National Risk Assessments

A CROSS COUNTRY PERSPECTIVE

OECD

National Risk Assessments

A CROSS COUNTRY PERSPECTIVE

OECD
BETTER POLICIES FOR BETTER LIVES

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Please cite this publication as:
OECD (2017), *National Risk Assessments: A Cross Country Perspective*, OECD Publishing, Paris.
http://dx.doi.org/10.1787/9789264287532-en

ISBN 978-92-64-28752-5 (print)
ISBN 978-92-64-28753-2 (PDF)

Revised version, October 2018
Details of revisions available at: http://www.oecd.org/about/publishing/Corrigendum_NRA.pdf

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Photo credits: Cover © Baseline Arts.

Corrigenda to OECD publications may be found on line at: *www.oecd.org/about/publishing/corrigenda.htm*.

© OECD 2017

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgement of OECD as source and copyright owner is given. All requests for public or commercial use and translation rights should be submitted to *rights@oecd.org*. Requests for permission to photocopy portions of this material for public or commercial use shall be addressed directly to the Copyright Clearance Center (CCC) at *info@copyright.com* or the Centre français d'exploitation du droit de copie (CFC) at *contact@cfcopies.com*.

Foreword

When disruptive events occur that could have a significant impact on the population and the national economy, governments have the primary responsibility for managing them. Citizens expect governments to manage the impacts of extreme events whether they come from natural disasters, terrorist attacks, industrial accidents or disease outbreaks. How can governments invest their finite resources most efficiently to mitigate the effects of these events? Since not all hazards and threats can be prevented, important trade-offs need to be made in preparing for different types of disaster risks.

The OECD Council Recommendation on the Governance of Critical Risks calls on countries to develop risk anticipation capacity linked directly to decision making, including through the adoption of all-hazards approaches to national risk assessment. National Risk Assessments (NRA) are an essential tool for building a multidisciplinary evidence-based understanding of the major risks facing a country in the medium term. For OECD countries that are also EU members, they are a key requirement under the Union Civil Protection Mechanism legislation. At a global level, the Sendai Framework for Disaster Risk Reduction emphasises the importance of risk assessments for achieving priority one of the Framework – understanding disaster risk. This understanding can contribute significantly to building consensus across government concerning strategic investments in prevention, protection, mitigation, response and recovery. NRA help governments map risks across various sectors using a systematic, all-hazards approach. They serve as an objective reference point for setting and defending priorities. This is especially useful when there is public pressure to redress the failures of the most recent disaster, often at the expense of more pressing needs or long-term priorities. An evidence-based approach to policy making requires assessing all risks methodically, reviewing the results, and determining how well prepared or vulnerable society is. This approach can help build preparedness for most disaster risks – including emerging risks.

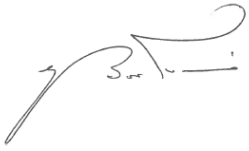
This report reviews country practices in NRA as tools for disaster risk preparedness. It identifies good practices drawn from detailed profiles of twenty countries. The country-specific analysis, presented in separate chapters, introduces the process and outcomes of NRA in different jurisdictions, and discusses the challenges faced by governments in carrying them out. These challenges tend to be related to the co-ordination of expertise across departments to produce a whole-of-government approach, which is crucial for building consensus. One solution is to engage expertise from the private sector and academia in these efforts in order to in generate objective feedback loops, avoid group-think and reduce any 'blind spots'. The findings point to the need to address governance issues related to the transparency of results and the accountability of the process.

Finally, the results emphasise the usefulness of communicating the outcomes of NRA to regional and local authorities to help them carry out risk management planning and inform the public about known risks. This will empower individuals and firms to take necessary action to reinforce business and community resilience to risks.

This thematic study is undertaken by the OECD, under the auspices of the High Level Risk Forum and in co-operation with the European Commission to study and share innovative practices in the governance of critical risks. The High Level Risk Forum brings together policy makers from governments, practitioners from the private sector, and experts from think tanks and academia to identify and share good practices and deepen their understanding of risk management.

Johannes Luchner
Director of the Crisis Management Directorate
European Commission

Marcos Bonturi
OECD / GOV



Acknowledgements

This report was prepared by the OECD Public Governance Directorate, led by Marcos Bonturi (Director). It was co-ordinated by Jack Radisch (Senior Project Manager) with the guidance of Stéphane Jacobzone (Deputy Head of the Reform of the Public Sector Division). Jack Radisch, John Tesh (Consultant) and John Roche (Policy Analyst) wrote the synthesis chapter. The country profiles were drafted by John Tesh, John Roche, Charles Baubion (Policy Analyst). Dr. Young Hoon Ahn from the Korea Research Institute of Local Administration (KRILA) provided a contribution for the Korea profile. Roberto Schiano Lomoriello provided valuable research assistance and substantive contributions to the country chapters.

This report has benefitted from the support of the European Commission's Directorate General for Humanitarian Aid and Civil Protection (DG ECHO) concerning the OECD/EU countries, as well as from the Ministry of the Interior and Safety (2017) of Ministry of Korea for the Korean profile. The Secretariat would like to thank participants at the OECD High Level Risk Forum in 2015 where experts discussed the country findings, and in 2016, where the discussion focused on the general synthesis. Particular thanks are due to all the experts from the 20 countries who provided informative results and feedback on the draft chapters. Preliminary findings from the first four country profiles were also presented at the EU Civil Protection Committee in June 2014 and the Secretariat would like to thank participants for the informative discussions.

Liv Gaunt prepared this report for publication. Kate Lancaster and Andrea Uhrhammer offered valuable editorial comments. The authors are grateful to Susan Rantalainen and Elisabeth Huggard for excellent support throughout the project.

Table of contents

ABBREVIATIONS AND ACRONYMS 13
EXECUTIVE SUMMARY 17
PART ONE: NATIONAL RISK ASSESSMENTS- A TOOL FOR GOVERNANCE OF CRITICAL RISKS 21
CHAPTER 1. THE EVOLVING PRACTICE OF NATIONAL RISK ASSESSMENTS IN OECD COUNTRIES 23
Purposes and objectives of National Risk Assessments 26
Methodologies used in national risk assessment 29
Transparency and Accountability 32
Multi-level governance and multi-stakeholder participation 33
CHAPTER 2. RISK ANALYSIS IN NATIONAL RISK ASSESSMENT 35
Scope of National Risk Assessment 37
Threat and hazard identification 38
Time Horizon 39
Impact Analysis 40
Likelihood and plausibility analysis 41
Risk monitoring and re-evaluation 42
CHAPTER 3. COMMUNICATING THE RESULTS OF NATIONAL RISK ASSESSMENTS 43
Raising public awareness about risks 44
Tools for interpreting risk analysis 47
Conclusion 49
CHAPTER 4. LESSONS LEARNT FROM DEVELOPMENT AND USE OF NRA 51
Identified benefits from the use of National Risk Assessment 52
Identified limitations to National Risk Assessments 56
Broader policy outcomes: framing risks at a higher level 57
CHAPTER 5. CONCLUSION AND AREAS FOR FUTURE ACTION 59
PART TWO: NATIONAL RISK ASSESSMENT – COUNTRY PROFILES 65

CHAPTER 6. AUSTRALIA 67
CHAPTER 7. AUSTRIA 77
CHAPTER 8. CANADA 89
CHAPTER 9. DENMARK 99
CHAPTER 10. ESTONIA 111
CHAPTER 11. FINLAND 121
CHAPTER 12. GERMANY 133
CHAPTER 13. HUNGARY 149
CHAPTER 14. KOREA 159
CHAPTER 15. THE NETHERLANDS 171
CHAPTER 16. NEW ZEALAND 183
CHAPTER 17. NORWAY 193
CHAPTER 18. POLAND 203
CHAPTER 19. PORTUGAL 215
CHAPTER 20. SLOVAK REPUBLIC 225
CHAPTER 21. SPAIN 233
CHAPTER 22. SWEDEN 241
CHAPTER 23. SWITZERLAND 255
CHAPTER 24. UNITED KINGDOM 267
CHAPTER 25. UNITED STATES 279
ANNEX A 289
ANNEX B 293
ANNEX C 297

Tables

Table 6.1. Likelihood level 71
Table 7.1. Austria's 2013 national security strategy – main classes of risk and threat 78
Table 7.2. 15 scenarios for the initial NRA 84
Table 9.1. Selected incident types 105
Table 9.2. Checklist of possible consequences of incident types in the Danish NRP 106
Table 10.1. Risk classes and risk types 116
Table 10.2. Criteria for deciding what qualifies an event as an emergency 117
Table 10.3. Measures of likelihood for risk scenarios 118
Table 11.1. Risks covered in risk scenarios 126

Table 11.2. Criteria for assessing the impact of emergencies 127
Table 11.3. Impact scale for tier 2 events..... 128
Table 11.4. Likelihood values and description..... 128
Table 12.1. Description of the reference area 138
Table 12.2. Example: 2013 Impact Assessment for "Winter Storm" 139
Table 12.3. Example: Threshold values for livestock impairment..... 140
Table 12.4. Likelihood scales..... 140
Table 13.1. Likelihood categories for hazards 154
Table 14.1. Typology of disasters in Korea..... 162
Table 14.2. Frequency of annual yellow sand..... 163
Table 14.3. Disaster events (2002~2011)..... 164
Table 14.4. Man-made incidents in a period of 2008~2010 164
Table 14.5. Number of Fatalities (2002~2011) 165
Table 14.6. Climate change impact sectors and risk criteria..... 166
Table 14.7. Measures of likelihood for risk scenarios 166
Table 15.1. Critical infrastructure and vital services..... 176
Table 15.2. Vital interests and impact indicators 177
Table 15.3. Likelihood scores 178
Table 17.1. Societal values..... 197
Table 18.1. Risk Scenarios..... 204
Table 18.2. Impact categories 210
Table 18.3. Likelihood and plausibility events 211
Table 20.1. Risks within the scope of the Slovak Republic's NRA 228
Table 21.1. 2013 National Security Strategy: Priority Areas of Action 235
Table 22.1. Five national protection values 245
Table 22.2. Indicators for the national protection values..... 246
Table 22.3. Scales for Impact Assessment 247
Table 22.4. Likelihood scales..... 248
Table 22.5. Uncertainty scale in the National Risk Assessment 249
Table 23.1. Hazards selected for the national risk assessment in 2011-2014 259
Table 23.2. Criteria for judging impact..... 260
Table 23.3. Likelihood estimation of hazards 261
Table 24.1. Assessment of the impacts..... 273
Table 25.1. SNRA National-Level Events 284

Figures

Figure 1.1. Policy objectives of the NRA 27
Figure 1.2. Typical National Risk Assessment Process 28
Figure 1.3. Inclusiveness in the NRA process 34
Figure 2.1. A Matrix for National Risk Assessment 36
Figure 2.2. Types of National Risks 38
Figure 3.1. Outcome of the NRA communicated to decision makers 46
Figure 3.2. Countries that use a risk matrix 48
Figure 3.3. Results and processes of NRA are made publicly available 48
Figure 6.1. Example of the bow tie diagram 70
Figure 6.2. The decisions that determine risk categorisation 73
Figure 6.3. Purpose and context for engagement with stakeholders – the NERAG framework 74
Figure 7.1. Indicative placing of the first 9 of 15 national risks of natural or man-made hazards in Austria's national risk assessment process 79
Figure 7.2. Austria's Cyber Risk Matrix 2011 81
Figure 7.3. Mapping the risk of mountain torrents in Austria 82
Figure 7.4. GERIAN – Scope and Concept for a NaTRAn 83
Figure 8.1. AHRA Process and Linkage to EM Planning 92
Figure 8.2. Example of Diverse Risk Event Scenarios Displayed on a Likelihood-Consequence Graph 93
Figure 9.1. Denmark's national crisis management system 101
Figure 9.2. NRP – Overall consequence assessment 108
Figure 10.1. Risk Profile (2013) 118
Figure 11.1. Serious regional accidents shown in a risk matrix 129
Figure 12.1. Assessing the likelihood of risks 142
Figure 15.1. The Netherlands Risk Diagram with logarithmic axes for the 2014 National Risk Assessment 180
Figure 16.1. Overlapping levels of responsibility for risk management action 185
Figure 16.2. Indicative National Risks 186
Figure 17.1. Bow tie model for risk analysis 198
Figure 17.2. Distribution of consequence types 199
Figure 22.1. Sweden's risk matrix 250
Figure 23.1. Stakeholders with responsibilities for disaster risk management 258

Figure 23.2. Risk matrix 2012 262
Figure 23.3. Risks matrix of frequency and damages in monetary terms 263
Figure 23.4. Risk matrix of malicious/intentional actions 263
Figure 24.1. Risk of terrorist and other malicious attack (left) Risk of natural hazards and major accidents (right) 276

Boxes

Box 1.1. Definitions of key terms 31
Box 2.1. All-hazards approach to National Risk Assessment 37
Box 2.2. National Resilience Planning Assumptions (United Kingdom) 41
Box 3.1 Risk Communication and Public Awareness 44
Box 3.2. United Kingdom: Cabinet Office Horizon Scanning 45
Box 14.1. Yellow dust storms 163

Abbreviations and acronyms

AEP	Annual Exceedance Probability
AHRA	All Hazards Risk Assessment (Canada)
AIT	Austrian Institute for Technology
ANPC	National Authority for Civil Protection (Portugal)
APCIP	Austrian Programme for Critical Infrastructure Protection
AUF	Workers' Youth League (Norway)
BBK	Federal Office of Civil Protection and Disaster Assistance (Germany)
BCPA	Business Continuity Planning Assumptions (United Kingdom)
CCS	Cabinet Office Civil Contingencies Secretariat ((United Kingdom)
CIMS	Co-ordinated Incident Management System (New Zealand)
CIP	Critical Infrastructure Programme
CNPC	National Commission for Civil Protection (Portugal)
COAG	Council of Australian Governments
CPD	Civil Protection Directorate
DEMA	Danish Emergency Management Agency
DES	Cabinet Committee on Domestic and External Security Co-ordination (New Zealand)
DESC	Domestic and External Security Co-ordination (New Zealand)
DHS	Department of Homeland Security (United States)
DRM	Disaster Risk Management
DRR	Disaster Risk Reduction
DSB	Directorate for Civil Protection (Norway)
EMA	Emergency Management Act (Canada)
EPCIP	European Programme for Critical Infrastructure
ERM	Emergency Risk Management
EUMS	European Union Member States
FCO	Flood Control Offices of the National Meteorological Administration (Korea)
FEMA	Federal Emergency Management Agency (United States)
FOCP	Federal Office for Civil Protection
FPEM	Federal Policy for Emergency Management (Canada)

GCS	Government Centre for Security (Poland)
GIS	Geographic Information Systems
GNP	Gross National Product
ICT	Information and Communications Technology
IRAWG	Interdepartmental Risk Assessment Working Group (Canada)
ISA	Internal Security Agency (Poland)
JTAC	Joint Terrorism Assessment Centre (United Kingdom)
LRFs	Local Resilience Forums (United Kingdom)
MIS	Ministry of Interior and Security (Korea)
MSB	Swedish Civil Contingency Agency
NATO	North Atlantic Treaty Organisation
NaTRAn	National Risk and Threat Assessment (Austria)
NCMP	National Crisis Management Plan (Denmark)
NCMP	National Crisis Management Plan (Poland)
NDGDM	National Directorate General for Disaster Management (Hungary)
NDMS	National Disaster Management System (Korea)
NDRA	National Disaster Risk Assessment (Switzerland)
NEMA	National Emergency Management Agency (Korea)
NEP	National Emergency Plan (Portugal)
NERAG	National Emergency Risk Assessment Guidelines (Australia)
NGO	Non-governmental Organisation
NMA	National Meteorological Administration (Korea)
NPG	National Preparedness Goal (United States)
NPS	National Preparedness System (United States)
NRA	National Risk Assessment
NRP	National Risk Profile (Denmark)
NRPA	National Resilience Planning Assumptions (United Kingdom)
NRR	National Risk Register
NSC	National Security Council
NSS	National Security System (Spain)
NSSRM	National Strategy for Security Risk Management (Slovak Republic)
ODESC	Officials' Committee for Domestic and External Security Co-ordination (New Zealand)
PHA	Preliminary Hazard Assessment tool
PNRRC	National Platform for Disaster Risk Reduction (Portugal)

QHSR	Quadrennial Homeland Security Review (United States)
REN	National Ecological Reserve (Portugal)
RVA	Risk and Vulnerability Analysis
SARS	Severe Acute Respiratory Syndrome
SEERISK	Joint Disaster Management Risk Assessment and Preparedness in the Danube Macro-Region
SKKM	Co-ordinating Committee for Crisis and Disaster Management (Austria)
SMEs	Small and Medium Enterprises
SNRA	Strategic National Risk Assessment (United States)
SNRA	Strategic National Risk Assessment (United States)
UNISDR	United Nations International Strategy for Disaster Reduction

Executive summary

National risk assessments (NRA) identify and analyse risks that have consequences of national significance. NRA help inform decisions concerning the emergency situations that require the attention of policy makers at the centre of government. They cover the entire risk management process, from analysing preparedness for different types of national risks to putting society on notice about them, and as a result are an essential tool for supporting a country's overall resilience. This report presents a unique overview of NRA across a range of countries. Part I provides a cross-country analysis distilling lessons from the use of NRA. It provides recommendations for countries that might wish to establish an NRA and can be a useful reference for countries seeking to reform their current practices. Part II of this report presents National Risk Assessment processes in 20 countries.

The value of a broad approach

In many countries, NRA cover natural hazards, infectious diseases, industrial accidents, terrorist attacks, labour strikes, cyberattacks on critical infrastructure, organised crime and the failure of institutions. Each of these risk scenarios may challenge governments to react quickly, often without warning. An all-hazards approach has proven beneficial in identifying and analysing interlinkages among natural phenomena and man-made events, and fosters the development of multidisciplinary risk scenarios.

Identifying risks with national significance

To develop a national portfolio of risks, central governments tend to adopt one of two approaches. The first approach is to conduct risk assessments from subnational levels of government, and attempt to aggregate these reports into a national inventory. This approach typically does not necessarily follow a standard analytical method, and it often misses risks that do not come under the responsibility of local authorities. These inventories based on disparate risks analysis provide no basis for discerning which risks are more or less important. A second, centralised approach brings together experts from across line ministries, and co-ordinates input to identify and assess the range of major risks according to common criteria that could have national-level significance. A few countries use both approaches, with the results of the bottom-up process serving as a starting point for the centrally managed process. They often involve:

1) Identifying and developing risk scenarios that could have national significance.
2) Scoring different risk scenarios in terms of their likelihood and consequence according to common criteria.
3) Attributing some comparative value to the risk scenarios based on the scores.

Governance of National Risk Assessments

The governance of a NRA is driven primarily by its objectives. In many countries the objective is simply to better understand risks and to inform emergency preparedness and civil contingency planning. In such cases, the process does not need to be particularly inclusive. The study found relatively few countries actually compare risks and use the results of risk analysis as a decision-making tool to guide the allocation of resources. Where this is the objective, however, a more inclusive process, whereby multiple ministries contribute to the analyses and apply a common approach, helps build consensus.

In the countries where the NRA follows a more inclusive process, expertise is mobilised from different levels of government, research institutes and academia, and even from the private sector. Broader participation helps to counter "group think", to question assumptions, and to help identify relationships among different types of risk scenarios. It provides an opportunity to designate responsibility for specific risks, and joint responsibility for complex risks that might otherwise "fall between the cracks" of government silos.

The results of NRA are typically subject to some form of oversight by higher levels of authority, but failure to accurately forecast future events does not lead to holding responsible the public officials involved in the process. Government-led reviews, audits and parliamentary hearings are sometimes held to scrutinize the results after a disaster or crisis when risk scenarios were not included in the NRA, but no official reprimands or sanctions have been issued. Such accountability measures would be unlikely to improve the quality of future NRAs, but it is still essential to learn from past mistakes. It is more important to insulate the NRA process from political meddling that would compromise its objectivity.

How can countries use NRA to communicate about national risks?

National risk assessments contain valuable information about how experts foresee a risk scenario playing out. This information might have high relevance for individual household and business decisions about where to locate or invest, or which suppliers to use. An increasing number of countries do not treat the results of NRA as classified information. Most make public at least a summary of the results to raise public awareness of risks and nudge citizens and businesses to take self-protective measures.

Independent review of the risk assessments by third parties is generally not permitted, as some of the underlying information on vulnerabilities is security-sensitive. For some countries, the results should only be communicated to policy makers and used by emergency planners, but views can differ. Some practitioners support the idea that NRA can be a tool to inform public perception of risks, even though there does not seem to be strong link between communicating NRA results and greater public trust in risk management policies. A minority of practitioners argue that it is not useful to communicate the results and that more locally targeted risk communication is needed.

Key Recommendations

- Deploy National Risk Assessments as part of a larger overall risk management strategy.
- Identify and engage stakeholders early and often.

- Adopt an all-hazards approach for National Risk Assessment.
- Use results of National Risk Assessments to inform policy decisions
- Assign clear responsibility for leading the process, and clarify risk ownership across government.
- Ensure that the methodology produces comparable results.
- Present the results to policy makers and/or appropriate legislative committees for formal adoption.
- Publish the results.
- Foster a continuous review process.

PART ONE:

National Risk Assessments - A Tool for governance of Critical Risks

Part One of this report provides a cross country analysis of the state of play in national risk assessments. It draws lessons on the process, governance and use of national risk assessments across some twenty OECD countries, and makes recommendations to countries that might wish to establish a national risk assessment in future.

Chapter 1. The evolving practice of National Risk Assessments in OECD countries

This chapter presents the purpose of conducting a national risk assessment, highlighting practices for country risk managers who wish to learn from the experiences of other countries.

Introduction

Beginning in the first decade of the 2000's a few OECD governments, mostly in the northern part of Europe and North America, began to develop a portfolio view of 'all-hazards' facing their national territory that could eventually result in major civil contingencies. The motives for these initiatives varied across countries, and in some cases overlapped, and could be categorised as: 1) the need for a systematic approach to risk identification whereby blind spots could be filled-in following a major civil contingency that revealed a lack of preparedness for certain risks; 2) the need for a comprehensive approach to preparedness that assesses different types of risks according to a common set of criteria (such as those linked to natural hazards and terrorist acts), and build consensus across ministries concerning priorities for investments in risk management measures; and 3) the need to better understand linkages between different types of risks, both in terms of causality (such as Natech risks) and to fully understand how capabilities developed to treat the consequences of one type of risk can in fact be useful to respond to many different types of risks.

Since 2009, the OECD has promoted "National Risk Assessments" (NRA) as good practice in country risk management, and they have become increasingly used as a policy tool to identify and analyse a range of events that could cause significant disruption at a national scale.[1] The first countries to perform NRA compared the relative likelihood and consequences of events as diverse as major floods, earthquakes, heat waves, terrorist attacks, civil unrest, pandemics and industrial accidents. With each new iteration the list of disaster scenarios assessed continues to expand, and now includes such diverse major risks as, inter alia, geomagnetic storms, organised crime, tsunamis, sand storms, and volcanic ash and gas clouds.

These pioneer countries were invited to share their practices and discuss their respective results at the OECD in the context of the newly created High Level Risk Forum starting in 2011. In a context where civil protection organisations were increasingly called on to enhance national resilience, interest grew in learning the processes used to plan about risks in a strategic way. By broadening their understanding of what could go wrong in their national territory, the process has been increasingly perceived as an opportunity to identify the capabilities needed to manage disaster impacts, and to analyse the extent to which those capabilities have already been developed.

