEGRAIN
Bureau de l'évaluation des normes et de la sécurité environnementale
Direction des études économiques et de l'évaluation environnementale
Ministère de l'Ecologie et du Développement Durable

Emmanuel MASSE
Bureau de l'évaluation des normes et de la sécurité environnementale
Direction des études économiques et de l'évaluation environnementale
Ministère de l'Ecologie et du Développement Durable

ITALY:
Andrea SANTUCCI
Directorate for Environmental Protection
Ministry of the Environment and Land Protection

Maria GRAZIA COTTA
Directorate for Soil Defence
Ministry of the Environment and Land Protection

Francesco TORNATORE
Basin Authority of Po river

Donato DI MATTEO
Head of Division for Industrial Risks
Directorate for Environmental Protection
Ministry of the Environment and Land Protection

Alicia MIGNONE
Science Attaché
Permanent Delegation of Italy at the OECD

JAPAN:
Kotaro NAGASAWA
Director of Europe Office
Infrastructure Development Institute

Yoshiyuki IMAMURA
Programme Specialist,
Division of Water Sciences, UNESCO

Takashi NAKAJIMA
Deputy- director of Europe Office
Infrastructure Development Institute

Kazuo UMEDA
Director of 2nd Research Department
Infrastructure Development Institute

Masaru KUNITOMO
Assistant Director for International Affairs,
River Planning Division, River Bureau
Ministry of Land, Infrastructure and Transport

Hideki HIRAI
Counsellor For Disaster Management
Cabinet Office

NORWAY:
Dagfinn BUSET

Adviser, Emergency Planning Unit
Rescue and Emergency Planning Department
Norwegian Ministry of Justice and the Police

Hilde Bostrøm LINDLAND
Project Manager
Directorate for Civil Protection and Emergency Planning
Ministry of Justice and the Police

Stein HENRIKSEN
Directorate for Civil Protection and Emergency Planning
Ministry of Justice and the Police

Terje-Olav AUSTERHEIM
Directorate for Civil Protection and Emergency Planning
Ministry of Justice and the Police

SWEDEN:
Ulf BJURMAN
Head of Department/Director
Swedish Rescue Services Agency

Alf ROSBERG
Project Leader
Swedish Rescue Services Agency

Jim SANDKVIST
Director
SSPA

Oskar HANSSON
Principal Administrative Officer
Swedish Emergency Management Agency

Maria MONAHOV
Research Co-ordinator
Swedish Emergency Management Agency

Louise SIMONSSON
Research Co-ordinator
Swedish Emergency Management Agency

SWITZERLAND:
Rudolf A. MÜLLER
Conseiller scientifique
Secrétariat d'Etat à l'économie

U.S.A.:
Larry W. ROEDER, Jr.
Policy Advisor on Disaster Management
Bureau of International Organizations
US Department of State

OECD Studies in Risk Management

Denmark

ASSESSING SOCIETAL RISKS AND VULNERABILITIES

Looking back on the disasters of recent years alone (the Indian Ocean tsunami disaster, Hurricane Katrina, terrorist attacks in New York, Madrid and London, avian flu, the 2003 heat wave in Europe), one could be forgiven for thinking that we live in an increasingly dangerous world. A variety of forces are helping to shape the risks that affect us, from demographic evolutions to climate change, through the development of mega-cities and the rise of information technology. These changes are clearly a major challenge for risk management systems in OECD countries, which have occasionally proved unable to protect the life and welfare of citizens or the continuity of economic activity.

The OECD Futures Project on Risk Management Policies was launched in 2003 in order to assist OECD countries in identifying the challenges of managing risks in the 21st century, and help them reflect on how best to address those challenges. The focus is on the consistency of risk management policies and on their ability to deal with the challenges, present and future, created by systemic risks. The Project covers a range of risk management issues which were proposed by the participating countries and together form three thematic clusters: natural disasters, risks to critical infrastructures, and the protection of vulnerable population groups. In the first phase of the Project,
the OECD Secretariat prepared a case study for each issue. The studies cover both recent international developments of interest and the national policy context, and come with a tool for self-assessment to be used later in the Project in order to review the national policies in question.

This work is now published as the OECD Studies in Risk Management.

www.oecd.org