At European level, the European Commission first issued a Staff Working Paper on Risk Assessment and Mapping Guidelines for Disaster Management in 2010. The goal was "to improve coherence and consistency among the risk assessments undertaken in the Member States at national level in the prevention, preparedness and planning stages and to make these risk assessments more comparable between Member States".[2]

A watershed moment for global interest in national risk assessment came during the Mexican Chairmanship of the G20, when experts from a set of countries that were active in the OECD High Level Risk Forum developed a G20/OECD Methodological Framework for Disaster Risk Assessment and Risk Financing in 2012.[3] This G20/OECD methodological framework concluded that country risk assessment is a critical foundation for disaster risk management and related financial strategies and requires clear rules and governance. In particular, the framework concluded that:

- Risk assessment needs to be comprehensive and well-orchestrated both within government and with stakeholders, requiring a robust governance process and framework;

- Agreed definitions and rules are needed to ensure consistent and reliable outcomes;
- Risk assessment outcomes need to be communicated to decision-makers and the public;
- Establishing a solid evidence base through the collection of data on hazards, exposures, vulnerabilities and losses is crucial to this effort and disaster risk management strategies overall.

The G20 framework established significant momentum at the international level enabling a forum for numerous countries to learn from the success of national risk assessments, and to consider how to develop such a process in their own countries. The G20 framework also offered complementary recommendations in terms of financial resilience, as it was developed as part of the G20 finance track.

This momentum carried forward to decision n° 1313/2013/EU of the European Parliament and of the council of 13 December 2013 on a Union Civil Protection Mechanism, which calls on Member States to develop risk assessments at national or appropriate sub-national level and to make these assessments available to the Commission by end of December 2015. That decision called on the Commission to develop guidelines, together with the Member States, on the content, methodology and structure of these assessments. This decision is to be evaluated by 2021. The Risk Management Capability Assessment Guidelines were subsequently issued in 2015 (2015/C261/03) and they explicitly recognise that the OECD recommended that methods be defined to support all stakeholder levels in determining acceptable levels of risk and that these methods and results be subject to transparent publication to raise awareness among all stakeholder groups.

The OECD adopted the Recommendation on the Governance of Critical Risks in 2014, which calls on countries to build preparedness through foresight analysis, risk assessments and financing frameworks, to better anticipate complex and wide ranging impacts, with the need to develop risk anticipation capacity linked directly to decision making. [4] In this context it calls on countries to, "adopt all-hazards approaches to national risk assessment to help prioritise disaster risk reduction, emergency management capabilities and the design of financial protection strategies". This momentum led to a wide range of countries experimenting and implementing national risk assessment and to a strong message on their utility at the World Conference on Disaster Risk Reduction in Sendai, Japan in 2015.

Analytical framework of the study

The information for this study was collected through a mix of questionnaires and panel interviews. The OECD Secretariat interviewed government officials with direct responsibility for coordinating their country's National Risk Assessment between 2013-2016. The questions used in the interviews were structured around good practices and policy guidance issued by the OECD in the context of the G20 as well as the European Union. This includes the G20/OECD Analytical Framework on Disaster Risk Assessment and Disaster Financing, and the European Commission Staff Working Paper on Risk Assessment and Mapping Guidelines for Disaster Management. The analytical framework for the interviews was developed before adoption of the OECD Recommendation of the Council on the Governance of Critical Risks. The information

contained herein reflects the state of National Risk Assessment in countries at the time information was collected from the various countries.

Purposes and objectives of National Risk Assessments

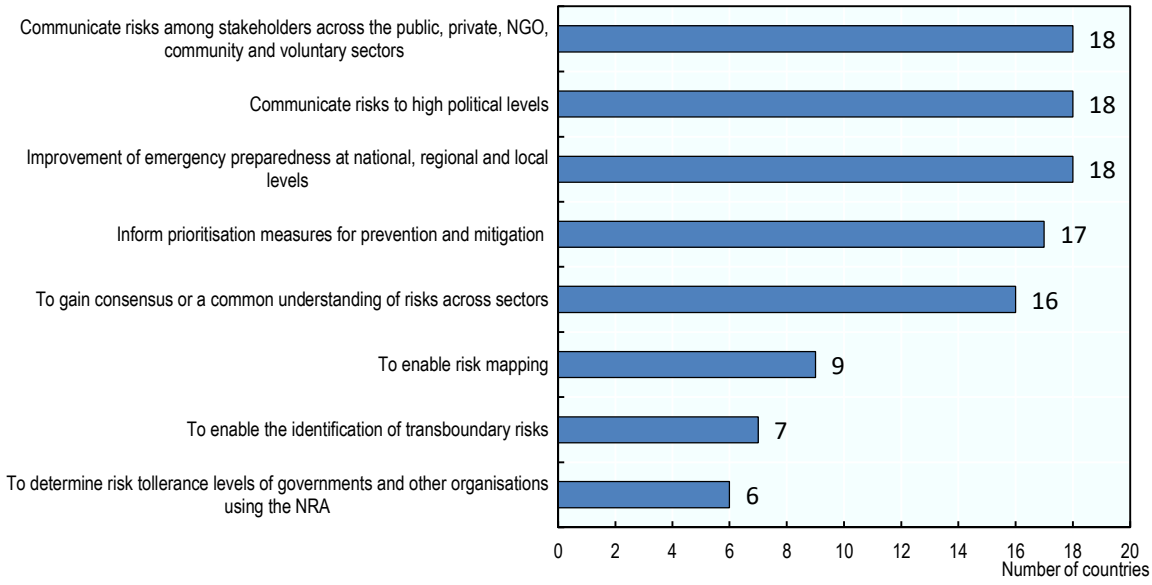
Recent shocks from natural and man-made disasters continue to cause significant social and economic disruption in OECD Member countries. A key objective of conducting a National Risk Assessments is to develop a comprehensive overview of the most serious risks facing a country as a starting point in civil contingencies planning. By identifying the full range of major risks, planners begin a process of reflection on the potential consequences if such events were to occur, the relevant skills and equipment required to manage those consequences, and whether it currently has the capacity to deploy those skills and equipment to the level of quality required and in the time needed. These fundamental steps of civil contingency planning may be inaccurate or biased if the underlying risk assessment process does not cover all risks or is rooted in defective methodology.

Across the surveyed countries, a wide range of aims and objectives are found for producing the current and future iterations of NRA (see Figure 1.1.) One of the most common purposes is communication about risks to the highest political level. Providing an easy to understand portfolio of all major risks sets the context for policy decisions at a strategic level. An equally popular purpose for conducting NRA is to improve emergency preparedness. OECD governments have many years of experience and in-depth working knowledge of risk analysis for specific types of risks, and most frequently for floods, earthquakes and forest fires. The technical expertise for specific hazards and threat analyses often reside in different government departments or agencies. National risk assessments provides a process to develop from this technical expertise a unified portfolio of natural hazards, infectious disease, terrorism and cyber risks, amongst others, and use this all-hazards portfolio to inform the design of emergency preparedness and / or crisis management planning.

Another purpose for NRA is to clarify responsibilities for emergency and crisis management when there is no designated risk owner for an event whose consequences have not been experienced in the past or might trigger knock-on effects. Likewise, some countries leverage the NRA process to develop consensus or a common understanding of risks across ministries. Countries often state that a purpose for conducting NRA is to establish priorities for treating different types of risks, although the OECD found relatively few examples to illustrate the results are actually used for this purpose. Overall, only about half the countries surveyed use national risk assessments as an input for risk mapping or to enable the identification of transboundary risks. The least common purpose found across countries for conducting a NRA is to determine risk tolerance levels.

A main difference in the purpose of conducting a national risk assessment relates to who its results are meant to inform. Some governments use the results to inform government actors on strategic investment decisions, e.g. concerning the development of preparedness capabilities to response to disasters. Other countries focus the design of NRA to educate a much broader group of stakeholders in the public, private, voluntary and community sectors. Further, one can distinguish those NRA used for near-term crisis management and those whose purpose is long-term capability building. In most countries surveyed, the objective of the assessment determines the methodology used, e.g. a deterministic approach to assessing likelihood or a probabilistic approach.

Figure 1.1. Objectives of National Risk Assessment



Note: Number of countries surveyed 20.
Source: Responses to OECD questionnaire on National Risk Assessments.

A high number of countries stated that the purpose of NRA is to inform and educate relevant stakeholders outside central government about the most important threats society faces. In this way, risk assessment can be leveraged to contribute not only to government plans, policies and actions, but also to its overarching objectives of reducing the vulnerability of all sections of society and building resilience from the bottom up.

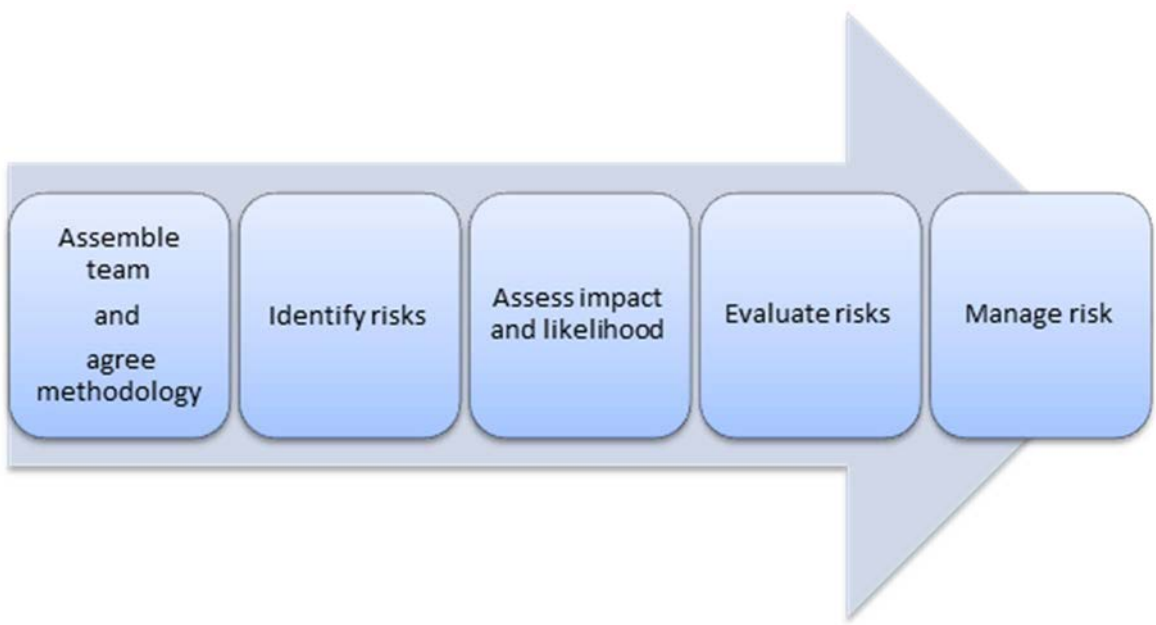
Relevant audiences may include lower tiers of government, at sub-national or regional level down to local levels where a NRA can provide guidance on the national risk picture and, in some instances, on how this may be reflected in regional or local risk assessments. The aim is to assist local authorities to reflect on a broader range of potential risks, and stimulate reflection on the need to define responsibilities, establish priorities, and build capability and capacity in much the same way as at the national level. Stakeholders in the private and voluntary sectors may also be consumers of NRA, including business communities, owners and operators of key infrastructure sectors that provide essential services, where an understanding of national risks can contribute to an understanding of interdependencies and stimulate investment in business resilience measures and self-help emergency preparedness.

National Risk Assessments can inform near-term crisis management and/ or medium term capability building. For many countries the process is part of a broader framework culminating in some risk management decision (Fig.1.2). The starting point is to convene a team of experts with specific knowledge of different types of risks and training them to apply a common methodology. This is followed by the identification of risks, often as deterministic scenarios, the assessment of impact and likelihood according to agreed qualitative and quantitative criteria, and the evaluation/scoring of the risk scenarios to make the results comparable. Discussions and decisions on managing risks tend to take place separately from the NRA process, but may be influenced or informed by the outcome.

The first step for governments is to catalogue the known range of civil contingency risks, and the existing range of capabilities, in order to anticipate the next potential crisis and marshal existing resources for response and recovery. For this kind of risk assessment (which we have termed a horizon-scanning risk assessment) the assessment timeframe is likely to be measured in months and, because there may be a limited time for detailed analysis, the screening of risks leans more to the qualitative than the quantitative. The next step is to build on knowledge of the existing stock of emergency response capabilities, so as to increase confidence that there are resources available for risk management measures and to fill gaps in capability, to meet the most serious, and most probable, contingencies over the lifetime of a government. Risk, vulnerability and capability analysis contribute to this. The most common timeframe for national risk assessments across countries is to scan for risks five years out; and the assessment will combine qualitative and quantitative methods.

Some countries extend the timeline for risk identification and analyses beyond five years. The aim in these cases is usually to conduct trend analysis of risk drivers with a view to better understand what risks might look like in the longer term future and, in some cases, to conduct initial analysis of the likelihood of a risk occurring and the impacts if it does occur. The aim of such foresight analysis is to provide strategic early warning of the ways in which the risk landscape may change in the future, enabling policy-makers to hedge their bets in designing disaster risk management policies and, potentially, providing an evidence base for investment in the resilience of infrastructure for the longer-term (twenty years or more). It is inherently difficult to quantify the future effects that risk drivers are likely to have, and the analysis is likely to take the form of comparative trend analysis.

Figure 1.2. Typical National Risk Assessment Process



Source: Authors

Methodologies used in national risk assessment

The study gathered information about the range of methodologies used in national risk assessments, and to discern the reasons behind why they were chosen. This report does not endeavour to critique the strengths and weaknesses of different methodologies, but to document what worked well in the experience of countries, or on the contrary proved cumbersome, so that different countries may take these lessons into account when considering a change in how they go about their own national risk assessment process. The study found that methodologies used to assess different types of risk scenarios ranged from relatively simple vignette descriptions of risk scenarios based on expert estimates of qualitative criteria, to more complex stochastic models or a mix of both qualitative and quantitative approaches.

Countries generally prefer to use qualitative approaches in national risk assessments when the range of risks to be identified is very wide and the officials charged with analysing them have neither the time nor expertise to carry out a detailed quantitative assessment of all risks. A lack of resources and expertise is often cited as a reason not to conduct more complex assessments that entail intricate analysis of probabilities and impacts. Nonetheless, the results of pre-existing quantitative analyses can be used to inform expert opinion and thereby complement the results of qualitative approaches. Indeed, the good practice is to require experts who provide opinions to provide references to such studies as a basis for their opinions. For example, a reasonable worst case scenario of a coastal flood may include descriptions of the consequences in terms of people killed, injured and displaced, and make an estimate of monetary damages. These estimates can be drawn from previous studies of similar past events that used quantitative models to arrive at their conclusions. The challenge is to achieve agreement between experts charged with making a qualitative assessment about the likelihood and impact of a specific risk scenario, e.g. as very low, low, high, very high. Often the expert teams involve working groups of officials drawn from across government departments or agencies with policy responsibilities relating to the range of risks within scope. This team generally includes experts with different subject matter expertise who refer to different sources of information and models in making the case for whether a specific risk scenario is more or less likely and severe.

The main aim of risk assessment may be simply to screen the risks, i.e., to categorise them in a way that aids decisions on whether they are of sufficient concern that risk management actions are needed or not. Screening assessments have value as a mechanism for briefing ministers and senior officials, describing in ‘broad brush strokes the relative likelihood and impacts of a range of disruptive events (OECD, 2012) that might affect the nation and engage responsibilities to provide protection, rescue or relief. Risk assessments that emphasise the qualitative over the quantitative approach have been able to achieve many risk governance purposes, such as:

- Securing consensus across Government on the most important risks for government to prepare for.
- Prioritising risks, so that risk management efforts are focused on reducing the gap between preparedness levels and the level.
- Clarifying strategic objectives for the most significant threats and hazards to guide the elaboration of prevention and mitigation measures.

- Anticipating near term risks and setting in motion adaptive crisis management measures.
- Promoting a risk management culture by educating policy-makers at the political and official level in the basics of risk assessment and management.

The qualitative approach to risk assessment has several limitations. First, they are generally rooted in the experts' knowledge of historical events, which reinforces the tendency to design risk management strategies based on past events rather than to anticipate future risks and understand the associated uncertainties. Second, they tend to lead to capability planning that looks backward at what was needed to manage the consequences of past events rather than forward looking anticipation of what consequences could occur in the future. Finally, in the absence of quantitative data it is more difficult to gauge with accuracy how much of a specific capability is needed to manage the consequences of a particular risk scenario.

Several countries argued that a deterministic approach is the only feasible methodology to compare different types of risks, because different assumptions and methods of calculations are used by the technical services in their line ministries to conduct quantitative risk assessments for specific types of risks. The results of these different models, therefore, have not been useful for the purpose of comparing different risks. It is important to point out that this has not prevented countries from continuing to try to develop quantitative models that can produce valid comparisons.

Countries used quantitative approaches to national risk assessment in two circumstances. First, where a government was considering the need for potentially high-cost risk treatment measures, quantifiable measurements were developed to increase confidence in the risk assessment. Second, a quantitative reassessment of has been used to determine whether risk treatment measures had the intended impact of reducing a risk to meet a previously calculated level of risk tolerance.

Quantitative approaches can be resource-intensive, and many countries have found that the benefits they present in additional certainty do not outweigh the cost and time it takes to conduct them. A common view in the risk assessment community of practitioners is that increasing certainty is worth the cost only up to a point. In many cases the risks being analysed are events that have not occurred, or occurred infrequently in past, and the data available is far from robust. An example that several countries pointed to was space weather, which presents different forms of hazardous natural phenomenon which can be measured, but the risks they present to electrical grids, satellites and aviation are based on very few actual events. Cross-disciplinary expertise is needed to understand and assess the nature and frequency of the hazard, and the vulnerability of infrastructure assets to its effects.

Definitions of terminology

National risk assessments generally involve experts from many different disciplines. It is important to establishing at the outset a common understanding of core terminology to promote the development of a consistent risk assessment approach. The experts conducting a national risk assessment in most countries use a source, or sources, of definitions to ensure a common point of reference and meaning of key terms. These include the definitions found in the European Commission guidelines (which are based on ISO 31000, ISO 31010, and ISO Guide 73, in combination with UNISDR terminology on disaster risk reduction), or a lexicon specifically developed by national experts (e.g.

the DHS Lexicon). These definitions have provided a useful starting point for national risk assessment work, although some countries prefer simpler, everyday language in order to make the process more readily understandable to non-expert participants in the process, and to external stakeholders. Among the numerous definitions provided as part of NRA, a large number of countries found it useful to provide explicit definitions to the terms in Box 1.1.

The collection of key terms used in national risk assessments provided some additional insight into the overall strategy and governance of major risks in several countries. For example, in defining the scope of risks that the NRA is meant to cover, many countries refer to "events of such magnitude that they overcome the capacities of regional or local communities to manage the consequences", whereas some refer to risks, the consequences of which, are of "national significance". The distinction is not necessarily apparent on its surface, however through panel interviews with country experts the distinction became clearer. The former meaning is focused on situations that overcome material capacity to cope with the adverse consequences of the event. This implies a policy that it is the proper role of sub-national levels of government to take responsibility for a certain level of emergency management. The latter meaning includes this first meaning, but also situations in which local communities are in principle not equipped to cope with the situation, for example a national labour strike or a political assassination. This distinction clarified that some countries are focused purely on civil contingencies and emergency management in the sense of rescue services, whereas other countries use a national risk assessment to identify and assess events that could destabilize a society not only due to a large number of injuries and damage to property, but also due to economic, political or reputational damage.

Box 1.1. Definitions of key terms

Among the key terms that the countries surveyed found useful to define are:

- **"Risk"** is defined in ISO 3010 as a combination of the consequences of an event (hazard) and the associated likelihood/probability of its occurrence; but in an everyday political sense as the uncertain consequence of an event that impact on things that are of value in society.
- "**All-hazard risk assessments**" are, accordingly, assessments of extraordinary events that encompass threats (of malicious damage) and hazards (whether man-made or natural) whose initial impacts engage the emergency services.
- **"Risk ownership"** is an arrangement whereby responsibility for risk management is assigned to a particular organisation, department or agency; the degree and type of responsibility that this entails can be subject to negotiation since some risks may have more than one owner depending on where the impacts may fall ("impact ownership").
- **"Impacts"** are defined differently by different nations according to a political judgement of the assets that are most highly valued; but, typically, these objects of value will include human, economic, environmental, political/social assets including public confidence, integrity of the democratic system and community cohesion.
- **"Risk evaluation"** is the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude are/is acceptable or tolerable. It is a "political or policy-making process in which social values and risk tolerance levels are factored in by ministers

Box 1.1 Definitions of key terms *(continued)*

and officials in order to decide about the objectives of policy, what measures can or must be taken to achieve those objectives, and whether the residual hazard is tolerable (BBK, 2011)."

- **"Risk management"**, in the context or the risks of emergency, is an umbrella term covering the various ways of reducing risk to a tolerable level, whether by preventing or reducing the likelihood of the hazard or threat materialising, by protecting objects of value, or by reducing the impacts. It encompasses therefore **"risk treatment"** (which itself encompasses protection, detection, response and recovery) and **"prevention"** (which can apply to the hazard or threat itself or its impacts).
- **"Resilience"** is defined as "the ability of a system, community or society to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions", which reflects UNISDR definitions in use in 2009. Most definitions make clear that national resilience is not an absolute but a characteristic of countries which determines how well they can resist, absorb, respond to and recover from shocks, but also entails an ability to adapt to adversity or a change in conditions whether in the short or the long term.
- **"Resilience capabilities"** is widely understood to be an umbrella term for human and technical means to accomplish a mission, function or objective necessary to achieve national preparedness and resilience goals; and encompassing both **"structural measures"** (for example civil engineering works) and **"non-structural measures"** (measures focused on the reduction of exposure and vulnerability). One country (the Netherlands) includes in its guidance for risk assessment practitioners a detailed five page list of capabilities in nine different areas (general capabilities; protection and prevention; protection of vital systems; population care, fire services; medical care; police assistance; recovery and aftercare) to aid systematic analysis of current capability and capability gaps. Another (the United Kingdom) encourages resilience risk analysts and programme managers to analyse capability in the areas of planning, legislation, alerting mechanisms, information, manpower, training, exercises, as well as equipment, logistics, and supplies.

Transparency and Accountability

National risk assessment requires, and provides an opportunity for, collaboration across government to assess different kinds of risks of national significance, and to reach a common position on the relative priority of these risks. The process of identifying and analysing risks can help also to clarify responsibilities for risk ownership within government.

In some countries it is the emergency planning legislation that set forth the degree of authority and accountability of government bodies in the risk assessment process. In more countries still legislation has been discussed and may be expected to be adopted in future that mandates the conduct of national risk assessment as a tool to support resilience planning. Still, many countries prefer a more informal arrangement in which responsibility for conducting a national risk assessment is determined as a matter of government policy rather than law. A common pattern is to assign accountability for emergency planning for each risk (and, in some cases, for each kind of impact) to a lead department or agency and to make the allocation public. But, because the impacts of national emergencies usually go much wider than can be managed by a single department, an overall co-ordination (rather than a directing) role is given to a lead department.

The role of the overall lead department varies between countries. Some lead departments are limited to a role in brokering agreement on risk assessment methodology, or collating contributions from other departments or agencies to the national risk assessment. A different model is to take a more directive role in steering the process of identifying, analysing and evaluating risks and resolving disputes, co-authoring and submitting the resultant risk assessments for the collective approval or notation of government ministers. In practical terms, a common phenomenon, in the early stages of national risk assessment, is that buy-in to the process by contributing departments increases as the benefits become clearer and as responsibilities – which may initially be controversial – are clarified, so that the process becomes much more truly collaborative.

The core of the national risk assessment process in most countries is a working group or committee comprising policy advisers from responsible government departments. In some processes, especially where the analysis has yet to go beyond the screening stage the involvement of subject matter experts is limited. Where there is a significant quantitative element to the assessment, however, countries have opened up to experts from within and outside government circles. The most advanced example of this is found in the Netherlands, where a formal network of analysts includes experts from government research establishments, the academic sector, and the private sector.

Government always retains control of the methodology and the identification of risk scenarios, but the analysis of possible impacts of the scenarios, and the associated likelihood, is carried out by working groups drawn from the network of risk analysts. In two other cases (the United Kingdom and Switzerland] the process is more internalised within government while still drawing extensively from relevant expertise from within and outside government.

Arrangements for independent validation of methodologies and of national risk assessment themselves vary widely. In most cases, governments have contented themselves with explaining the basis on which the assessment is done and making the outcome available to the public and political oversight bodies. In a few, the process has been subject to scrutiny by an independent reviewer who may be within or outside government. Briefing of Parliamentary Committees is an increasing feature.

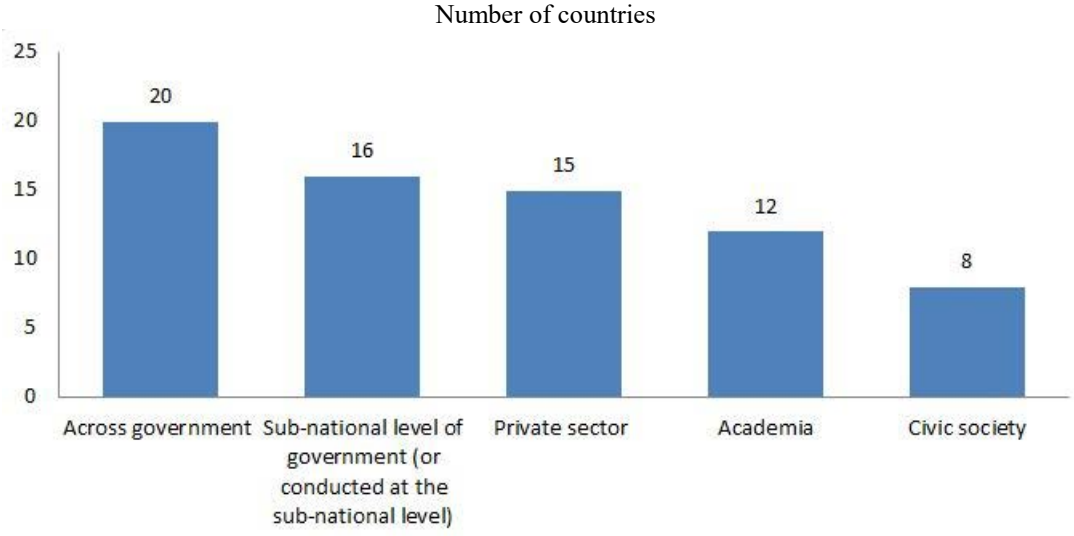
Multi-level governance and multi-stakeholder participation

For most countries, an important function of a national risk assessment is to encourage and assist sub-national lower levels of government to carry out assessments of the risks of emergency in their areas of responsibility (Figure 1.3). In the United Kingdom for example, guidance on methodology consistent with that used at the national level is issued to local levels together with information on the risks in a form that facilitates their interpretation of the significance of risks in the national risk assessment. In some cases there is direct participation by officials from regional or local government and, in still fewer cases, the national risk assessment is itself fed by regional or local analysis of risks

A particular focus of most national risk assessments is the risk of disruption of essential services resulting from damage to infrastructure assets or networks. The practice of involving infrastructure owners or operators in risk analysis varies widely. Estonia has passed legislation requiring risk assessment for 46 different kinds of essential service to be carried out by (currently) some 125 different service providers under the supervision of the government departments responsible for overseeing the sectors. A

more common approach is to rely on sponsoring government departments to carry out the risk assessment, or a government-industry forum with involvement of service providers, regulators and government officials to review the assessment and the interpretation of it in infrastructure sector resilience plans. Most countries find that commercial and security sensitivities inhibit publication of risk assessments and plans, but have opted for limited, sanitised publication to promote public confidence in the robustness of the analysis and planning.

Figure 1.3. Inclusiveness in the National Risk Assessment process



Note: Number of countries surveyed 20.
Source: Responses to OECD questionnaire on National Risk Assessments.

Notes

1. OECD(2009), Innovation in Country Risk Management ; Available at : https://www.mmc.com/content/dam/mmc-web/Files/Innovation-in-Country-Risk-Management-2009.pdf

2. Staff Working Paper on Risk Assessment and Mapping Guidelines for Disaster Management, http://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf

3. OECD Analytical Framework on Disaster Risk Assessment and Disaster Financing. https://www.oecd.org/gov/risk/G20disasterriskmanagement.pdf

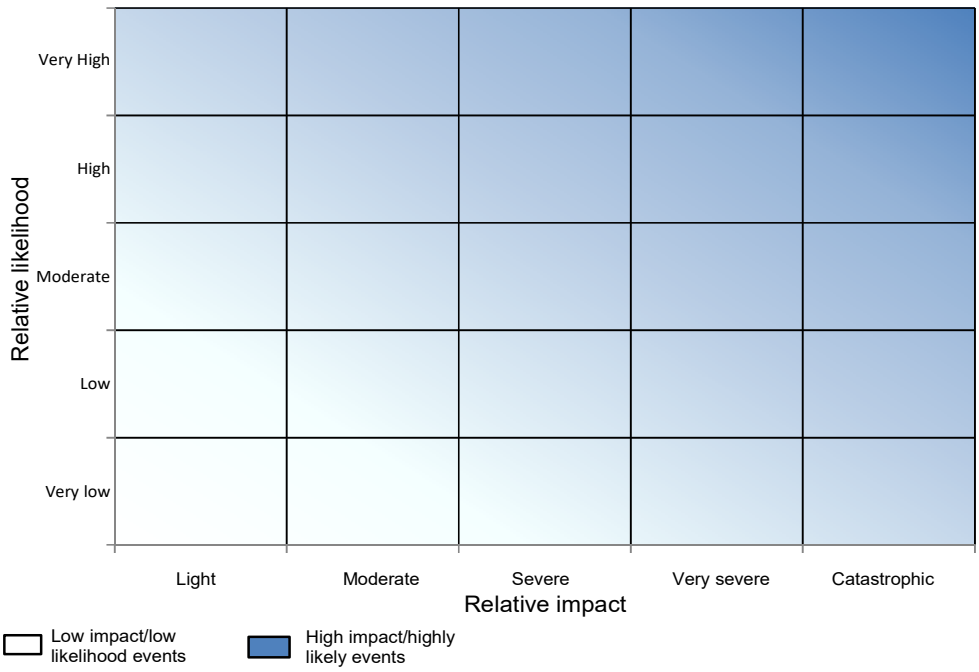
4. The OECD Recommendation of the Council on the Governance of Critical Risks, http://www.oecd.org/gov/risk/Critical-Risks-Recommendation.pdf

Chapter 2. Risk analysis in National Risk Assessment

This chapter presents the methods for risk analysis in National Risk Assessment, including its scope, threat and hazard identification, time horizon, impact analysis, likelihood and plausibility analysis, and risk monitoring and re-evaluation.

The pioneer countries in national risk assessment practiced a certain degree of collaboration, which can be seen in how they take a common approach to the overall process, even if the methodological details of risk analyses differ. The countries with the longest established NRA begin the process with a comprehensive overview of the various types of disaster, emergency or crisis that might significantly affect all or parts of their country. They select a sub-set of these events and develop risk scenarios, which illustrate the main features and origin of each event. They then analyse the risk scenarios in terms of two components, severity of consequence and its likelihood, with each component determined by a group of experts who apply agreed upon sub-criteria to attribute a qualitative ranking, e.g. from very low to very high. Each qualitative ranking can be attributed a quantitative score, e.g. 1-5, with 5 being the highest score for both severity and likelihood. Once risks are scored they can be plotted on a matrix. Figure 2.1 provides an example of a two dimensional matrix on which the scored risk scenarios can be plotted as a fixed point representing the relative likelihood and relative severity of consequence. Such risk matrixes provide an easy to understand picture for policy makers to contextualize the overall risk portfolio of a country.

Figure 2.1. A Matrix for National Risk Assessment



Source: Authors

National risk assessments are a relatively recent policy tool. Identifying good practice proceeds from observing where different countries are following similar approaches and agree that it produces tangible benefits. While it is important for each country to create a methodology that reflects its own unique conditions, it is as useful for practitioners to understand the reasons for variations in practice in the following areas.

Scope of National Risk Assessment

Accepted best practice is to adopt an 'all-hazards' approach to risk assessment which includes all the risks of emergencies that countries might reasonably expect to face within the time horizon agreed to in the methodology. This is important for crisis management and capability planning, whether the purpose is primarily to identify the top risks for which contingency planning and capabilities are needed at a national level, or the emphasis is on consequence management and on the level of capability required to reduce the impacts that are common to a number of risks. In either case, a broad-brush approach provides a better assurance that there are no significant contingencies whose omission might skew the assessment.

Box 2.1. All-hazards approach to National Risk Assessment

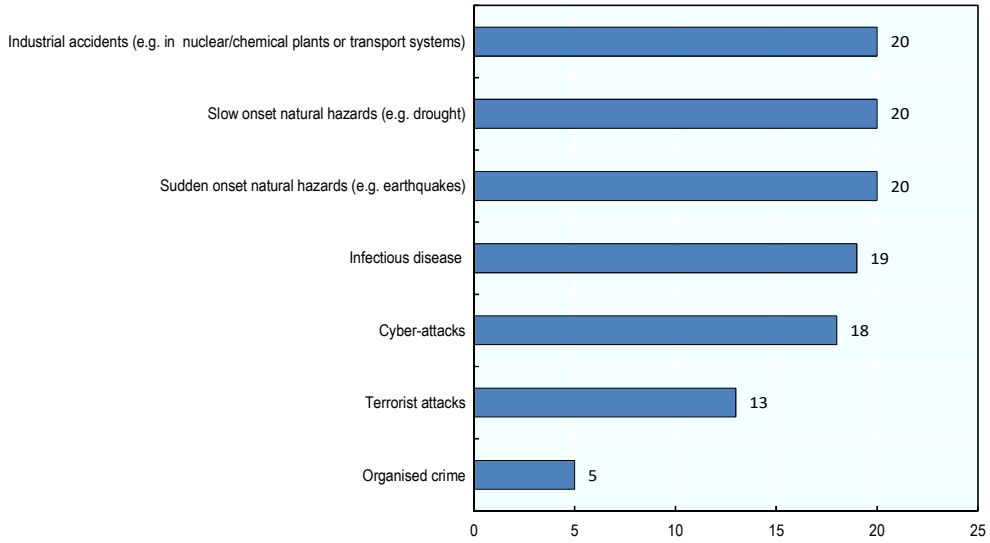
The OECD/G20 framework on disaster risk assessment and risk finance suggests that countries should identify a broad range of natural and man-made hazardous events and assess those that could cause significant damage and disruption to their vital interests. A holistic approach is important to uncover complex risks arising from vulnerabilities and interdependencies across sectors. To capture all hazards in a NRA process, a whole-of-government approach, involving all relevant government agencies and ministries, helps to assess the full spectrum of risks, and identify gaps in risk ownership and preparedness. This continual process benefits from being documented, monitored and regularly re-evaluated over time.

Source: Disaster Risk Assessment and Risk Financing (G20/OECD Methodological Framework 2012 http://www.oecd.org/gov/risk/g20oecdframeworkfordisasterriskmanagement.htm

All countries assess multiple risks; however, as can be seen from Figure 2.2, not all countries adopt an all-hazards approach. An all-hazards approach is perhaps the "Gold Standard" of risk management in which a very advanced form of crisis management is deployed using the full spectrum risk management paradigm. An all hazards approach covers all types of major hazards or threats, whether natural or man-made, and fosters an integrated assessment of a country's portfolio of risks, be they sudden or gradual in onset. It facilitates the identification of commonalities and interlinkages between natural phenomena and man-made events, the possible sequencing of hazardous events and follow-on impacts across borders. Events such as disruptions to trans-boundary infrastructures and suppliers of critical goods and services, or failing institutions, may themselves trigger new hazards and multiply exposures. An all-hazards approach should also facilitate the development of a comprehensive financial strategy for disasters, but not one country interviewed suggested that their risk analysis is leveraged for this purpose.

A high number of countries surveyed in this study adopt a form of the all-hazards approach, but more than half the countries have placed restrictions or caveats on the inclusion of more sensitive information in their risk assessment process. In particular threats to security (e.g. terrorism and cyber-attacks) pose difficulties for an open and inclusive risk assessment process. Some governments withhold information on terrorist capabilities and intentions from the NRA process, and on the vulnerability of their intended targets – which together are the main components of calculations of the likelihood or plausibility of such threats. Most governments also omit such information from their public facing risk registers. Although governments find the consequences of terrorist acts to be less sensitive information and fairly well understood in any case, information behind assessment of the current level of terrorist threat is closely guarded.

Figure 2.2. Types of National Risks



Note: Number of countries surveyed 20.
Source: Responses to OECD questionnaire on National Risk Assessments.

The majority of countries surveyed in this study adopt a form of all hazards approach. There are exceptions where more than half the countries surveyed have placed restrictions or caveats on the inclusion of more sensitive information in their risk assessment process. The inclusion of threats to security (terrorism; cyber-attacks) can pose challenges for an open and inclusive risk assessment process. Some nations may withhold from the process detailed information on terrorist capabilities and intentions, and on the vulnerability of their intended targets – which together are the main components of calculations of the likelihood or plausibility of such threats. Most will in any case omit such information from their public facing risk registers. But information on the likely effects of terrorist acts is in general much more widely known and less sensitive, so most nations have found an accommodation in which the impacts of security threats are included in the analysis even in those cases where the current level of the threat is not.

An area of controversy is the extent to which risk assessments can or should address 'steady-state' risks, which are risks of everyday phenomena (for example crime, air pollution, uncontrolled migration) that do not satisfy therefore a definition of emergency that includes only exceptional events. Most do not: on the grounds that NRA are complicated enough without such a very significant expansion in their scope. But longer-term assessments of risk (for example by the US SNRA, UNITED KINGDOM NSRA, prospective Dutch National Risk Profile) may include both events and developments that include the risk of perpetuation of intolerable levels of harm from these phenomena, or a notable increase in those levels, in order to inform calculations of the right balance of investment in risk management.

Threat and hazard identification

Risk identification should ideally consider all possible hazards in a probabilistic assessment. But national risk assessment on a probabilistic basis is not practical, so all nations surveyed use scenarios selectively to illustrate the different types of risk. Some

adopt a staged process where risks are first identified and placed on a 'long list'; this then undergoes an initial screening process designed to produce a shorter list of threats and hazards for which scenarios are developed; and these scenarios are then subject to comparative analysis designed, in different degrees, to quantify and to rank them. The numbers of risks identified, developed through the use of scenarios, and then analysed, can vary significantly. In two cases, hazard 'catalogues' were developed in the first instance itemising over 100 risks, from which a short-list was developed numbering, in one case, some 80 risks which were developed into vignettes (relatively simple illustrative scenarios) which were used for the assessment. In the other case, fewer (between 30 and 40) but more detailed scenarios were developed. For most countries, much smaller numbers of risk were identified in the first stage, with between 15 and 35 being developed into scenarios. All countries include scenarios illustrating both harm from common agents (such as storms, floods, terrorists) but also harm to critical assets (such as power distribution nodes); this in part satisfies the need for NRA to encompass multi-risk assessments – assessments of the cascading effects for example of a flooding disaster on power distribution and so onto other essential services – as well as the effects of single risks.

In addition, this holistic approach assisted these countries to identify more complex risks arising from vulnerabilities and interdependencies across all sectors, both public and private.

Risk events may have a range of possible outcomes, and some scenarios attempt to describe the range by illustrating a number of different possible outcomes of the event described, typically: the worst or best case outcomes, and an outcome somewhere in-between (often described as the 'expected outcome', or the 'reasonable worst case' scenario or outcome, representing the worst that could reasonably happen discounting extreme manifestations of the risk). Other countries develop separate scenarios for similar risks with different levels of severity – this is the United Kingdom approach to terrorist threats – but all need to ensure that the ranking of risks is done using a comparable level of severity to avoid a distortion of the comparison; and cross-country comparisons need to take into account different practices in use by different nations (for example the United Kingdom uses Reasonable Worst Case Scenarios; Poland best-case; the Netherlands use 'lower limit', 'upper limit', and expected or 'forecast value' which is the basis on which comparisons are made within the Dutch NRA). These levels of severity can become standards, or reference points for decisions on the level of investment in risk management. Clarity on the method used is important even though, for most nations, the decision to mitigate risk implied by the assessment of these scenarios is a matter of policy reflecting a government's risk tolerance and usually not reached before the risk evaluation stage.

Time Horizon

The 2012 report noted that the five nations initially surveyed had all defined a timescale for the risk assessment, and that most were interested in a five year period reflecting a wish to encompass all kinds of events that were likely to occur within the foreseeable future, with reasonable confidence that the resources allocated and capabilities developed to manage risks would be unlikely to be wasted. A secondary purpose of choosing a 5-year timescale was to enable risk managers scope to timetable capability improvements, and encourage a forward-looking approach, going beyond the purely historical analysis of risks arising in the recent past, and reflecting near term risk

drivers. Countries that have undertaken national risk assessment since then have tended to follow the same approach although some (e.g., Germany) do not see the point of estimating probabilities over a five year period, preferring a one-year timescale.

A key consideration is whether risks are assessed in their mitigated or unmitigated state. Most countries take into account at least some of the controls that they currently have over the risks or their impact: for example, flood risk assessment will take into account the existence of permanent flood defences and will therefore, in effect, be an assessment of the risk of flood barriers being overwhelmed or by-passed. But the analysis is often implicit rather than explicit. An exception is the Australian system of risk assessment in which controls, over the hazard itself and over the impacts, are factored directly into the assessment at the impact assessment phase.

Impact Analysis

A common feature of all national risk assessment processes is that they consider not only multiple risks but also multiple impacts or consequences. Annex C shows the main criteria and sub-criteria in use among the countries surveyed most of which fall in the following five categories:

- Health and wellbeing of the population, with the consequences of an event being measured , for example, by the numbers of deaths that are likely to occur, cases of injury or illness and in some cases the requirement to evacuate populations caused by the hazard
- Economic consequences, as measured by the demand-side and/or supply-side effects of an emergency
- Disruptive effects to the supply of goods and services essential to the welfare of the population, measured by the extent/intensity/duration of disruption of a wide range of service (typically: energy, food, water, transport, communications, health, finance; and, less typically, education) and/or the destruction of infrastructure networks related to these
- Environmental damage, measured with varying degrees of precision but usually encompassing the geographical extent and persistence of the harm caused; and sometimes identifying separately damage to protected sites
- Political or social impacts, including effects on public order and safety, public psychological impacts such as outrage or anxiety, damage to cultural assets, infringement of territorial integrity, loss of reputation of the government (nationally or internationally).

Most countries have devised a scale, usually from 1 to 5, to distinguish a relatively mild impact from progressively more serious impacts up to a level which is regarded as disastrous or catastrophic; and agree (and often publish) the values for each kind of impact that correspond to each point of the scale. Recognising the degree of uncertainty in the assessment of impact, most countries attempt to identify 'order of magnitude' differences between one level of impact and another, by means of a logarithmic progression. Some have elaborated mechanisms whereby impact types that are regarded as more important than others within the same primary category are given special weight. As a consequence, the assessments of impact can be used in various ways:

At the level of the primary criteria, the impact scores are usually aggregated for the purposes of making an overall comparison of risks. No particular weighting is given to

the main categories of impact, although there may be a system of weighting at the subordinate level.

In the evaluation phase, a differential approach to particular types of impact can be adopted by changing the weighting given to the main categories, or by creating separate presentations of the risks showing the priority that each would have if only a limited set of impact criteria were taken into account.

An alternative approach is to carry out an impact analysis, taking the types of impact that are common to a number of risks and analysing them to establish a range of values (quantity, extent, duration, etc.) that can be used for generic impact planning purposes.

For example, one country [the United Kingdom] uses its national risk assessment to calculate the range of impacts that might be expected from the most common risks, in 20 areas[1]; (Box 2.2) and these are used to explore risk tolerances and, in capability analysis work, to determine the capacity required to be resilient to the standard the government wishes.

Box 2.2. National Resilience Planning Assumptions (United Kingdom)

The United Kingdom uses its national risk assessment the range of impacts that might be expected from its most common risks:

- Functional planning assumptions: Human Fatalities with Infectious Disease; People with Illness; Human Fatalities caused by Conventional Incidents; Human Casualties caused by Conventional Incidents; Biological Release; Radiological Release; Chemical Releases; Debris/Rubble; Major Flooding; Displaced Persons; Influx of British Nationals; Animal Diseases;
- Essential services planning assumptions: disruption of: Water Supply; Transport; Oil and Fuel; Gas; Electricity; Telecommunications; Health; Financial Services

These are used to explore risk tolerances and, in capability analysis work, to determine the capacity required to be resilient to the standard the government wishes.

Source: National Risk Register of Civil Emergencies 2015 edition. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419549/20150331_2015-NRR-WA_Final.pdf

Likelihood and plausibility analysis

An additional common feature of national risk assessment processes is that they consider the likelihood and/ or probability of events, with most using a five point scale ranging from those events that are as likely as not to happen in the next five years (or equivalent). The category for least likely events is seen to be reserved for those events that have as little as 1 in 2,000 to 1 in10,000 chance of happening in any given year. The intervening points on the scale increase logarithmically by a factor of ten. Calculations of probability are worth making for two main reasons:

- to enable governments to devise risk management strategies that take account both of the impact of disasters and their likelihood; and to decide on the most effective allocation of resources as between reducing the factors contributing to the likelihood of an event occurring and reducing the likely impacts (in whichever of the categories of impact is most affected by the risk)

- to enable governments to take an informed view of risk tolerance, and to apply (for example) a discounting factor to risks of emergency that may be very serious in their impacts but are relatively unlikely to occur.

Earlier surveys have drawn attention to the need for a different approach to calculating the risk arising from natural hazards or man-made accidents (which are largely a function of the hazard potential; the exposure of populations and assets to the hazard; and the vulnerability of the same) than to estimating the 'plausibility' of the risk of a successful terrorist attack for example. The latter is commonly agreed to be a function of the capabilities of terrorists and their intent or motivation, combined with a factor representing the vulnerability of their intended targets. The difficulty of assigning a common scale to these different approaches has been overcome in some cases by presenting threats and hazards on a separate risk matrix using qualitative scales in one case and quantitative scales in the other. Others consider that the method of calculating probability in either case is sufficiently similar, and subject to a similar degree of uncertainty, and that the benefits of weighing all the risks on a broadly comparative basis outweighs the possibility of error.

Measuring confidence or uncertainty: with any qualitative or quantitative analysis there is often a degree of confidence that is lacking in the results of a NRA. Norway, Canada and Sweden make a point of highlighting and characterising uncertainty in the analysis of risk scenarios. An assessment of the degree of confidence in the assessment can inform decisions as to whether to conduct further analysis or research, to reduce the uncertainty, or to continue with risk treatment but include sensitivity analysis to reduce the chance of over- or under-estimating the investment in capacity required to reduce the risk to a tolerable level.

Risk monitoring and re-evaluation

The 2012 report noted that 'a cyclical process will help to support regular review and re-assessment of hazards, exposures and vulnerabilities, including periodic re-evaluation of the risk assessment process, its governance, methods and practices'. Most countries have adopted iterative or cyclical review covering all elements of the risk assessment process. Some now review risk assessments at longer intervals, in order to increase the time available for analysis of key risks while admitting new risks and risk scenarios into the assessment, and to allow for a routine re-appraisal of the existing stock.

Notes

1. The 20 areas covered by the United Kingdom national resilience planning assumptions are:

Functional planning assumptions: Human Fatalities with Infectious Disease; People with Illness; Human Fatalities caused by Conventional Incidents; Human Casualties caused by Conventional Incidents; Biological Release; Radiological Release; Chemical Releases; Debris / Rubble; Major Flooding; Displaced Persons; Influx of British Nationals; Animal Diseases; Essential services planning assumptions: disruption of : Water Supply; Transport; Oil and Fuel; Gas; Electricity; Telecommunications; Health; Financial Services.

Chapter 3. Communicating the results of National Risk Assessments

This chapter presents the various options that exist for communicating the results of National Risk Assessment, to raise public awareness, as well as the tools for interpreting risk analysis.

Raising public awareness about risks

Wide communication of risk assessment to the public delivers significant benefits to policymakers and emergency planners at the national and sub-national levels of government. Risk assessment that are perceived to be objective and impartial helps to build and sustain public trust, which is crucial to acceptance of extraordinary measures during times of crisis. Transparency in the risk assessment process can also contribute to its wider public credibility. Wide communication of risk assessment can also help in embedding risk reduction knowledge into governmental policies, spatial planning strategies, regulations and standards, such as regional and local planning, zoning, and building codes, which can have significant impacts on disaster risk reduction.

Risk assessment outcomes need to be communicated to the highest levels of policy decision-makers and the public by using internal and external communications to effectively communicate the results of the risk assessment to those stakeholders in an easily readable format (Box 3.1) (OECD, 2012).

Box 3.1 Risk Communication and Public Awareness

Internal and external communication

Effectively communicate the results of risk assessment and use them to inform the highest levels of policy decision makers

Public awareness strategies

Implement communication strategies to educate citizens and businesses about the hazards and threats facing the country, promoting the development of a "risk culture "and provide guidance on what they can do to prepare for the major risks

Tools for interpreting risk analysis

Document and deliver hazard and risk information in an easily readable format, such as mapped hazard and risk information for a defined area, or as a risk matrix or risk curve showing possible events and their likelihood and expected impact.

Source: Disaster Risk Assessment and Risk Financing - G20 OECD Methodological Framework. http://www.oecd.org/gov/risk/g20oecdframeworkfordisasterriskmanagement.htm.

Of those countries covered for this study, most of them (Figure 3.1) present the outcome of national risk assessment in the form of a risk matrix which visually represents the relative likelihood and impact of risk scenarios, together with detailed analysis of the risks in which likelihood and impacts are scored according to criteria agreed at the outset. The presentation of the full range of risks provides a broad understanding of the major risks facing national Governments, and may help to calibrate perception of the risks.

It can also facilitate consensus on the country's overall risk profile and on the priorities for action at a country level. There is also an advantage where countries have a range of risk scenarios in the development of horizon-scanning risk assessments, such as the "United Kingdom's Forward Look" (Box 3.2) which are designed to cue short term adaptive contingency planning in anticipation of emergencies. The risk assessment can also provide a source of plausible scenarios to assist in national crisis management exercises on a single or multiple themes. In these cases, the matrix can provide the basis of a national exercise programmes in which management of and response to the most significant national risks is rehearsed over a period of years.

Box 3.2. United Kingdom: Cabinet Office Horizon Scanning

The UK's Forward Look Concept

In 2001 the UK introduced a horizon-scanning risk assessment or "Forward Look" to support the Government's central crisis management machinery (known as the Cabinet Office Briefing Rooms or COBR). The Forward Look is based generally on open-source information on the prospective risk of disruptive challenges within a 6-12 month period, designed to help to trigger 'adaptive' crisis management (adapting contingency planning and last minute adjustments of capability). It is part of a family of risk assessment tools to help emergency planning for the short, medium and long term within the UK. The Forward Look is a 6 month horizon-scanning risk assessment used to trigger crisis response planning and recommendations to government ministers on the prioritisation and handling of risks in the short term.

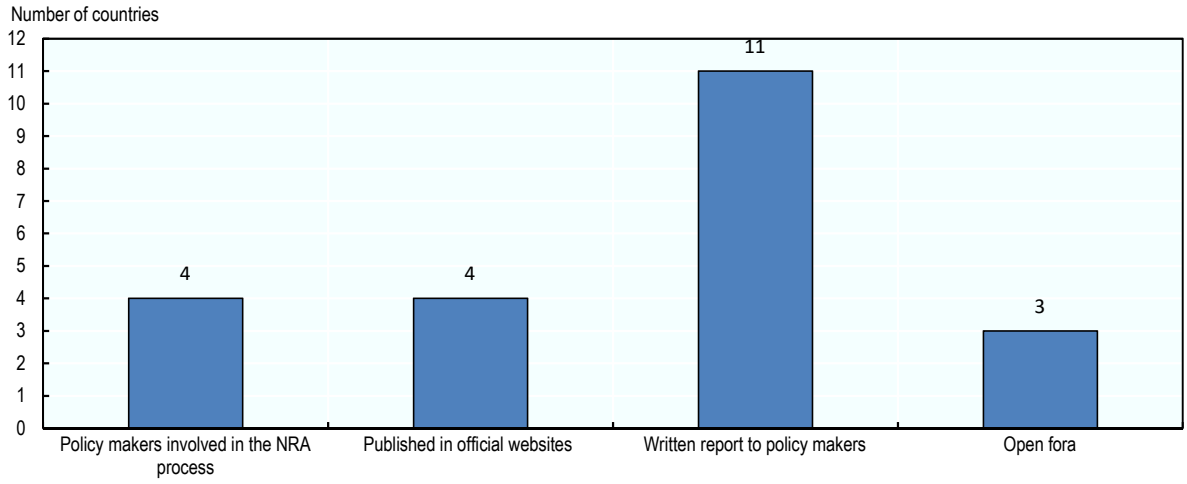
The Forward Look is done in 5 steps over a three-month cycle (some elements are updated more regularly):

- **Step 1** is the prior step to agree the make-up of a cross-government team, and the methodology to be used, to produce the Forward Look. The team consists of officials from all government departments and agencies having responsibilities either for the risks themselves or for impact mitigation, plus subject-matter experts as required from the science, industrial health and safety or other expert communities. Simplicity and speed of analysis are essential, so a 3-by-3 matrix is agreed as the framework for risk evaluation (rather than the more complex 5-by-5 matrix used for national risk assessment).
- **Step 2** is to identify risks of social/economic/political disruption, using scenarios which represent the realistic worst case and/or the realistic expected case. The expected outcome of this stage of the assessment is a manageable list of between 20 to 40 candidate risks.
- **Step 3**, once the scenarios are accepted, assesses the impact that the scenarios would be expected to have, according to the criteria agreed in step 1.
- **Step 4**, which can be carried out at the same time or follows immediately after step 3, assesses the likelihood of the event materialising and having the impact assessed in step 3. A rough (low/medium/high) estimation of likelihood is used.
- **Step 5** assembles the data in steps 3, 4 and 5 in one matrix for the purposes of comparing the different risks. The purpose of the matrix is to enable recommendations to be made to Ministers using a varied range of criteria. The final aspect is Ministerial consideration of this quarterly risk assessment, leading to action to anticipate and manage the risks in accordance with the decisions taken.

Source: United Kingdom National Risk Assessment.

In addition the matrix can also be used to support the formulation of risk management strategies, enabling ministers and senior policy makers to agree their approach to the management of: 1) risks that have high impacts and relatively high likelihood; 2) those with high impacts but occurring much more rarely; and 3) those more frequent events that have relatively moderate consequences. In most cases, the process of formulating risk management strategies depends, either explicitly or implicitly, on a process of risk evaluation, described by one nation [Germany] as "a political or policy-making process in which social values and risk tolerance levels are factored in by Ministers and officials, in order to decide upon the objectives of policy, what measures can or must be taken to achieve those objectives, and whether the residual hazard is tolerable". One nation [Finland] uses the risk matrix, in effect, to determine the threshold between risks that should be delegated to sub-national tiers of government, and those that must by default be managed by the national government.

Figure 3.1. Outcome of the NRA communicated to decision makers



Note: Number of countries surveyed 20.
Source: OECD survey mission reports, referred to in Annex B.

Risk communication is undertaken in varying degrees to stakeholders in the wider public/government sector, to national infrastructure providers, and to the broader business and social communities. Figure 3.1 shows that the majority of countries communicate the results of the national risk assessment to the highest political levels and decision makers. The widest communication of risk assessment can increase risk reduction knowledge within government, in developing policies, spatial planning strategies, regulations and standards. These include regional and local planning, zoning, and building codes, which can have significant impacts on disaster risk reduction. The clear understanding of the prevailing risks assist with understanding the potential legislative or regulation changes that may be required to mitigate for, deal with the results or fund the aftermath. The objective in all cases is to familiarise these stakeholders with the range of risks for which they may want or need to be prepared, and in some cases – particularly infrastructure owners/operators - to encourage enterprises to improve their own resilience characteristics, and to build resilience into new assets at the planning stage. Whilst the exposure varies considerably, depending on how advanced the risk assessment process is, risk communication to the following sectors has occurred:

- Wider public sector: a number of countries publish guidance to the wider public sector on how to carry out risk assessments in their own area of responsibility; this can be accompanied by information from the National Risk Assessment indicating the government's view of the kinds of risks that should be identified and analysed in local risk assessments, suggested criteria for the assessment.
- Infrastructure owners/operators: best practice is to involve the providers of essential services in the confidential risk assessment process, as subject matter experts and in order to obtain their buy-in to the need for resilience. This can be prohibitive because of the large - and growing – number of infrastructure-based services qualifying as essential to public welfare; and one country [Estonia] has passed legislation requiring essential service providers themselves to carry out risk assessment, under the supervision of their sponsoring government department, and using risk scenarios provided by the government. Another [the United Kingdom] has set up a government-industry forum to develop

infrastructure resilience plans for each of the main sectors, based on the National Risk Assessment and on the sectors' own understanding of their risk environment.

- Business/other communities: This report points to the different practices among countries as regards publication of risk assessment results: some [Netherlands, Norway, the United Kingdom, see section 3.2] actively work not only to make results widely available to decision-makers in the different sectors (government; infrastructure) but also to publish at least some aspects more widely including the Netherlands for example; others [US; Canada] have chosen to classify and only circulate internally the results of their risk assessments. Since then, most countries have found it possible to publish at least some useful material from their national risk assessment process, by redacting material that is sensitive from a security or a commercial standpoint (whose publication would therefore inhibit the full sharing of threat and vulnerability data in the assessment), and so help to inform business continuity planning in the economy as a whole, and wider community resilience schemes.

Tools for interpreting risk analysis

From this study we can see (Figure 3.2) that 78% of countries use a risk matrix to visually represent the likelihood and impact of the risk scenario with the remainder found not to have a matrix developed at this point or not seeing the necessity to use it as one of the tools for interpreting or communicating the risk analysis. On the other hand, we can see (Figure 3.3) that 72% of countries make the results of the process of the NRA publicly available.

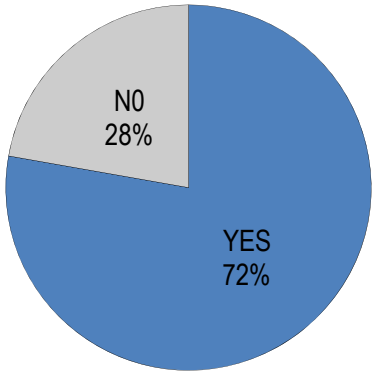
In the case of the United Kingdom matrix is one of the main communications products used to illustrate (in pictorial format) the range of risks which have been identified and is used as a tool to provide information in that format to a wide range of stakeholders. The government and policy makers have accepted the need to be transparent in order to raise awareness in all sectors of society. In the United Kingdom this is linked to the overall civil contingency strategy of protection in awareness and resilience. This strategy of openness has led to the NRA been circulated through the local resilience forums since 2011. These forums involve the local community in all its forms including the business community who need to be informed and to take action against the prevailing threats that exist now and may happen in the future.

This has the added value of an overall inclusive approach to the management of risk and protecting society generally. The published risk matrix takes the form of two distinct matrices which illustrate (1) the risk of terrorist or other malicious attack and (2) the risk of natural hazards and major accidents. The time period chosen for both matrices is determined over a 5 year period but differ in respect to "relative plausibility of occurrence" in the terrorism matrix and "relative likelihood of occurring" in the case of natural hazards and major accidents.

In common with the United Kingdom, Norway utilises a risk matrix and in contrast it does not contain a risk scenario for acts of terrorism. Norway produces a risk matrix that aggregates the results of 14/17 risk scenarios along axes for consequence and probability. For each scenario these two components are assigned a score from very low to very high, and these scores determine where a scenario is plotted on the matrix. Malicious risk scenarios are not represented. Behind this decision is the view that it could be misleading to attribute a probability score to malicious incidents in a way that implies comparability

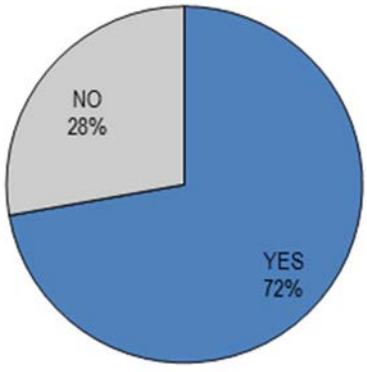
to natural and accidental incidents. By including malicious incidents in the previous edition, the results were misinterpreted by some to mean that an attack was totally unlikely within one year, whereas the intention was only to convey the relative likelihood of such an incident occurring within the next year.

Figure 3.2. Countries that use a risk matrix



Note: Number of countries surveyed 20.
Source: OECD survey mission reports, referred to in Annex B.

Figure 3.3. Results and processes of NRA are made publicly available



Note: Number of countries surveyed 20.
Source: OECD survey mission reports, referred to in Annex B.

The 2013 edition of the NRA is publicly available, providing broad information on 14 risk areas for which scenarios (two scenarios for three areas) were developed. The intention at the time of the review was to expand the risk assessment, to a maximum of 25 generic scenarios in the next few years, and to explore ways in which the Norwegian NRA can be exploited to improve national resilience.

Transparency in the case of Norway is ensured, both in development of the NRA methodology and its outcomes, by means of a public document distributed to Ministries, Agencies and local authorities to complement their own work on vulnerability and risk assessment. Information about the NRA process and its outcomes are open to the public – both on the Directorate for Civil Protection website and in print. Additionally, the results

are sent to all main stakeholders. Furthermore, DSB gives presentations on the NRA in different fora, mostly in ministries or authorities, including the regional and county government level that have special responsibility for safety and security. Presentations are rarely given to businesses, however, which generally conduct their own risk assessment and could be interested in the NRA as a backdrop to their own efforts. Feedback has been solicited from all major stakeholders with a view to improving the NRA methodology and presentation.

The next phase for Norway's NRA follows significant user feedback from various levels of society who found it useful as a starting point for work to bolster security and emergency planning. This open approach has led to engagement from all sectors at all administrative levels with at least a standardised approach. It has also led to an ongoing evaluation process which based on feedback received has led to explore ways in which the Norwegian NRA can be exploited to improve national resilience.

In the Netherlands the main tools for interpreting risk analysis are the risk matrix and chart in the published NRA. These are based on equal weighting being given to each of the ten impact indicators, but sensitivity analysis is also carried out, exploring the effects of using different weightings (for example, by applying the weighting to the 5 'vital interests'). Similarly, the effects of using the worst case or best case scenarios can be explored and the effects displayed on a diagram specifically designed to show the degree of uncertainty in the analysis of the risks. The Netherlands also carries out capability analysis in relation to the risks in the NRA, and systematically compares the capabilities required in order to make calculations of capacity (the amount of capability required) in each of the main capability areas.

Regional risk assessment is carried out according to similar methodology, although not for purely national risks (like space weather); and risk mapping (for fire hazards, floods and chemical/radiation hazards) is also carried out at regional level. Amongst the other tools available for risk management is an application for mobile phones ("crisis.nl") which provides information to citizens on common hazards, in particular flooding. The Netherlands are in the process of reviewing the next steps for the national risk assessment. A replacement is proposed to the current NRA with a National Security Profile developed on a four year cycle to replace the existing NRA done every year.

Conclusion

One of the main advantages of engaging all stakeholders, public, private, academic and wider community in the process of wide communication of the results of risk assessment has been improved stakeholder engagement in operationalising the risk analysis at local levels and the implementation of changes in their planning for risks. In addition, the overall transparency in the national risk assessment process helps to communicate basic messages about the most serious risk types and predicted changes to these risks in the future. The wide communication of risk assessment can increase risk reduction knowledge within government, in developing policies, spatial planning strategies, regulations and standards. These include regional and local planning, zoning, and building codes, which can have significant impacts on disaster risk reduction. The clear understanding of required legislative changes is a pre-requisite to the smooth passing of legislative change. The availability of this information on government websites outlined in a clear unambiguous way to all stakeholders goes a long way to ensure transparency and acceptance of the steps that have to be taken to mitigate these risks.

Chapter 4. Lessons learnt from development and use of NRA

This chapter presents the lessons learnt from development and use of National Risk Assessment, including its benefits for strengthening the implementation of risk management policies, for policy making, and for resilience programmes as well as the identified limitations.

Identified benefits from the use of National Risk Assessment

The merits of the national risk assessment process must be judged by their usefulness to countries wishing to improve national resilience. The capabilities and capacities required for this can take many forms, from an increased awareness of risk, through improved organisation for crisis management, to structural and non-structural measures. The benefits of NRA are correspondingly heterogeneous, but the results of the survey suggest that they fall into one of the following categories. Most countries, including some which have relatively recently started to do national risk assessment have identified benefits from the process itself even before they are able to proceed to the risk evaluation and risk management stages.

Benefits for strengthening the implementation of risk management policies

1. Promotion of risk awareness at all levels of government

It has been found in this study that the process of systematically assessing risks has helped to promote risk awareness at all levels of government in addition to a clearer understanding of what happens when disasters strike. This aspect helps to promote an understanding of the nature of disaster risk while avoiding the need to speculate on, or to try to predict, future shocks in an inherently unpredictable risk landscape. NRA can also help to achieve consensus on what the reasonable worst case risk scenarios facing a country are. The use of NRA to develop partnerships between different tiers of government is exemplified by the German approach to use risk assessment to inform responsibility-sharing between the federal government and the Lander.

2. Collaborating across Government sectors

The collaborative nature of the NRA process has helped to create a healthy culture of cooperation within government with less institutional 'stove-piping' or bi-lateral communications with more open and overarching discussion forums put in place. In addition where there are already strong patterns of collaboration between the main policy actors, this has been reinforced.

3. Promoting new forms of cooperation between policy-makers and subject-matter experts

The use of cross-disciplinary approaches in risk analysis has promoted new forms of cooperation between policy-makers and subject-matter experts. This has been beneficial to both and created new networks across boundaries. The adoption (and road-testing) of an agreed methodology for assessing likelihood, plausibility and impact have made dialogue on the risks between experts from the different sectors much easier. This process has also facilitated the formulation of consensus on the risks and the workshops to analyse scenarios were instructive to participants who gained insights into other stakeholder's perceptions and a deeper understanding of the nature and complexity of crises. The NRA process creates an important arena for discussion of serious national events, the creation of new networks, and creation of consensus across subject and sector boundaries.

4. Prioritising the national response to a major emergency

There were some reported 'early wins' from the risk assessment process: in one case, the process of sourcing and gathering data assisted in prioritising the national response to a major emergency even before the process of risk assessment had been completed; in

others, countries have been able to leverage the results of risk identification work in the design of scenarios for crisis simulations and exercises, and using the risk maps that informed part of the risk analysis process to prioritise areas for emergency protective measures during flooding events.

Benefits for policy-making

NRA provides the evidence base for high-level policy decisions on priorities and risk management strategies addressing the two main components of risk: the likelihood of emergencies and their potential impact. Benefits here in policy making are:

1. Facilitating engagement of, and providing a basis for consensus at the highest levels

The National Risk Assessment process facilitates engagement of, and providing a basis for consensus at, the highest levels of the government (ministers; senior officials) and in some cases Parliaments on the strategic aims and priorities of resilience policy.

2. Providing an objective basis for the risk evaluation

The process provides an objective basis for the risk evaluation phase in which broader political as well as strategic judgements can be brought to bear on the objectives of security and resilience policies, priorities for risk treatment and the tolerability of the residual hazard being examined. StaOne nation (Germany) found that the NRA can be useful in determining an effective balance between prevention and resilience in the national strategy.

For the top risks, enjoying a priority for risk treatment, NRA properly constructed can provide a consistent basis for understanding the risks in all their dimensions (the nature and potential of the hazard, the extent of the exposure of a nation's citizens and critical assets to it, their vulnerability, and the impacts) through the use of scenarios that illustrate the range of possible outcomes of emergencies, and may also be used to explore the pathways by which the hazards may come to harm or disrupt objects of value to the country. The Netherlands' practice of exploring the lower limit and upper limit for each risk, while basing the comparison with other risks on the expected value (or most likely score), represents best practice in exploring the range of possible outcomes.

In countries with a wide-ranging and diverse disaster risk portfolio, Governments may initially want to use risk assessment to distinguish those risks that should be the drivers for building capability at the national level, and what the priorities should be. The two countries adopting this approach initially started with a long-list numbering over 100 risk types. NRA here perform a 'screening' function with a qualitative or semi-quantitative approach providing an objective basis for ranking the risks and developing, in effect, a short list of events for priority treatment. Judgements about priorities tend to favour the assessed impacts of the events or developments assessed but may take into account their likelihood and the degree of uncertainty associated with the assessment. Good practices in this area can be found in the United Kingdom, the Netherlands; and best guidance is the Australian NERAG.

An approach that is common to all countries surveyed is to provide the basis for 'scoring' of risks, to determine their ranking and relative priorities and so to identify the most significant risks threatening national assets of value. Some carry out an extensive screening process to do this (as above); for others the screening process is less extensive and consists of using historical evidence or canvassing stakeholders, to develop a short-

list and work through the list as and when the analytical resources become available to do so. Some short lists are very short – a handful of the most obvious risks affecting the country as a whole. The most developed short-lists can in due course number up to 30-40 risks. Their significance may be that they are truly nationwide risks, or that they are potentially catastrophic (e.g., earthquakes; pandemics), or highly likely (severe weather; terrorist attacks), or both (severe flooding); or that there is too much uncertainty about either likelihood or impact for the risk to be tolerated without further analysis.

3. Clarification of Departmental Responsibilities

The National Risk Assessment helps to identify lead agency responsibilities within departments and agencies and, in some cases, between different levels of government for risk management and mitigating the consequences of disasters.

4. Facilitating collaboration between public and private sectors

Effective collaboration within the public sector, and between public and private sector stakeholders, means that the NRA can assist in securing consensus on priorities for the deployment of resources that may be in short supply. RA can be used to provide the basis of partnership between the public and private sector, by providing an agreed view of the risks. The Dutch and the Swiss have developed good practice in engaging the private sector (especially owners and operators of national infrastructure); the United Kingdom National Infrastructure Resilience Plan, which is based on the NRA (in which infrastructure owners/operators are not directly involved) and related guidance on infrastructure resilience to hazards, is worth reviewing.

5. The creation of a culture of risk management

The top risks facing most countries are by their nature complex and cross-cutting. The process of understanding risk is beginning to create a culture of risk management and growing interest in the potential of risk assessment to help formulate a forward-looking national risk management strategy.

6. Facilitates risk communication and awareness

The national Risk Assessment process helps governments to communicate basic messages about the most serious risk types. It is also helpful to demonstrate the way in which they are headed for the future to a broader more risk aware public and to other sectors of the economy. Being open about the risks helps contribute to risk awareness and the avoidance of complacency.

7. Inform horizon scanning for near term risks.

National Risk Assessment can connect with the whole continuum of risk management, and can also inform some shorter term horizon scanning. For example, the United Kingdom 'Forward Look' also provides best practice in the use of national risk assessments to inform horizon-scanning for near term risks for strategic crisis management, although it would be reasonable to say that 'forward look and the United Kingdom domestic horizon-scanning committee predated the NRA and could be sustained without it.

Benefits for Resilience Programmes

This is also useful for governments, with risk assessments now starting to provide evidence for improvement planning for continuity of government and emergency

response functions during disasters, and for community resilience programmes. In addition they are useful for risk-informed planning to provide insights for other security related initiatives such as national strategies for critical infrastructure protection. In particular, countries which have set up resilience programmes have found NRA useful in the following ways:

1. Prioritising decisions on risk mitigation

The National Risk Assessment process has been found to be useful in informing decisions on which risks should be prioritised for risk mitigation work by governments and on the best approach to mitigating such risks through prevention, improved preparedness for consequence management, or a mixture of both.

2. Capability planning

The National Risk Assessment process is used in capability analysis work to identify the capabilities needed to mitigate risks, identify the scale of the task needing to be planned for and therefore how much capability (capacity) may be required. An important step in deciding on the best treatment is to analyse existing risk controls and capabilities. Some do this as part of the risk assessment process and of these the Australian NERAG provides a good model for how to factor in the existing range of capabilities when constructing risk scenarios. Others carry out an assessment of existing capability as part of the subsequent risk treatment phase and, of these, the Netherlands and United Kingdom are as good as any. Risk assessments can also help to frame the requirement for generic capabilities that target the consequences of emergencies rather than the risks themselves; the United Kingdom approach to deriving consequence planning assumptions represents the best practice in aspect of resilience capability building, since it provides a consistent basis for judging not just capability but the capacity that may be required to insure against the worst case outcomes of a wide range of hazards and threats.

3. Build capability for community resilience at regional or local level

The National Risk Assessment process can assist to inform programmes which build capability at regional or local levels, and NRA can be used to promote community resilience and in this respect. Making the NRA available as a (in one case at least, web-based) tool for other sectors/local authorities use to assist emergency planning in their areas of responsibility is reported to have had real results in terms of operationalising the risk analysis at local government level. In this case local authorities having both completed their analysis using the method recommended by government and implemented changes to their planning for the risks of emergency. A number of countries have followed the United Kingdom example of publishing elements of their national risk assessments to mobilize households and businesses

4. As a basis for broader planning

The National Risk Assessment processes have provided useful background for broader planning to improve the resilience characteristics of all sectors. This includes the broader economy, where risk assessments form the basis for the exploitation of new national and international standards on business continuity and organisational resilience. For the environment, longer term assessment of the potential effects of climate change is beginning to feed into the national adaptation planning and building regulations.

Identified limitations to National Risk Assessments

While risk assessment can provide immediate benefits, translating risk assessment into resilience and budgeting for resilience is commonly seen as providing more of a challenge. A national risk assessment does not by itself define an acceptable level of risk or resilience for a country; rather it seeks to provide an objective assessment of the scale of challenges faced for the information of policy-makers, politicians and other stakeholders". The most commonly quoted limitations or challenges are as follows:

1. The challenge of risk evaluation

Judgements of how much investment will be proportionate to the risk can be informed by risk assessments, but given the impossibility of total mitigation, need also to be qualified by a political understanding of the tolerability of the residual risk after measures have been taken. For many countries, the most difficult challenge is therefore the need to set [what Germany calls] "protection goals" reflecting what is factually and politically feasible and to justify these goals by reference to a risk assessment that does not (and cannot) factor in these kinds of political judgement. For some countries, this may lead to a temptation to over- or under-state the level of risk portrayed in the risk assessment.

2. Using NRA to inform budgetary provision for resilience

This continues to defeat most countries. In the main this is because national resilience is not an absolute good to be purchased but a quality or characteristic of countries which is only partly engendered by investment in capabilities and capacities. In part also, it is because the costs of resilience have to be spread across a number of risks with a wide range of owners. The benefits to stakeholders are often hard to express in financial terms, many of them being non-material. Two countries, one on a limited basis Switzerland has attempted to put a financial value on the losses in their NRA process and Hungary, most have found (like Germany) that they lack independently validated data on economic loss assessments even for critical infrastructure.

3. The challenge of auditing resilience

A number of countries have pointed to the difficulty of using risk assessments in measuring the degree of resilience achieved as a result of the national resilience programme. In Germany with relatively mature programmes, there have been proposals made for a strategic-level audit of resilience capabilities, to see whether there has been a reasonable return on investment in resilience and to ensure that the burdens are being equitably shared between stakeholders.

Most countries have based their risk assessments on the inherent level of risk posed by the various kinds of event under assessment and are not able (or not yet) to demonstrate or measure the effect of mitigation measures on residual risk levels. Capability programmes can be audited but the heterogeneous nature of resilience capability means that the results of such audits may not be a true measure of resilience.

4. The foresight challenge

Increasing numbers of countries are being drawn to look much further ahead at the factors driving risk for the future and to speculate on the effects that these factors may have on risk. 'Over-the horizon' risk scanning may have different time-frames depending on whether the objective is to provide strategic early warning of future developments in the risk profile of the country to help the government decide on its priorities for longer-term investment (United Kingdom and in future the Netherlands). This helps

governments hedge their bets in building national resilience (US), or to assess the need to build additional (or less) resilience in national infrastructure assets with a lengthy life expectancy. National risk assessments are a necessary but not sufficient basis for this kind of risk trend analysis.

5. Resource constraints limitations

Some countries have pointed to the difficulty of finding the right **trade-off** between the resource requirements for detailed analyses, on the one hand, and the level of residual uncertainty on the other when analysis is less than thorough. These considerations come into play especially as countries start to move beyond analysing the kinds of capability required for emergency response, towards capacity planning (how much capability is needed or justified) and the requirement for thorough financial planning. These moves tend to be accompanied by a reduction in reliance on qualitative assessment of impacts and likelihood towards more quantitative assessment which in turn demands improved data (historical, scientific, and technical). This may only be on a selective basis. This in turn gives rise to limitations caused by **resource constraints** (i.e., availability of experts and financial funds to conduct risk assessments on a sustainable basis) which may inhibit the detailed research needed to assess particular risks. Although risk assessment itself is not a particularly expensive activity, there are categories of resource, especially for areas requiring cross-disciplinary approaches that may be in short supply.

6. Participation of stakeholders and experts in risk assessment

A key resource directly constraining the effectiveness of the risk assessment is the participation of stakeholders and experts in risk assessment. Most countries report that there are limits to the availability of some key stakeholders in their NRA processes. There is a requirement to further examine improvements in governance, in the engagement of stakeholders in the private, academic and NGO sectors, as well as at regional and local government level.

Others who have done this for longer have suggested that there is a problem of 'risk assessment fatigue'. This is when the initial benefits have been reaped and successive iterations are seen to have progressively smaller yields and before the risk management culture has had time to become properly embedded in the body politic.

7. Methodological issues

Methodological issues are on the whole comparatively less challenging. In this respect there continue to be issues concerned with the validity of the comparison between the likelihood of threats and the plausibility of hazards, the weight to be given to non-material impacts, the most useful approach to treating uncertainty; and the correct approach to multiple risks.

Broader policy outcomes: framing risks at a higher level

The main outcomes of the process have been that national risk assessments have helped to give perspective to the risks facing nations, and to elevate national resilience as a policy priority. As 'objective, dispassionate, inventories' of what would have to be reckoned with in a disaster, they have helped to make the case for investment in resilience in an increasingly competitive national security field, and informed the optimal allocation of scarce resources.

These include variations of National resilience strategies usually incorporating national security strategies, identifying specific risks as priorities, and setting out the approach to risk prevention, protection of the public and other key assets including the preparedness for response and recovery plans. These include: Contingency plans for the most serious kinds of emergency, with mechanisms to improve governments' ability to anticipate them: National resilience programmes which aim to bring about improvements to the capabilities and capacities of emergency responders at all administrative levels, as well as the community: Infrastructure and business resilience programmes: usable analysis of risk trends in order to provide a longer term perspective to major national security programmes.

The outcomes have been that national risk assessments have helped to give perspective to the risks facing nations, and to elevate national resilience as a policy priority. As objective, dispassionate, inventories of what would have to be reckoned with in a disaster they have helped to make the case for investment in resilience in an increasingly competitive national security field, and informed the optimal allocation of scarce resources. These are the beginnings of a risk management culture.

Chapter 5. Conclusion and areas for future action

This chapter presents the overall conclusions from the cross country analysis, and identifies key areas for future action.

This report presents a cross country overview of the process and methods that governments use to conduct national risk assessments. The United Kingdom pioneered this increasingly popular tool in 2004/05 to proactively manage complex emergency risk portfolios in a coordinated manner, closely followed by the Netherlands. Yet the systematic analysis of risks has been a feature of some governments' core decision-making for at least twenty years. Early starters included Australia and New Zealand, which began using the risk management standard that would become the basis for the International Standards Organisation standard 31000: 2009 on Risk Management. Estonia developed guidelines on risk assessment for government ministries in 2002, and Denmark developed a first guidance on Risk and Vulnerability Analysis in 2005 for voluntary use by departments and agencies.

The way in which risk analysis is used by countries depends on the nature of the challenges that they face. Some disaster risk profiles are dominated by the threat of major natural hazards, which presents significant challenges for the country's balance of investment in prevention, protection and response capabilities. For some, the greatest risk is uncertainty – from a concern that the worst of the harm may come from perils or vectors that are least understood. Many countries consider themselves to be relatively free from disaster risk, with no major threat dominating. But nearly all suffer from the unpredictable and often cascading consequences of the interaction of traditional, and quite well-known, hazards with new and less well known vulnerabilities arising from advances in science and technology and the greater interconnectedness of societies (OECD 2011).

The inability of governments to predict how these kinds of composite disasters may affect the safety of their citizens has strained public trust at the same time as responsibilities for risk management have increased. Most governments surveyed, therefore, are strongly motivated to communicate, to populations that are used to more absolute standards of protection against traditional security threats, that the risk of disaster cannot be eliminated and may not be controllable; and that, in times of austerity, choices have to be made on how much to invest in resilience to events that may be very destructive but rare, and how much in the more commonplace but less damaging incidents. Resilience differs from traditional notions of security also because it is not (or not only) a public service or good that governments have to provide, but a characteristic of communities large and small for which some measure of responsibility lies with the communities themselves. But, even in the larger sense, it is a government responsibility to provide a framework within which business and other communities can reinforce their own resilient qualities. Communicating the outcome of risk assessments provides the basis of guidance on risk and how it can affect these communities.

These two driving factors (growing risk and responsibilities; the need to mobilise sceptical publics and other stakeholders) determine the main ways in which NRA can be used.

Within government – to build consensus, and to optimally allocate limited resources to protect citizens, economic livelihoods and property, building capabilities in a way that is proportionate to the risks.

Outside government – to engage with stakeholders in the wider public sector, private sector and communities to obtain their assistance in building broader socio-economic resilience.

Key areas for future action

This report draws on an exceptional wealth of information, based on the experience of a wide range of countries, some of which with the longest history and the deepest experience in this area. As a result of the cross country analysis, the following nine actions should be considered by governments when thinking to establish national risk assessments or review existing ones.

- **Deploy National Risk Assessments as part of a larger overall risk management strategy** where the National Risk Assessment has been used, its main value is to inform a larger overall risk management strategy. It is a crucial part, of a risk management cycle, where the results of the NRA can be used for a variety of emergency management and planning functions including the evaluation of risk, which determines what the government's risk appetite is and the priority attached to reducing particular risks. In this instance these functions benefit from the prior involvement of policy makers as one of the key groups of stakeholders in the risk assessment process. Therefore, risk assessment should not be wholly contracted out even to subject-matter experts and should remain in the realm of policy makers within government institutions.
- **Identify and engage stakeholders early and often.** The identification of and engagement with stakeholders is among the most significant tasks that practitioners of National Risk Assessments should begin early and conduct often. Through engagement and consultations, the NRA process can meet the need of diverse sets of stakeholders. This prior engagement facilitates discussion and agreement on the method of assessing risk and for roles to be clear is an important feature. Discussion of methodology needs to recognise that it is for governments and decision makers to decide on the scope of the national risk assessment, on criteria for the risk assessment, and on risk evaluation, but where non-government bodies (e.g., the private sector) are engaged in the process, their interests should be consulted. This early engagement increases the pool of policy-makers and subject-matter experts who have developed a degree of understanding of the principles and potential application of risk assessment. The optimal mix of experts helps build a common understanding of the assessment, develop consensus on the outcomes, and buy-in to the resulting action plan. This should include subject matter experts both within and outside government circles including government research establishments, academic institutions and the private sector. The encouragement of broad participation will foster buy-in and support for the outcomes. This helps in building resilience and assists in crisis situations where an analytical approach to impact assessment and the existence of an estimate of the intensity, scale and duration of likely impacts can provide responders with a head start.
- **Adopt an All-Hazard approach for National Risk Assessments.** All countries in this study consider a wide range of risks that they might reasonably be expected to experience in the foreseeable future. Fewer countries than expected, however, include the full range of risks that could cause significant physical harm and eventually fall within the remit of civil protection or emergency management agencies. The fewer the exclusions the better, if the value of comparative risk assessment is to be maximised.

- **Use results of National Risk Assessments to inform policy decisions**. Risk assessment is not conducted for its own sake. Many countries could make fuller use of the results of NRA to inform risk management functions and planning decisions in a civil protection context. While most countries do use the results to establish a contextual overview for the design of civil protection exercises and training modules, far fewer countries use them for capabilities based planning, investments and/or funding decisions for risk prevention and mitigation measures, heightening the awareness and understanding of risks in the population, and the development of emergency management plans.
- **Assign clear responsibility to lead the process, and clarify risk ownership across government.** Countries need to review the governance and co-ordination mechanisms that are necessary to integrate information from a diverse set of government bodies, with a cross government mandate and to promote horizontal integration. The wider implications of national emergencies imply the process should involve an overall lead co-ordinating body with access to Cabinet level authority and the mandate to enlist experts from across government departments. One or more departments should be designated as the "risk owner", i.e., front line responsibility for managing the consequences, of every risk identified in the National Risk Assessment. Such co-ordination has historically been a weakness when carried out in an ad hoc fashion, or as a specialist function of a single ministry. The co-ordination implies setting up a framework policy or legislation for all-hazards risk management; a new central government body or existing body with an enhanced cross-government mandate; and an inter-Ministerial committee or processes to promote and reinforce horizontal integration of risk policies
- **Ensure that the methodology produces comparable results.** The methodology for a National Risk Assessment should produce results that make it possible to compare one national risk to another using the same criteria for analysis. While the details in methodology will differ due to a country's unique conditions, the results should be suited to support civil protection planning, the impact categories should be measurable and uncertainties should be identified and explained.
- **Present the results to policy-makers and/or appropriate legislative committees for formal adoption.** Presentation and adoption of reports by government raises awareness of risks, promotes transparency and fosters high level dialogue on the acceptable levels of risks, which is key to designing coherent risk management policies. A formal process of validation at high level puts the government's stamp on risk ownership for complex risks, and can incentivise experts to collaborate in the process from across government.
- **Publish the results** of the National Risk Assessment. Governments should make the National Risk Assessment outcomes accessible both within and outside government. The outcomes should be communicated more broadly to the population in an abridged or declassified format to promote business and community resilience, and also to regional and local authorities to remind them of their responsibilities for a national level emergency response. Risk communication enhances the accurate perception of risk, but most individuals and organisations tend to focus on the risks to which they are directly exposed. A failure to notify, on the other hand, imparts a sense of complacency and underestimation of the prevailing risks that could lead the public to take insufficient precautions.

- **Foster a continuous review process.** The experience shows that most countries see the need for continuous iteration of their risk assessment, and its adaptation to changing contexts to provide reassurance to stakeholders that it is reliable, and that it continues to be relevant in light of changes in the risks, as an evidence base for strengthening country resilience. It is common to see this as a cyclical process in which not only the risks, but the criteria for assessing them, and other methodological aspects, are subject to review. The cycle does not have to be an annual cycle (and many countries find yearly reviews both onerous and unnecessary once the NRA is established) but it has been acknowledged that it should be reviewed on a regular basis.

References

Commission Staff Working Paper: "Risk Assessment and Mapping Guidelines for Disaster Management" SEC (2010) 1626, Brussels 21.12.2010. Available at: http://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf

Germany: Federal Office of Civil Protection, Method of risk Analysis for Civil Protection. Available at: http://www.bbk.bund.de/SharedDocs/Downloads/BBK/EN/booklets_leaflets/Method_of_%20Risk_Analysis.pdf?__blob=publicationFile

Kates R.W, C Hohenemser and J Kasperson (1985): Perilous Progress: Managing the Hazards of Technology, Westview Press, Boulder.

Government of Hungary, National Disaster Risk Assessment Framework and Strategy, Hungary: Methodology and Process of the National Risk Assessment.

Cabinet Office of the United Kingdom (2017).National Risk Register of Civil Emergencies. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf

OECD (2011), Future Global Shocks: Improving Risk Governance, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264114586-en.

OECD (2012), Analytical Framework on Disaster Risk Assessment and Disaster Financing. Available at: https://www.oecd.org/gov/risk/G20disasterriskmanagement.pdf.

OECD (2014), Recommendation of the Council on the Governance of Critical Risks. Available at: http://www.oecd.org/gov/risk/Critical-Risks-Recommendation.pdf.

OECD (2009), Studies in Risk Management, Innovation in Country Risk Management.

Further reading

AS/NZS 4360:1995 Risk Management

ISO 31000, ISO 31010, and ISO Guide 73

PART TWO:

National Risk Assessment – Country Profiles

Part Two of this report presents summaries of the National Risk Assessment processes in 20 countries, based on information collected through interviews conducted between 2013 and 2016. Each country summary provides an overview of the governance framework within which national risk assessments are conducted. The country summaries also describe the objectives of the National Risk Assessments, and provide details of the methods in use for analysing, assessing and evaluating national risks; the use of national risk assessment to inform public policy design, and to raise wider public awareness about risks. The summaries also document challenges that countries have encountered, as well as the perceived benefits and final uses of National Risk Assessments. The information reflects the state of National Risk Assessment in countries at the time collected.

Chapter 6. AUSTRALIA

Australia was one of the first countries to develop a standardised risk management approach to the identification of hazards. This chapter discusses the governance framework for risk management in Australia and the importance of the National Emergency Risk Assessment Guidelines (NERAG) which introduced the reform methodology for a top down bottom up approach to risk management. The chapter also discusses transparency and accountability in the context of the risk assessment process and the hazard identification approach initiated by the NERAG. Impact analysis, likelihood and plausibility analysis form part of the process with a standardised approach being provided. The NERAG also advises that likelihood calculations can be based on elements of probability within the overall approach. The chapter discusses risk evaluation monitoring and re-evaluation as part as the ongoing risk management process as well as the importance of using the national risk profile to raise awareness of risks.

Key Words: Governance; Hazard and Impact analysis; Lessons learnt; Standardised approach.

Introduction

In 2004, in response to concerns about potential increases in the frequency of severe weather events, the Council of Australian Governments (COAG) concluded that a new approach to natural disasters in Australia was needed involving a fundamental shift in focus beyond response, relief and recovery towards cost-effective, evidence-based disaster mitigation. Supporting this approach called for a "systematic and widespread national process of disaster risk assessment". In 2007, the Australian Emergency Management Committee endorsed a National Risk Assessment Framework to support the development of an evidence-base for effective risk management decisions and to foster consistent base-line information on risk. The National Emergency Risk Assessment Guidelines (NERAG) have been developed as one of the first outputs of the framework's implementation plan. As such, they provide a methodology to support the reform commitments and risk and data objectives recommended by COAG.

Governance framework

Australia is one of the pioneers of a risk management approach to hazards, having (twenty years ago, with New Zealand) developed a risk management standard (AS/NZS 4360: 1995 Risk Management) which, in its 2004 version formed the basis of the International Standards Organisation's ISO 31000: 2009 on Risk Management, and was adopted by many organisations in and outside Australia as the basis for their approaches to risk management. The publication of NERAG guidelines follows the pattern of providing a consistent basis for risk assessment at all levels (local, State, national) and for organisations in the public, private and voluntary sectors. Where risk assessment is carried out by public authorities, they will follow the methodology in the NERAG, the purpose of which is accordingly to "improve the consistency and rigour of emergency risk assessments, increase the quality and comparability of information on risk, and improve the national evidence-base on emergency risks in Australia, providing therefore a contextualised emergency risk assessment consistent with the Australian/NZ version of ISO 31000".

The NERAG does not dictate the governance arrangements that will be appropriate to governments and other organisations using the guidelines, but the guiding principles for emergency risk management (ERM) make the clear the importance of:

- Mainstreaming ERM activity so that it is effectively integrated into standard business practices of organisations, governments and communities.
- Involving decision-makers and other stakeholders in a transparent way.
- Basing decisions on ERM on the best available data and information from a variety of sources, ensuring that decision-makers are aware of the limitations of data and modelling, and of any divergence of opinion among experts.

Aims and Objectives

The purpose of risk assessment is described in the NERAG in the following terms: a sound understanding of the risk of disasters is necessary to allow communities, organisations and governments to understand and measure the risks involved and to decide on the appropriate measures to manage them:

- to minimise their consequences
- to determine risk management priorities
- to compare the levels of risk against predetermined standards.

The NERAG points out that, in Australia, risk assessment models can generally be categorised by their complexity, which can range from simple – mostly qualitative approaches which are mainly used for "screening" risks – to detailed models which often use quantitative models and can involve higher order spatial data analyses and impact modelling. The more complex models are often used to supplement qualitative approaches, the level of complexity being determined by the need to address uncertainty and the rigour required, in particular, to justify high-cost risk treatments.

NERAG also points to the value of risk assessment work in communicating risk to all stakeholders – internal and external – who may need to be involved in the process of risk management, because they have either particular responsibilities or a vested interest in the process.

Definition of key terms

The NERAG sets out a Glossary of key terms.

Transparency and accountability

NERAG emphasises the need for communication and consultation with internal and external stakeholders throughout the risk management process. Those with responsibility or a vested interest should not only be kept informed but also be invited to contribute to the process, in order to establish a common understanding of how decisions are made. NERAG also invites consideration of the use of adversarial groups or stakeholders in the process to minimise any ongoing criticism, and reduce the possibility of subjective bias in the assessment process; and systematic recording of differences in the perception of risks by participants.

Multi-level governance and multi-actor participation

The purpose of the NERAG is to promote consistent use of risk assessment by governments, organisations and communities at all levels.

Risk analysis

The risk assessment process is portrayed in NERAG as integral to the risk management framework outlined in the Australian and New Zealand standard. It has five steps: establishing the context for the risk assessment; identifying risks; analysing risks; evaluating risks; and treating risks (for definitions see Annex B). A workshop environment is recommended but alternative structured approaches are also described.

Scope

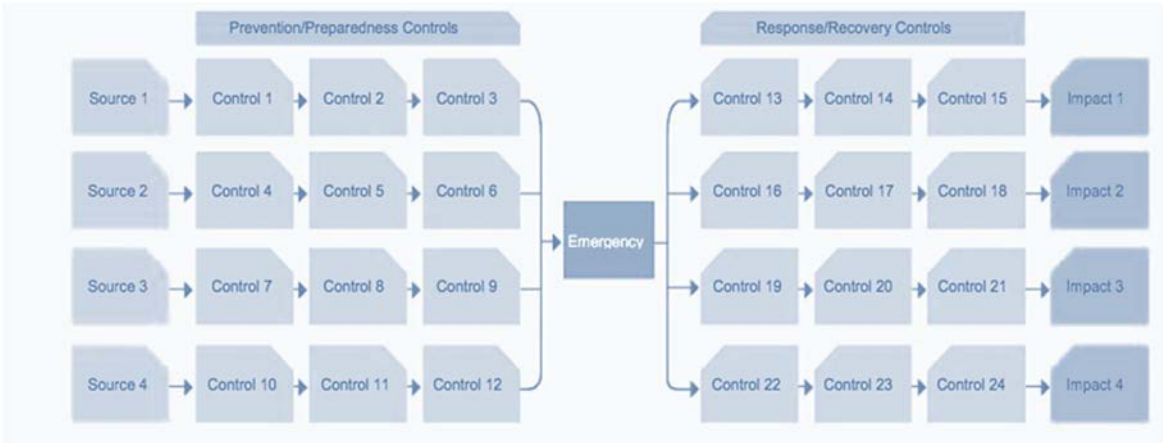
The first of the five steps (establishing the context) is designed to set the basic parameters for the risk assessment including the scope. The over-riding objective of managing the risks of harm to communities from all sources means that an all-hazards approach is taken including sudden onset natural hazards (such as bushfire, cyclone, storm surge, debris flow, tsunami and tornado), disease (human, animal and plant),

insect/vermin plague, and risks arising from technological and other anthropogenic sources. The guidance draws attention to the need to consider multiple sources of risk, and secondary or consequential effects of either single or multiple risks; and also, to consider both "risks from" hazards and "risks to" key assets or objects of value.

Hazard Identification

A scenario-based approach is proposed, in which all hazards or threats to communities are identified and described in terms of the hazard, the vulnerability of the community and the associated risk of harm. NERAG encourages a comprehensive gathering of information on the sources of risk, current controls, events and their possible causes, areas of impact and potential consequences. Historical information, theoretical or computational analysis, expert opinions and stakeholder interests are pooled; and risks are identified by using a "bow-tie" diagram (Figure 6.1) that illustrates (a) pathways leading to the emergency; and (b) prevention/preparedness and response/recovery controls. The bow-tie diagram is recommended because it combines the advantages of team-based brainstorming and of more structured techniques such as systems analysis, because it is a graphic representation of the relevant emergency, depicting a storyline for a loss to a community which identifies areas that are critical in controlling risk.

Figure 6.1. Example of the bow tie diagram



Source: National Emergency Management Committee (2010), "National Risk Assessment Guidelines", Emergency Tasmanian State Emergency Service, Hobart.

Impact Analysis

NERAG offers a choice between qualitative, semi-quantitative and quantitative methods of measuring impact and the likelihood of particular consequences occurring. In practice, it suggests that qualitative analysis (which is based on people's experience of risk rather than any more objective calculation) is used to obtain a general indication of the level of risk and to reveal the major risk causes, to which at a later date more quantitative analysis is applied as part of the process of development a business case for risk treatment. Since risk controls (behavioural, procedural and physical) are built into the risk scenarios and risk analysis, the NERAG methodology is unusual in building into the process a first stage of assessment of the effectiveness and reliability of existing controls.

Consequences tables are provided which set out an independent and standardised rating for each of six categories of impact:

1. People – relates to the direct impacts on the physical health of people and the ability of the health system to manage.
2. Environment – relates to the impacts on the ecosystem of the area including fauna and flora.
3. Economy – relates to the economic impact on the governing body as reported in the annual operating statement for the relevant jurisdiction, and industry sectors as defined by the Australian bureau of statistics.
4. Public administration – relates to the impacts of the emergency on the governing body's ability to govern.
5. Social setting – relates to the impacts on society and its social fabric, including its cultural heritage, and resilience of the community.
6. Infrastructure – relates to the impacts on the area's infrastructure/lifelines/utilities and its ability to service the community.

The ratings proceed from "insignificant" to "catastrophic" in five steps, each of which is greater by a factor of between 3 and 10 than its predecessor. An example showing the scales recommended for use in estimating economic consequences is at Annex 6.A1.

Likelihood and Plausibility Analysis

A standardised approach is also taken in the measurement of the likelihood of a particular level of harm being sustained. NERAG advises that likelihood calculations can be based on probability and can be expressed in various ways, such as recurrence intervals, exceedance probabilities, return periods, probabilities or frequencies. But NERAG advocates annual exceedance probability (AEP), or the chance of the event occurring once in a year, to determine likelihood, expressed as a percentage. A logarithmic scale is used for likelihood levels, because the probability of emergency events can cover several orders of magnitude (Table 6.1).

Table 6.1. Likelihood level

Likelihood	**Annual exceedance probability (AEP)**	**Average recurrence interval (ARI) (indicative)**	**Frequency (indicative)**
Almost certain	63% per year or more	Less than 1 year	Once or more per year
Likely	10% to <63% per year	1 to <10 years	Once per 10 years
Unlikely	1% to <10% per year	10 to <100 years	Once per 100 years
Rare	0.1% to <1% per year	100 to <1000 years	Once per 1000 years
Very rare	0.01% to <0.1% per year	1000 to <10,000 years	Once per 10,000 years
Extremely rare	Less than 0.01% per year	10,000 years or more	Once per 100,000 years

Source: National Emergency Management Committee (2010), "National Risk Assessment Guidelines", Emergency Tasmanian State Emergency Service, Hobart.

The outputs generated by the risk assessment are used to determine possible action. Before decisions are made, however, NERAG recommends an indication of the

robustness of the risk assessment approach. To achieve this, the level of confidence in the risk assessment process is used to identify and communicate uncertainty.

Assessing confidence helps to avoid misleading results, because influences in the process (e.g., subjective perceptions or lack of data) can be identified and addressed. Assessing confidence also addresses decision makers' concerns for whether there is a need for more detailed risk assessment. "Confidence" refers to the:

- Reliability, relevance and currency of the evidence used to support the assessments.
- Use of appropriate expertise as part of the risk assessment process to assign consequence and likelihood levels.
- Level of agreement between stakeholders.

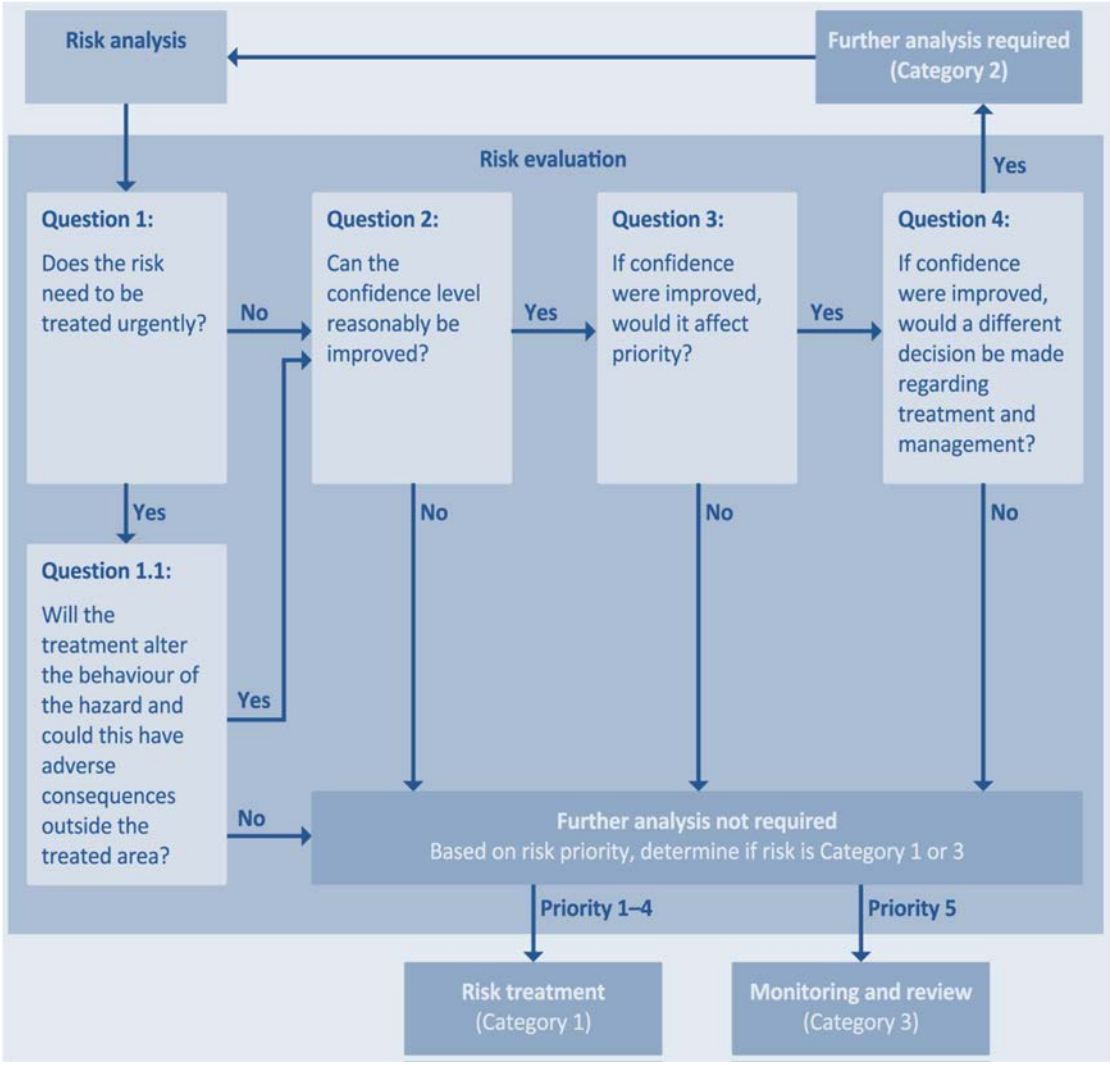
Confidence must be assessed at least once for each risk assessed. Confidence assessments can refer to the risk level, or independently to the likelihood and consequence levels. Accordingly, there are two options assessing confidence: a single overall confidence assessment; and separate confidence assessments of likelihood and consequence, which can then be used to derive an overall confidence level.

Risk evaluation, monitoring and re-evaluation

Risk evaluation process is carried out to assign a priority to each risk, based on the risk level and confidence associated with that risk. The priority is a level from 1 (highest priority, requiring the highest level of attention) to 5 (lowest priority, requiring monitoring and maintenance of existing controls). Prioritisation of risks guides practitioners and sponsors to the order in which risks need to be addressed. The response to a level of priority is either to improve the confidence level of the risk (if possible) through research, further expert opinion or further studies , or to treat the risk by taking action to reduce the likelihood or consequence of the risk, or to monitor and review the risk as part of the ongoing risk management process. Priority is determined by the risk level (higher risk level leads to higher priority) and the level of confidence (lower confidence leads to higher priority). Each evaluated risk is placed in a risk register and assigned to one of the following categories as demonstrated in Figure 6.2:

- **Category 1: Risks requiring treatment (with confidence to determine treatment objectives)** for which the information contained in the risk register provides guidance to determine treatment objectives.
- **Category 2: Risks requiring further analysis and subsequent re-evaluation** in the form of a revised baseline assessment or a detailed assessment, which will then lead to a re-analysis and re-evaluation of the risk.
- **Category 3: Risks (currently) requiring ongoing monitoring and maintenance of existing controls** during the ongoing risk management process.

Figure 6.2. The decisions that determine risk categorisation



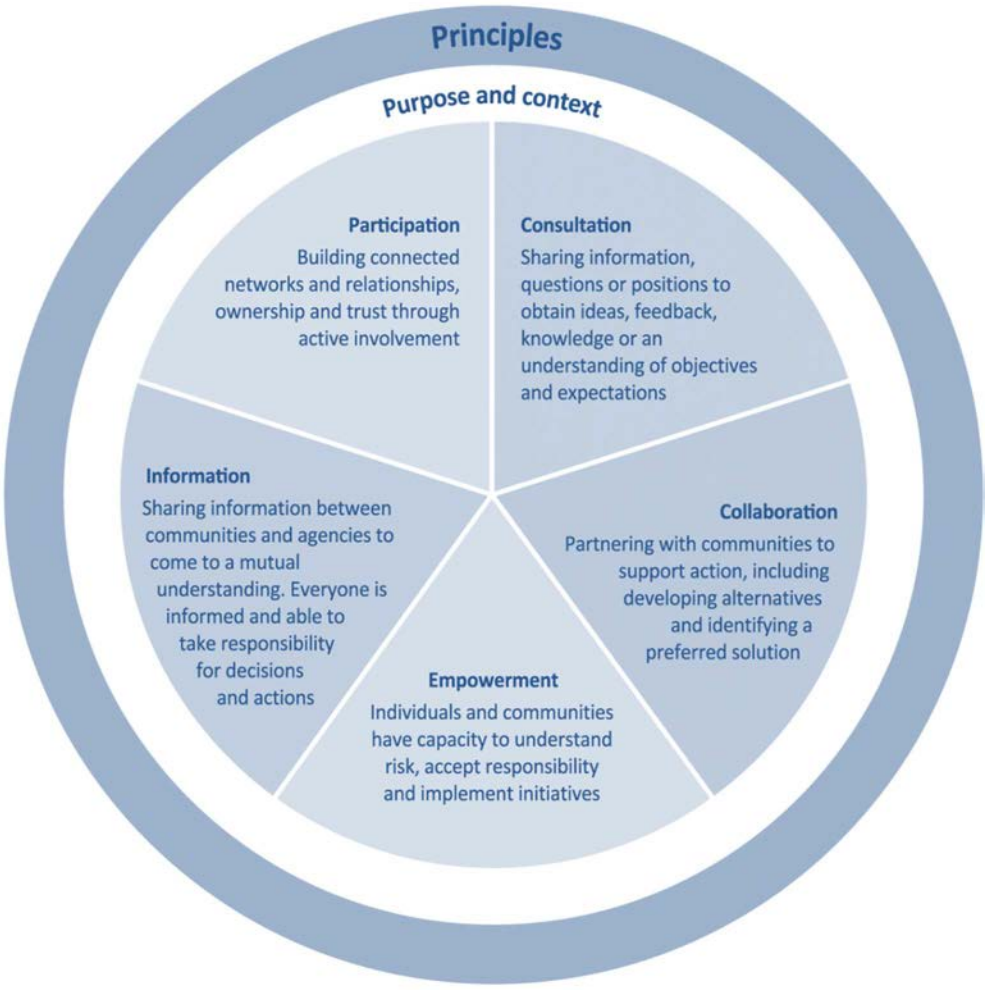
Source: National Emergency Risk Assessment Guidelines (2015), Australian Emergency Management Handbook Series, available at: https://www.aidr.org.au/media/1413/nerag-handbook10.pdf.

Communicating the results of National Risk Assessment

Using the National Risk Profile to raise awareness about risks

NERAG advocate continuous engagement with the many stakeholders involved in the risk assessment process, and the community. It emphasises the need for clarity about the objectives of communication and understanding of what stakeholders can contribute (their capacity, strengths and priorities), recognition of the complexity and the potential connections inherent in the diversity of the stakeholders; and the principle of partnership with stakeholders to support existing networks and resources. Figure 6.3 shows the NERAG's framework for engagement with stakeholders, being circular to show that one engagement approach is not necessarily better than any other, and that different approaches are legitimate depending on the purpose and context of a particular situation. Good engagement practice relies on choosing the right approach or combination of approaches for engagement in different situations.

Figure 6.3. Purpose and context for engagement with stakeholders – the NERAG framework



Source: National Emergency Risk Assessment Guidelines (2015), Australian Emergency Management Handbook Series, available at: https://www.aidr.org.au/media/1413/nerag-handbook10.pdf.

Tools for interpreting risk analysis

NERAG sets out a number of analytical tools, with comments on the alternatives and recommendations on the preferred choice.

Main lessons learnt and policy outcomes

NERAG recommends setting a timeline for monitoring and reviewing the outcomes of the process. This and the responsibility for programming reviews should be included in the risk management framework. The reason given is that nature of emergency-related risk changes over time, and so do priorities, perception and culture. The monitoring and review process should be documented as part of reporting the risk register and risk management plan, including:

- Ensuring the identified controls are operating effectively and adequately, and have not changed over time.
- Ensuring the best and most up-to-date available information is used as evidence for the likelihood, consequence and confidence levels.
- Incorporating information from emergency events that may have occurred since the last risk assessment.
- Accounting for changes in the context of the risk assessment.
- Identifying and accounting for emerging risks.

References

National Emergency Risk Assessment Guidelines (2015), Australian Emergency Management Handbook Series. Available at: https://knowledge.aidr.org.au/resources/handbook-10-national-emergency-risk-assessment-guidelines/

National Emergency Management Committee (2010), "National Risk Assessment Guidelines", Emergency Tasmanian State Emergency Service, Hobart.

Further reading

Australian/New Zealand Standard: Risk management, Standards Association, 1995, Melbourne. Available at: https://infostore.saiglobal.com/preview/as/as4000/4300/4360-1995(%2ba2).pdf?sku=381545

Annex 6.A1

Table 6.A1. Economic consequence levels and criteria

	Criteria	
Level	**Loss in economic activity and/or asset value**	**Impact on important industry**
Catastrophic	Decline of economic activity, and/or Loss of asset value greater than 4% of gross product produced by the area of interest	Failure of a significant industry or sector in area of interest as a direct result of emergency event
Major	Decline of economic activity, and/or Loss of asset value greater than 0.4% of gross product produced by area of interest	Significant structural adjustment required by identified industry to respond and recover from emergency event
Moderate	Decline of economic activity, and/or Loss of asset value greater than 0.04% of gross product produced by area of interest	Significant industry or business sector is significantly impacted by the emergency event, resulting in medium-term (i.e., more than one year) profit reductions directly attributable to the event
Minor	Decline of economic activity, and/or Loss of asset value greater than 0.004% of gross product produced by area of interest	Significant industry or business sector is impacted by the emergency event, resulting in short-term (i.e., less than one year) profit reductions directly attributable to the event
Insignificant	Decline of economic activity, and/or Loss of asset value less than 0.004% of gross product produced by area of interest	Inconsequential business sector disruption due to emergency event

Source: National Emergency Risk Assessment Guidelines (2015), Australian Emergency Management Handbook Series, available at: https://www.aidr.org.au/media/1413/nerag-handbook10.pdf

Chapter 7. AUSTRIA

Austria's National Risk Assessment or as the Austrian Government has called it, the National Risk and Threat Assessment (NaTRAn) was developed as a result of a new national security strategy introduced in July 2013 which replaced the 2001 Security and Defence Doctrine. This chapter discusses the background of this new initiative based on a new risk management approach which relies on strategic planning and a common methodology for analysing the risks across a number of areas. An important element of the strategy discussed is the dual function of the strategy being able to meet the demands of both national and international requirements. This includes the various EU Directives and programmes and deadlines for implementation of critical infrastructure and cyber response requirements. The chapter also discusses the approach that Austria has taken in respect to governance and the participation by the multiplicity of stakeholder in the different levels of government and those with horizontal cross-cutting responsibilities in the risk assessment process.

Key Words: Hazard and Impact analysis; Lessons learnt; National Risk and Threat Assessment; Participation; Risk based approach.

Introduction

In March of 2011 the Austrian Government agreed a new national security strategy, replacing the 2001 security and defence doctrine. The new National Security Strategy was subsequently endorsed in July 2013 by the first Chamber of the Austrian Parliament (Nationalrat) and the Government was requested to implement the Strategy. Implementation will be subject to periodic evaluation by the National Security Council (NSC) and a review process has been established. Austria's security strategy brings under one umbrella both external security and a domestic resilience initiative[1] under a "comprehensive security provision concept" based on national risk and threat assessment (NaTRAn) covering a broad range of strategic-level threats and hazards (Table 7.1).

Table 7.1. Austria's 2013 national security strategy – main classes of risk and threat

1. Conventional military attack	9. Organised crime, drug trafficking
2. International terrorism	10. Corruption
3. Proliferation of WMD	11. Illegal immigration
4. Domestic or regional conflicts/turmoil	12. Failed integration
5. "State failure"	13. Scarcity of resources, climate change, environmental damage, pandemics
6. Natural or man-made disasters	
7. Cyber attacks	14. Piracy and threats to transport routes
8. Threat to strategic infrastructure	15. Financial and economic crises

Source: Austrian Security Strategy (2013)

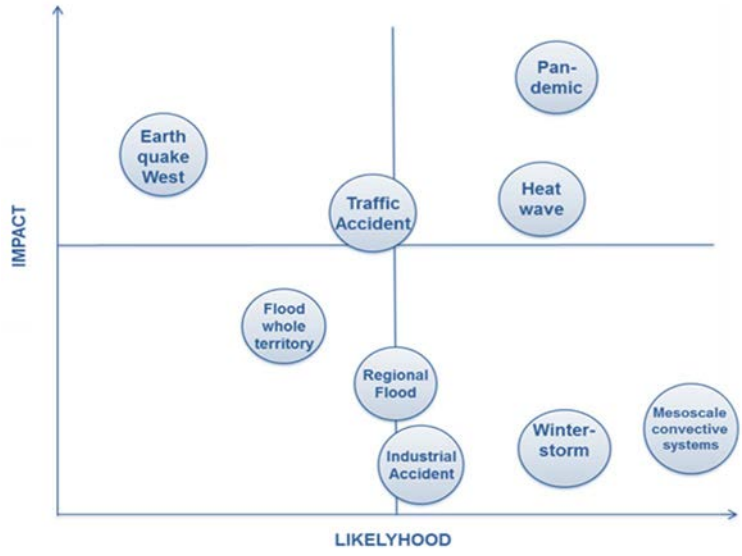
As part of the new national security strategy, a national resilience initiative was established, based on a risk management approach and relying on strategic planning in the areas of: civil protection against natural or man-made disasters, critical infrastructure protection, cyber security, and uncontrolled illegal migration. A common methodology for analysing the risks in all these areas has been in development since November 2013.

Implementation of this approach coincided with the decision of the European Parliament and Council of December 2013[2] that Member States should develop risk assessments at national or sub-national level and make available to the Commission a summary of the relevant elements by December 2015 and every three years after. Austria's approach to national risk assessment also took into account the recommendations of the OECD Council of Ministers on the governance of critical risks, the global United Nations International Strategy for Disaster Reduction (UNISDR) post 2015 Framework for Disaster risk Reduction as well as the implications of the EU Floods Directive. All of these pointed to the utility of national risk assessment in determining the priority for investment in reducing the risks of disasters and building resilience.

In 2013, the national Co-ordinating Committee for Crisis and Disaster Management (SKKM – a body set up in 2004 to co-ordinate Austria's crisis and disaster management system) set up a group of risk specialists to elaborate a first disaster risk analysis. The Federal Ministry of the Interior, as the lead authority in Austria for co-ordination of civil protection and disaster management approaches, provided a first report to the Federal Government on the state of play in national disaster risk assessment which was endorsed by the Council of Ministers on 23 September 2014. The report described the status quo (Figure 7.1) and Austria's approach to establish a comprehensive national risk assessment. This is not yet a complete national risk assessment and, as is the case in a number of countries, there is some hesitation about making direct comparisons between all these very different areas of risk.

The next steps are conceptualised in parallel and within a project called GERIAN (Gesamtstaatliche Risikoanalyse) funded under the National Security Research Program. GERIAN envisages a "family" of risk assessments operating under broadly consistent methodologies and covering the areas of: Natural/Man-Made Disasters; Cyber Risks; critical Infrastructure Protection; Energy Resilience; Health; Finance; and Uncontrolled Migration. This approach will now be applied to a number of risk scenarios. It is not yet clear whether or not all the different risk categories will in fact end up being presented on a single risk matrix. The sum of all risk assessments will provide a comprehensive picture of a National Risk and Threat Analysis (NaTRAn).

Figure 7.1. Indicative national risks in Austria's national risk assessment process



Source: presentation of the Office for Security Policy Federal Ministry of the Interior on national Risk Assessment in Austria.

Governance framework

Aims and objectives

The NaTRAn will enable the Austrian government to comply with the EU Directive and other international policies relating to the identification, analysis and management of critical risks. In the policy sense, the national risk assessment is designed to focus

national attention on the risks that provide the basis for the national resilience concept within Austria's security strategy. Risk assessment within each of the sectors within the strategic risk "family" is designed to help elaborate and meet the specific objectives in the national security strategy relating to that sector, viz.:

- Maintaining social peace and social cohesion in Austria and promoting a good and safe coexistence.
- Ensuring the availability of vital resources.
- Enhancing the resilience of the public and private sector when faced with natural or man- made disruptions and disasters.
- Maintaining an efficient national economy and taking precautions for the eventuality of crisis- related economic disruptions, safeguarding the supply of vital goods to the population, and protecting critical infrastructure.
- Maintaining a liveable environment as part of comprehensive environmental protection and minimising the negative effects of natural or technological disasters.
- Combating international terrorism, organised crime and corruption.
- Promoting a broad awareness of security amongst the population.

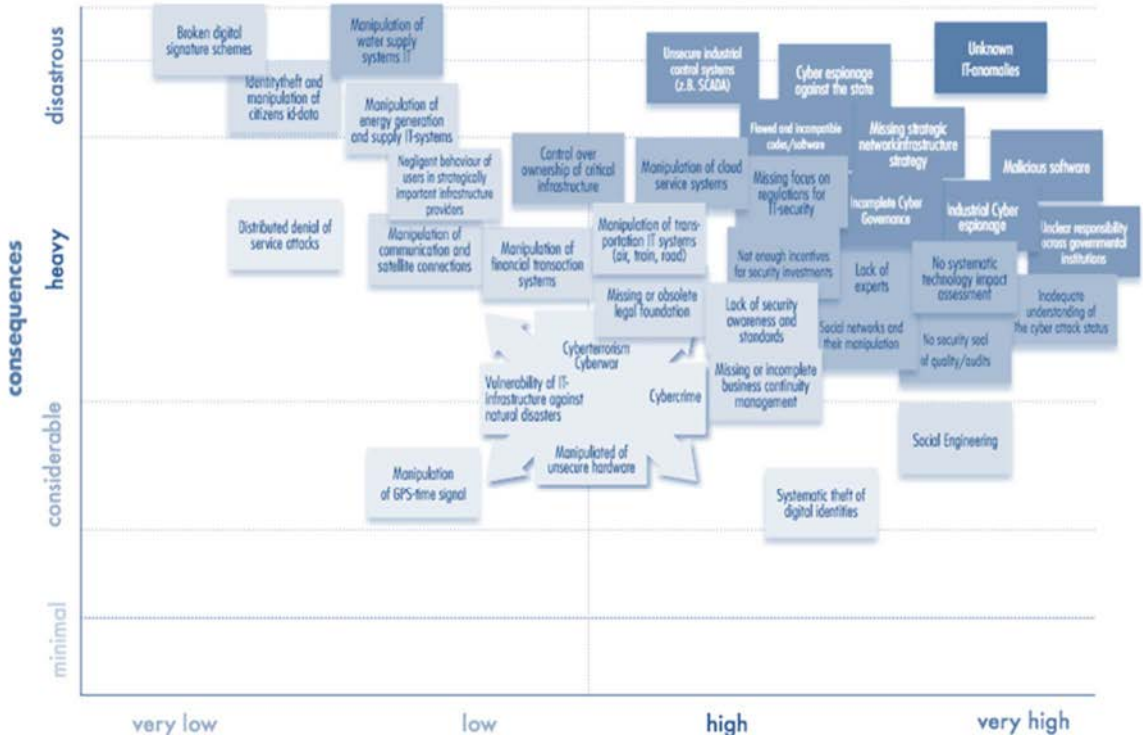
Critical Infrastructure Protection

The Austrian Programme for Critical Infrastructure Protection APCIP has run from April 2008, which is the date of the adoption of the APCIP by the Federal Government, to November 2014 when the master plan 2014 was agreed by the Federal Government. The APCIP relies on owners and operators of critical infrastructure creating resilient institutions as a precondition of availability of vital resources, using standard approaches to risk management, business continuity and security management which include understanding the risks in their area of operation. In the APCIP implementation plan there are seven fields of actions and 31 actions. The structure is influenced by the European Programme for Critical Infrastructure (EPCIP) but it is stated to be independent of the European programme in its content. 400 private institutions are involved in the process, 100 of which are considered critical national Infrastructure.

Cyber Risks

Cyber Risks form part of the overall risk assessment process. Under the APCIP enterprises operating critical infrastructure are encouraged to implement comprehensive cyber security architectures. These are outlined at a high level in the Austrian Cyber Security Strategy which is a comprehensive document based on international best practice. A Risk Assessment Matrix has been drawn up using a qualitative process. This aspect has to be further developed. Ministry of the Interior and Defence are the lead agencies in this regard with cognisance of the NIS Directive being taken into account for implementation. Figure 7.2 shows the Cyber Risk matrix.

Figure 7.2. Austria's Cyber Risk Matrix 2011



Source: Federal Chancellery of the Republic of Austria (2013), Austrian Cyber Security Strategy.

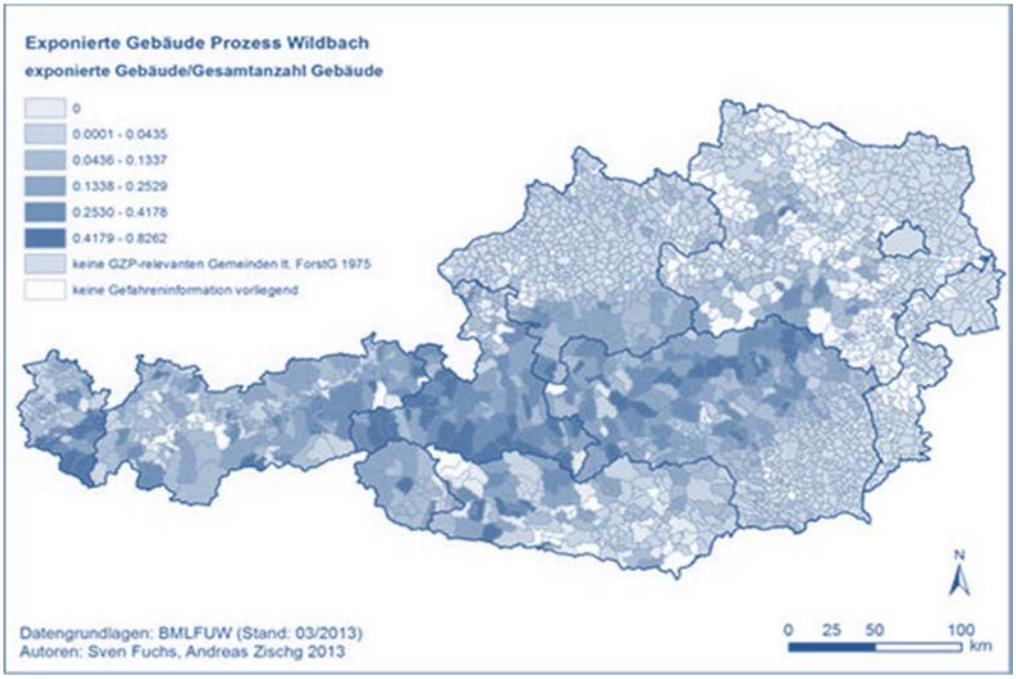
One issue is the extent to which the Austrian NRA should strive to add value to this segmented approach, above the value of setting out a broadly comparable methodology for risk assessment; recognised aims of an integrated National Risk Assessment are:

- The promotion of cross-departmental collaboration and collaboration between the public, private, academic/scientific, community and voluntary sectors in understanding cross-cutting risks (i.e., those that touch a wide range of departmental and sectional interests).
- Collaboration also with neighbouring countries (for example Austria – together with Bavaria – leads work under the EU's strategy for the Alps (EUSALP AG 8) to improve risk management and manage climate change, including prevention of major natural risks).
- The pooling and targeting of scientific expertise and understanding through research of the risks and measurement of their impacts, to assist in making provision for their mitigation, at national but also at sub-national level and in the main infrastructure sectors, who participate voluntarily as part of their responsibility to be resilient institutions.
- Development of capabilities designed to anticipate and respond to incidents that are beyond the capacity of sub-national bodies.

Nine of the 15 risks had been analysed by the time of the first report to Ministers in 2014, so clearly there is little to report at this early stage on the prospects for realising these aims. But already some benefits were being felt from the process of carrying out

integrated cross-sector risk analysis. There is already extensive risk mapping in Austria for the main recurrent kinds of natural or man-made hazard (Figure 7.3).

Figure 7.3. Mapping the risk of mountain torrents in Austria



Source: Presentation of the Office for Security Policy Federal Ministry of the Interior on National Risk Assessment in Austria.

Transparency and accountability

The GERIAN project has been an open process, with the study of options for an Austrian NRA, conducted by the Austrian Institute for Technology (AIT), being published and the outcome – in terms of the process – being well enough known to those with an interest. Overall responsibility for co-ordinating this process lies with the Federal Ministry of the Interior, as the lead authority in Austria for co-ordination of civil protection and disaster management approaches.

Multi-level governance and multi-actor participation

The Austrian general approach is that risk analysis is not the responsibility of a single government authority but a horizontal cross-cutting area, dealt with by different bodies across different levels of administration, at national, regional and local level.

At national level there is a number of Ministries with lead responsibilities for the NaTRAn for core issues, and these maintain policy units with responsibility to carry out security policy threat (or risk) assessments, and to produce policy papers setting out the resulting policy aims and implementation plans. An example is the responsibility for national cyber security which rests with the Ministry of the Interior and is establishing a cyber-security centre which will issue an annual report on the threats. The most notable body dealing with protection against natural hazards is the Federal Ministry of Agriculture, Forestry, Environment and Water Management, which maintains hazard and risk maps for rivers as well as risk management plans pursuant to the EU Flood Directive, including a food risk assessment. Taken together, these various departments could

produce a proliferation (possibly in the hundreds) of risk assessments using different methodologies. In the main the purpose of NaTRAn is to establish a broad level of consistency at the strategic level so that these sectoral risk assessments can contribute to the national picture.

Below the national level, provincial governments have the main responsibility under the constitution for disaster management, and are required to carry out hazard analysis and risk assessments at the regional level. Operators of critical infrastructure have developed their own methods of risk analysis to underpin their "tactical" responsibilities for infrastructure protection and resilience. In many cases, risk analysis has been done for many years, and the Austrian government has sought to build on the foundation provided by this historical record of risk analysis. This provides both benefits (in the existence of an extensive evidence base for national risk assessment) but also challenges (because of the differences in methodology).

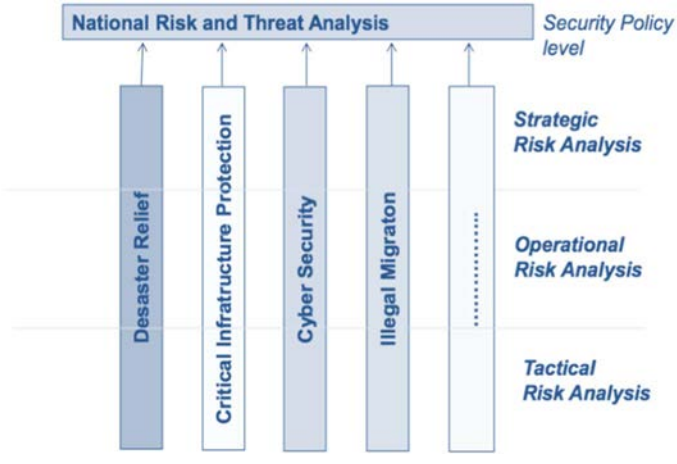
Risk analysis

The Austrian government reported in late 2015 that procedure and methodologies are primarily based on the European Commission guidelines, on ISO 31000 and on the national risk management standard ONR 49000. Following the AIT study, some practices of other European countries have been adapted for use in the Austrian NRA programme.

Scope

The scope of the National Risk and Threat Analysis (NaTRAn) is in principle very broad, as shown in Figure 7.4. The model shown here also illustrates that, while the NRA is a policy tool, the concept envisages risk analysis embracing not only the strategic level but also at the operational and tactical level (mainly: critical infrastructure sites under risk management by owners/operators).

Figure 7.4. GERIAN – Scope and Concept for a NaTRAn



Source: Presentation of the Office for Security Policy Federal Ministry of the Interior on national Risk Assessment in Austria.

Hazard identification

At this stage, the risk assessment is focused on the most common kinds of hazard set out in the first column on "Disaster Relief". "Multi-risks" are not considered. Table 7.2

lists the 15 scenarios within the disaster relief category, which are intended to be the main focus for a first NaTRAn.

Table 7.2. 15 scenarios for the initial NRA

Scenario Number	Scenario Title
1	Floods all over Austria
2	Floods affecting primarily western Austria
3	Winter storm (nationwide)
4	Storm (western Austria)
5	Mesoscale convectional systems (locally in several provinces)
6	Heat wave
7	Earthquake in eastern Austria
8	Earthquake in western Austria
9	Earthquake in southern Austria
10	Serious road accident
11	Industrial accident
12	Supply disruptions (large-scale electricity outage) (48 hours)
13	Pandemic
14	Accident in a nuclear power plant
15	Terrorist attack

Source: presentation of the Office for Security Policy Federal Ministry of the Interior on national Risk Assessment in Austria.

Impact analysis

According to the Austrian government's report from late 2015, the Austrian NRA will use a five-point scale for measuring impact. The impact categories are: human impacts (deaths and injuries); economic damage; environmental damage and political/social concerns.

When scoring overall impact, weighting is given to the impact category that scores the highest so that an event which caused very significant economic damage, but very little human or environmental harm, would be weighted towards the economic score. There is at present no separate presentation of risk by category of impact.

Likelihood and plausibility analysis

Likelihood is measured on a five point stepped scale, with the highest likelihood being a one in a year chance of happening, and the lowest being less than one in three hundred chance. Austria has not adopted the approach of assessing likelihood over a forward-looking five year period.

Risk evaluation, monitoring and re-evaluation

The reliability of the knowledge and data, and the extent of consensus, whether on the scenario, the impact, or the probability are assessed on a three-point scale (low; medium;

high) to inform the risk evaluation phase, so that those charged with determining the tolerability of the risk know how confident the analysis of risk is. Confidence in the nine risks analysed in the first risk matrix is considered to be medium to high, with a high degree of consensus in the assessment and knowledge of the risks being medium to high.

The purpose of the risk evaluation phase is to consider explicitly whether the risks are tolerable (which might be because it is objectively low, or because existing controls are thought to be adequate, or because the reduction of the risks to a more tolerable level would involve expense out of proportion to the damage that might be caused) or need to be treated, either through structural measures or non-structural measures. Judgements are made about the extent of residual risk, and about "black swan" events where the potential harm is significant but the probability of the event is either very low or not known or knowable. In such cases, risks may be monitored or further research commissioned.

The NRA is likely to be reviewed on a three-year cycle, with more risks being brought in initially from the natural hazards list.

The inputs are largely quantitative and will be updated every 3 years with the next update expected in 2018. In order to identify the risks a number of processes are carried out, e.g., the identification of vulnerabilities and the creation and discussion of different scenarios e.g., what and how. The thought process in respect of time is innovative and includes (the life time of a person) as a basic baseline. Risk owners are continuously identified. For instance the department of Health took risk ownership for heatwaves and held a workshop to further analyse the risk for the heatwave scenario in a mainly qualitative manner. This is an ongoing process and needs to be further developed in practical terms. The process itself is well on the way in view of the fact that identification and setting out of scenarios lead to studies which identify root causes of risk and therefore mitigating measures which may be applied. A mitigation measure – the national heat protection plan – is currently developed by a working group. Furthermore in this regard the Climate Change Adaptation Strategy was reviewed in 2016.

NRA Excursions

There are no multi-risks scenarios examined, but Austria has extensive mapping of the most common hazards and this forms the basis for much of the work on the NRA.

Communicating the results of a National Risk Assessment

Using the National Risk Assessment to raise awareness about risks

The risks that featured in Austria's first NRA are very well known to the Austrian people and there is plenty of information and data to inform local emergency planning including extensive mapping. An NRA will reinforce but not substitute for this existing body of information.

Main lessons learnt and policy outcomes

Lessons learnt

It is early days for the Austrian NRA to be learning lessons. The work that has been done so far bears out an impression that has underpinned work on the national crisis and disaster management system for a number of years (it was originally adopted in 1986 and revised by the federal government in 2004) that the country's risk portfolio was getting

more complicated: hazards more frequent and intensive; risks of man-made accidents more pronounced as volumes increase; and risks of disruption of critical infrastructure – in particular long power outages – offering a prospect of cascading or secondary effects that make the hazards more unpredictable; and the cross-boundary risks of radiological leakage from nuclear power plants, and of international terrorism. There is much single issue or partial risk assessment work that provides detailed evidence of this including a very detailed historical database. The Government has made the deliberate decision to use this information and data to construct a NRA rather than super-impose an NRA created from scratch according to the methodology it has created through GERIAN; and this is probably correct given that the capability and capacity building function is some way off being put in place.

Benefits

Notwithstanding the short time since the NRA was launched, there have been some early benefits; examples are:

- Using the government's soft convening power to bring together cross-disciplinary science and policy expertise to bear on issues of risk: providing in one case an inventory of scientific work that will yield benefits in considering the cross-disciplinary issues.
- The identification of risks hitherto underestimated in existing risk analysis (an example given is the risk to health of heat waves affecting the whole or major parts of the country) which appear not to have previously gained attention and now being addressed stronger in Austria.

The emphasis in the national security strategy on a risk based approach indicates that a risk management culture might be adopted by all levels of government and not just those which have a statutory duty to understand the risks to which their areas of responsibility are prone.

Limitations

There is a risk that the NaTRAn structure (Figure 7.4) may itself result in a 'stove-piped' approach to national risk assessment, which means that some of the benefits of an "all-hazards approach" – in particular a more cross-cutting approach to capability building - may be hard to secure. Less importantly – since no country has yet managed to used NRA for financial planning - there is at this stage no prospect of the NRA being used for budgetary planning purposes although there is a reasonable prospect that the priorities eventually decided upon by government will in time be reflected in budgetary priorities.

Notes

1. Austria has adopted the approach not to set-up a comprehensive "National Resilience Strategy" but to achieve the strategic goal of a "resilient State and society" in a number of sub-programmes (e.g., disaster relief, critical infrastructure protection, cyber security)

2. Decision 1313/2013/EU dated December 2013 – Article 6

References

Federal Chancellery of the Republic of Austria (2013b), Security in a new decade – Shaping security Austrian Security Strategy, Vienna.

Federal Chancellery of the Republic of Austria (2013a), Austrian Cyber Security Strategy, Vienna.

Presentation from the Federal Ministry of the Interior, Office for Security Policy, July 2016, National Risk Assessment in Austria APCIP, Cyber Risks.

Further reading

Stefan Schauer Brigitte Palensky Martin Latzenhofer Martin Stierle 2015, GeRBA Gesamtstaatliche Risiko- und Bedrohungsanalyse Studie im Rahmen des KIRAS-Forschungsprogrammes

Presentation from Andreas Pichler, on Progress in Natural Hazard Risk Reduction in Austria BMLFUW.

Chapter 8. CANADA

The Canadian All Hazards Risk Assessment (AHRA) has been developed as a result of the government's acknowledgement that there is an increase in natural and man-made threats and lessons learnt from domestic and international events which could also affect developed nations such as Canada. This chapter discusses the approach to emergency management in Canada and the governance framework in the risk assessment process which revolves around the concept of an all hazards approach with the objective of assessing and viewing risks in a standardised approach using a common set of principles and steps. While the AHRA methodology is published, transparency and accountability does not extend to full publication of the identified risk profile due to national security concerns. The introduction of legislation dictates specific roles and responsibilities to a lead ministry and specific ministries with responsibility for their own sector. This is discussed in the chapter as a core element for a standardised risk assessment methodology leading to effective multi-level governance and multi-actor participation.

Key Words: All Hazards Risk Assessment; Best practice; Governance framework; Legislation; Lessons learnt; Multi-actor participation; Risk scenarios.

Introduction

Canada's rationale for developing an All Hazards Risk Assessment (AHRA) methodology stems from the realisation and acknowledgement of the existence worldwide of a range of natural, human borne infection and man-made threats. The Government of Canada have acknowledged that these events are happening with increasing frequency and complexity. This complexity and frequency stem from climate change, increased terrorist threats and the interconnectedness and interdependencies as a result of globalisation and natural and political forces.

Risk such as pandemics, severe acute respiratory syndrome (SARS), earthquakes in Japan and Haiti, and terrorism are examples of events discussed that can also affect developed nations such as Canada. Threats such as floods, hurricanes, cyber-attacks and forms of ideological radicalisation need ongoing review by the Government of Canada in collaboration with the provinces and territories. Lessons have been learnt from such events and international best practice has been introduced in the form of an effective all hazards approach to risk management. The Government and its partner organisations have introduced a methodology and best practice in the form of legislation, regulations, policies and guidelines to address risk and assign risk responsibilities.

The most important piece of legislation from this perspective is the 2007 Emergency Management Act (EMA), which establishes the federal role in emergency management agencies and dictates specific roles and responsibilities of the Minister of Public Safety as well as those of all Ministers in the Canadian Government. This 2007 Act has been cited as "the overarching legislative umbrella in emergency management". The Act identifies the Ministry of Public Safety as the lead government ministry and mandates this ministry to provide leadership and guidance to federal level government institutions. This includes the preparation, maintenance and testing of emergency management plans. Results of this mandate include a Federal Policy for Emergency Management (FPEM) and an associated set of tools which include a set of guidance documents to assist the process. The development of these guides and the implementation of an All Hazards Risk Assessment Methodology are mandated to Public Safety Canada, a Governmental Organisation which was created in 2003 to ensure co-ordination across all federal departments and agencies responsible for national security and the safety of Canadians and all those who live in Canada. Public Safety Canada works with five agencies and three review bodies, united in a single portfolio and all reporting to the same Minister. In this case the Minister of Public Safety and Emergency Preparedness.

The organisation works with other levels of government, first responders, community groups, the private sector and other nations on national security, border strategies, countering crime and emergency management issues and other safety and security initiatives, such as the National Information Exchange Model. Its mandate is to ensure the government approach to Canada's safety is highly organised and prepared to confront threats to national security. Public Safety uses an integrated approach to emergency management, law enforcement, corrections, crime prevention and border security.

The approach to Emergency Management in Canada

The classic international best practice paradigm approach of prevention, mitigation, preparedness, response and recovery has been deployed with a co-ordinated multi agency

risk assessment process across all ministries and agencies in Canada. The stated objectives of this approach is premised on the assumption that the risks are co-owned and co-managed with the intention that this methodology will produce a whole of government risk picture to lend support in emergency management across all federal government institutions and to ensure that interdependencies are recorded and managed. This methodology is meant to feed into the potential for prioritisation of funding in the high risk areas and the creation of "a community of practice" or forums to share good practice, assist in the development of lessons learnt and increased resilience.

The AHRA initiative incorporates expertise from a wide range of federal government institutions and applies an all hazards approach. It is a comprehensive and integrated means for assessing the impact and likelihood of both malicious and non-malicious hazards and threats that Canada could face over a five year period. By assessing the risks associated with all hazards in an integrated way, efforts may be broadly effective in reducing the vulnerability of people, property, the environment and the economy.

Governance framework

Public Safety Canada (PS) is the lead co-ordinating department for emergency management in Canada and has the legislated responsibility under the Emergency Management Act, 2007, to perform an all hazards approach to risk assessment.

All safety and security departments are part of an Interdepartmental Risk Assessment Working Group (IRAWG) which meets regularly to discuss the all hazards risk assessment process and related matters. Public safety Canada acts as a co-ordinator during the scenario development process, working to facilitate scenario development between members of relevant departments.

The risk assessment process revolves around the concept of all hazards with the objective of assessing and viewing risks in a standardised fashion using a common set of principles and steps. This ensures consistency at a national and/or federal level. The process dictates that the hazards are considered at the beginning of each new cycle with this annual assessment focussing on the most probable and consequential risks. The idea is that a consolidated picture will be formulated over a number of iterations of the process over several cycles with ongoing input by federal experts in the particular risk scenarios. By assessing the risks associated with all hazards in this integrated way it is considered that this will be broadly effective in reducing the vulnerability of people, property, the environment and the economy.

In specific terms the objective of this approach is important as it enables federal government institutions to perform an all hazards approach consistently and efficiently as part of their risk management responsibilities under the Emergency Management Act and other relevant legislation and policies.

It addresses the interconnected nature of Canada's risk environment provides a means to produce a collective judgment of risk assessments currently being carried out by different federal government institutions and provides a whole-of-government picture to inform future actions and initiatives.

It can be seen to support the relative ordering of risk events based on their ratings at a federal level, while enhancing decision-making processes within the Government of Canada. It provides an overall risk picture to decision-makers and provides them with a

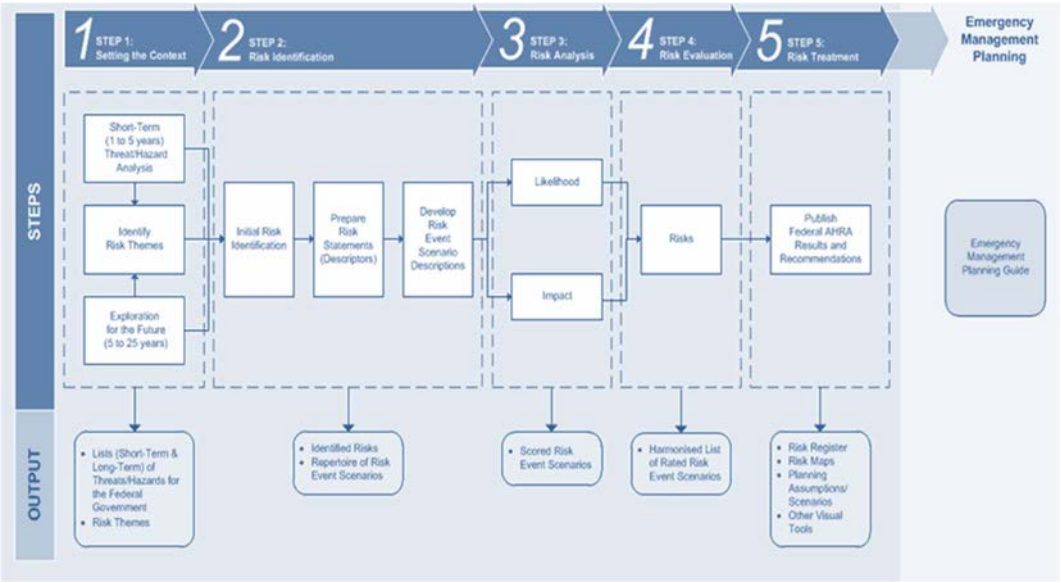
decision making tool to decide how to use the results in prioritising and capturing those risks that are significant in a federal context.

The All Hazards Risk Assessment (AHRA) is primarily used for the emergency management planning functions for departments that own specific risks. Canada is currently undertaking implementing a National Mitigation Program, tying this very closely to the AHRA. In addition to Canada's National Platform for Disaster Risk Reduction (DRR), the National Mitigation Program, although in its developmental stage, aims to provide funding to provinces and local level communities to assist them with mitigation efforts. These include specific physical infrastructure, training, or emergency response capabilities more generally. The Program requires funding to be tied to risk assessment, linking the local and provincial levels to the AHRA.

Risk Profile

To date some 22 risk scenarios have been identified. The federal AHRA process is based on a methodology with ISO 31000 risk management principles in mind and is based on a standard set of guidelines involving the following steps of risk context, identification analysis evaluation and treatment. The process employs a scenario based risk assessment approach and is linked to the overall emergency management approach outlined in Figure 8.1.

Figure 8.1. AHRA Process and Linkage to EM Planning



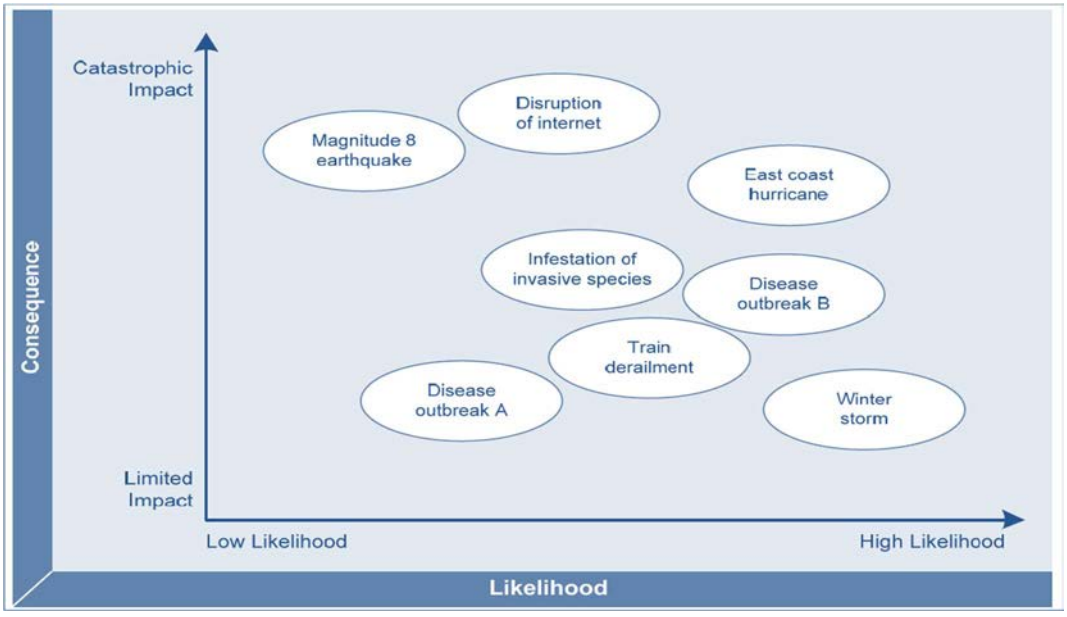
Source: Building a safe and Resilient Canada, All Hazards Risk Assessment Methodology Guidelines 2012–2013, p. 5, available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ll-hzrds-ssssmnt/ll-hzrds-ssssmnt-eng.pdf.

The AHRA process is meant to create a multi-dimensional, high-level view of risks faced by Canadians, while bringing diverse risks from various sources into the same high-level view, as Shown at Figure 8.2.

The outputs from the AHRA process should provide decision-makers with an improved understanding of the relevant risks. These are seen as a combination of the likelihood and the consequence of a specified hazard or threat being realised. Generally,

risks translate into events or circumstances that, if they materialise, could negatively affect Canada and Canadians.

Figure 8.2. Example of Diverse Risk Event Scenarios Displayed on a Likelihood-Consequence Graph



Source: Building a safe and Resilient Canada, All Hazards Risk Assessment Methodology Guidelines 2012–2013, p. 6, available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ll-hzrds-ssssmnt/ll-hzrds-ssssmnt-eng.pdf.

The hazard risk domain is covered by the federal AHRA methodology. However, the operational risk domain (e.g., day-to-day issues confronting an institution) is not, although these aspects may be considered and factored in setting the context prior to identifying risks and assigning impact ratings during Risk Analysis.

As Canada covers a large land mass area of 9.985 million km², a localised approach to events is considered appropriate. Examples of this process have been given in respect to flooding where this is most appropriate. In the national context terrorism (cyber) and pandemics are also high areas of concern. Each domain is responsible for their risk assessment which feeds into the AHRA. Health is a highly established domain, working collectively on risk assessment across the federal, provincial and local community. To this end, although pandemic still rates very highly in terms of potential impacts and likelihood, there are extensive mitigation policies and processes in place.

Transparency and accountability

The AHRA methodology is published publicly on Public Safety's website and results and methodology are reviewed by the Interdepartmental Risk Assessment Working Group (IRAWG). Results of the AHRA are presented to a committee of senior officials through a presentation and final report. Discussions and results are tracked in a risk scoring tool and through meeting minutes.

At present, the results of the AHRA are classified due to the presence of national security information. It is however distributed to senior officials responsible for emergency management at the federal level. Currently, there is no public distribution of results. To this effect, Canada is considering adopting a similar policy to that of the United Kingdom. Where two versions of AHRAs are produced, one public and one sanitised. However, any changes to the current AHRA programme would warrant further discussion as a considerable amount of time and resources were invested to establish an initiative which includes the national security community and an all hazards approach to risk assessment. Initially, Public Safety Canada considered not taking an all hazards approach, thereby only focusing on natural hazards and the health sector. International best practice has seen an increasing role for the security sector in a strategy that includes all the stakeholders in a holistic approach. The difficulties with the security sector involvement appear to have been solved and they now play an active role in the process. In view of this additional dimension there is caution in respect to making the overall results public at this time.

Use of expert opinion & Control for Bias

The IRAWG is used to vet results before they are presented to the committee of senior officials. The idea is that a consolidated picture will be formulated over a number of iterations of the process over several cycles with ongoing input by federal experts in the particular risk scenarios. If a person or government agency disagrees with a result, discussions can occur around why a scenario received such a score. Scores can be adjusted if new or relevant information necessitates.

Multi-level governance and multi-actor participation

Public Safety Canada is the lead co-ordinating department for emergency management in Canada and has legislated responsibility under the 2007 Emergency Management Act which establishes the federal role in emergency management, and the role and responsibilities of the Minister of Public Safety as well as those of all Ministers to perform an all hazards approach to risk assessment. All safety and security departments are part of an Interdepartmental Risk Assessment Working Group (IRAWG) which meets regularly according to current developments of the AHRA and to discuss AHRA related matters. Once one cycle has been completed and a new cycle is about to follow, a meeting will be initiated with that community to talk about what risk they will assess the next. On an annual basis there are 6-8 meetings held. Public Safety acts as a co-ordinator during the scenario development process, working to facilitate scenario development between members of relevant departments. 25 to 30 institutions participate in the AHRA exercise.

Risk analysis

Risk scenarios

Canada uses detailed scenarios which are collaboratively developed between Public Safety Canada and other agencies that can be expected to play a role in an emergency response. The scenarios chosen are most plausible scenarios. The assessment of those scenarios is based on events that have happened and are built on historical data. A more detailed scenario was chosen, versus a scenario vignette (description), to allow a level of detail which would enable departments to understand the scale, complexities and features of an incident. Because of Canada's highly varied geographical and cultural conditions, a

less detailed scenario could not apply to the specific conditions which may be expected in different locations.

Uncertainties

Confidence ratings are assessed for each category. A higher degree of confidence indicates evidence was provided to back up a response. Lesser amounts of evidence produce a less confident answer. When results are demonstrated in a risk picture, the central point is surrounded by an ellipse which demonstrates the level of confidence and an area in which the risk is likely to lie. In scenario development a risk event scenario template is available in order to scope out the scenarios in a detailed way. This template also seeks to limit assumptions and unknowns which may interfere with the risk scoring process.

Time horizon

A 5-year time horizon was chosen because it provides sufficient time for planning purposes and also allows for some foresight into changes in hazards and threats. Mitigation measures can also be established within a 5 year timeframe. The considered time-frame from which events are considered in the AHRA process is therefore short-term (within the next 5 years) threats/hazards. Long-term threats/hazards (that span 5 – 25 years into the future) are not currently considered in the AHRA.

Risk monitoring and re-evaluation

The AHRA process is iterative in nature in recognition of the fact that the array of risks facing Canada as well as the level of knowledge about these risks is constantly changing. The assessment of risks of a federal interest will be done on an annual basis, starting officially in June every year with the identification of priority threats and hazards.

Communicating the results of National Risk Assessment

Internal and external communication

While there is currently no public distribution of results of the risk assessment process or the prevailing risks this appears to be up for consideration. The authorities have examined best practice in other jurisdictions such as the UK in the context of the all hazards approach. In addition, the AHRA methodology is published on Public Safety's website.[1]

Public awareness strategies

Public Safety's website contains an array of advice to the public which include an outline of the rationale to be prepared for both natural and other emergencies and what to do before during and after an emergency. These include a list of ten natural hazards and other hazards including bomb threats chemical, nuclear emergencies and biological incidents. This is broken down into 13 regions in which the hazards are identified by individual region.

Accessible at: http://www.getprepared.gc.ca/cnt/hzd/index-en.aspx

Tools for interpreting risk analysis

Much work has been completed to streamline Canada's Risk Assessment Process. Documents and guides have been developed by Public Safety Canada, in close partnership with Defence Research and Development Canada - Centre for Security Science, as part of the Federal All Hazards Risk Assessment initiative endorsed by the Assistant Deputy Minister Emergency Management Committee in October 2009. These documents contain tools and detailed methodologies where the primary audience are the federal regions who are mandated by legislation to carry out risk assessments. These tools include SWOT and PESTLE Analysis, Risk Taxonomy Chart, Risk Event Scenario Description Template, Rating Example Index outlining scenarios which affect Canada's reputation and influence and an Economic Category Assessment Tool. The objective of these templates/tools is to provide consistency across regional boundaries and streamline the process.

Main lessons learnt and policy outcomes

Lessons learnt

In bringing relevant departments and colleagues together to discuss risk, and putting risk on the agenda for departments, this process has been successful in building relationships. Similar to other processes however more work is needed. This includes the development of capability based planning and the AHRA's incorporation into mitigation planning. The original intent of the AHRA was for emergency management planning. An important lesson highlighted in the process was the significance of educating and building understanding of the importance of risk assessment. As the process took hold, the importance of the AHRA became more apparent. Particularity to inform exercise planning and training and most importantly the mitigation process. It also informed discussions on preparedness response and the concept of resiliency.

Next steps

To this end, the future AHRA cycle will explore new areas, including capabilities assessment focusing on detailed scenarios. These may be broken down to time periods to assess what resources, policies or programmes are in place for the future. The next steps in the AHRA will be likely to explore how to work with sub-national emergency management organisations. Drawing on provincial level expertise and exploring how to integrate provincial level risk assessments with a mainly federal level AHRA In addition to future work on capabilities assessment and sub-national inclusion to AHRA, further work may need to be done on how scenarios are selected.

Policy Outcomes

The All Hazards Risk Assessment methodology and process are the result of a pilot on the all hazards risk assessment initiative successfully completed in October 2011. There was an expectation that as the process evolved, best practices would be developed. In addition, collaboration with international organisations such as the OECD, the World Economic Forum and the International Council on Risk Governance would bring clarity and lessons learnt to the process. In addition, ISO accreditation was obtained as the federal AHRA process is based on a methodology as identified in ISO 31000, "Risk Management – Principles and Guidelines". The analysis of the prevailing situation in world events will need to be constantly monitored in order that these inevitable new

trends can be assessed. Partnership with the above mentioned international organisations can assist to predict the likelihood of this happening.

References

Public Safety Canada (2013), Building a safe and Resilient Canada All Hazards Risk Assessment Methodology Guidelines 2011-2012. Available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ll-hzrds-ssssmnt/ll-hzrds-ssssmnt-eng.pdf

Further reading

ISO 31000:2009, Risk management – Principles and guidelines and ISO Guide 73:2009, Risk management – Vocabulary. Available at: https://www.iso.org/iso-31000-risk-management.html

Chapter 9. DENMARK

The Danish Emergency Management Agency (DEMA), as the lead agency, has the responsibility to develop the risk assessment process (National Risk Profile 2013) in Denmark. The NRP is a broad perspective on the most serious natural and man-made risks affecting Denmark at this time. This chapter discusses the governance framework and organisational structure for crisis management including the role of DEMA in developing the NRP. Transparency and accountability is provided by the publication of a suite of guidance documents to assist in this process and consultation has taken place with international agencies and neighbouring countries. In respect to hazard identification and impact analysis the NRP is based on historical events that have affected Denmark in the past and therefore considered likely to occur in the future. Communication of the results of the NRP is a core element of the strategy as public and private sectors are in a position to develop their own response as a result of the published content.

Key Words: All hazards approach; Consultation; Communication; Governance; Guidance; Judgement; Multi-actor participation; Risk awareness.

Introduction

The Danish Emergency Management Agency (DEMA) published a first "National Risk Profile" in 20131. This NRP was drawn up partly on DEMA's own initiative, and partly in response to the European Council's conclusions in April 2011 on 'Further Developing Risk Assessment for Disaster Management within the European Union'. It takes the form of a list of ten of the most serious natural and man-made risks of emergency, according to DEMA's judgement, and a narrative description for each of the characteristics, possible consequences, past occurrences, and possible future trends. A reserve list of another twenty risks is included but the risks are not described in any detail. The published NRP contains a chapter showing in "radar" form the results of DEMA's analysis of the seriousness of the consequences of each type of incident relative to each other. Ambitions for this first National Risk Profile have been deliberately constrained:

- The NRP provides a quarry of information useful for emergency planning and capability building by responsible authorities in the public sector and also for private sector organisations interested in building business continuity and resilience; but does not itself drive investment in resilience capabilities by these authorities.
- The NRP responds to initiatives to improve the coherence and consistency of risk assessment practice among EU Member States, by adopting some features comparable with other countries (in particular Sweden, Norway, the Netherlands and UK) to provide a shortlist of risks of sufficient severity to entail involvement by the national government in emergency response; but prefers an "NRA-lite" approach to methodology, in particular: by not taking into account assessments of the likelihood or plausibility of risks; by using judgement rather than systematic quantification in estimating degrees of impact of the types of incident assessed; by focusing on history and trends and not developing scenarios; and in the use of terminology.
- The NRP is – as its title suggests - a significant piece of risk communication, going beyond some of the risk registers produced by other countries in the detailed examples and analysis of future trends for each of the top ten risks; but no attempt is being made at this stage to obtain feedback from the NRP's intended users to see whether it is meeting their needs on a voluntary basis or not.

The National Risk Profile forms part of a suite of guidance provided by DEMA to other parts of the Danish government on crisis management and preparedness planning in keeping with its remit to improve emergency preparedness in Denmark. For example, a companion piece to the NRP is on-line guidance on techniques for risk and vulnerability analysis which, together with a scenario bank, provides responsible authorities and private sector entities with the means of conducting more systematic and detailed risk assessments in their areas of responsibility.

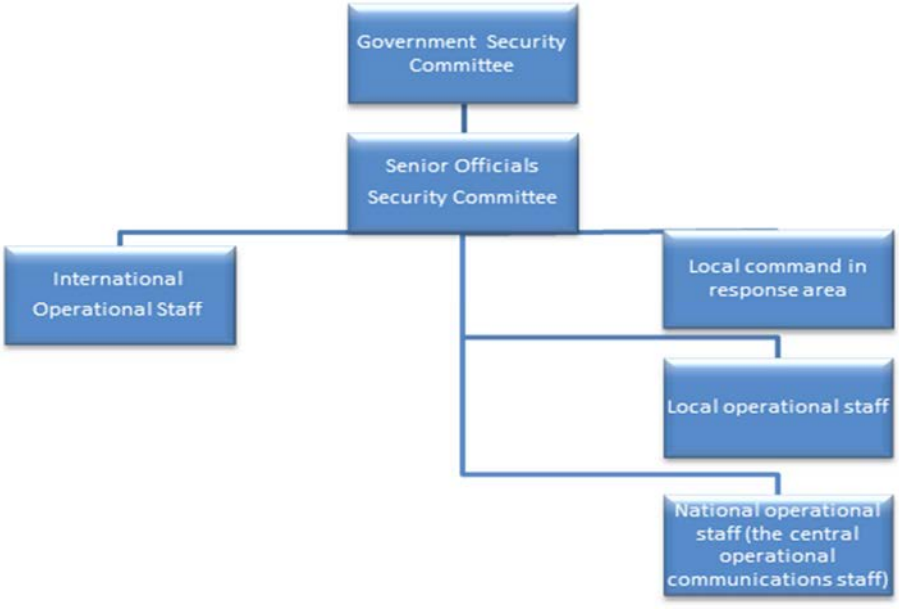
DEMA has been consulting other European Union Member States (EUMS) on their NRA work and will be reviewing the NRP over the coming year with a view to making changes that will increase its utility as an authoritative source of information and risk data for building resilience in Denmark.

Governance framework

DEMA forms part of the Danish national crisis management system which is described in a National Crisis Management Plan (NCMP) drawn up under an Emergency Management Act. This places the responsibility for crisis management and preparedness, and for cooperation with other authorities, on lead departments and agencies. It emphasises the principle of subsidiarity: emergency management and crisis management should be handled at the local level, as close as possible to the crisis. According to emergency management legislation, the NCMP itself is produced by the Minister of Defence, supported by a Crisis Management Group which includes the Prime Minister's Office and ministries of Defence, Justice, Health, Foreign Affairs as well as a number of agencies including DEMA. The Crisis Management Group must plan and conduct a national exercise to test the NCMP but has no role in the event of a crisis.

The organisational structure for crisis management, under the authority of the Government Security Committee, is shown in Figure 9.1. The National Operational Staff is a virtual organisation drawn from the national police, DEMA, Defence Command Denmark, the Defence Intelligence Service, the Security Intelligence Service, the Danish Health and Medicines Authority and the Ministry of Foreign Affairs, which are the core members. A similarly constituted International Operational Staff exists for major incidents that affect the safety or security of Danish citizens abroad.

Figure 9.1. Denmark's national crisis management system



Source: Adapted from: The Danish Emergency Management Agency (DEMA) 2015, Crisis Management in Denmark.

DEMA is an authority under the Ministry of Defence with a remit to improve preparedness for major accidents and disasters in Denmark. To that end it carries out a number of operational and regulatory tasks related to emergency response, and undertakes a supporting role in assisting responsible public sector authorities and private sector companies to develop their own crisis management capabilities and preparedness. Under Danish Emergency Management legislation, DEMA receives preparedness plans from all

state authorities with a view to providing feedback and advice and spreading consistency and best practice. DEMA has no directive powers in this but must operate by influencing and informing the responsible authorities; and its resources have been reduced through budget cuts in recent years.

First produced in 2013, the National Risk Profile (NRP) is not supported by a specific legal framework but is one of the instruments by which DEMA carries out its remit to improve preparedness and promote consistency within the national crisis management system. The NRP also responds to the European Council's 2011 decision encouraging the development of national risk assessment for disaster management within the European Union.

Aims and Objectives

According to its preamble, the NRP provides an overview of the most serious natural and man-made risks, with the objective of "contributing to preparedness planning assumptions among organisations within different sectors, across sectors, and at the central level of the national crisis management system". The intention is that the NRP be used by these organisations to support their own risk and vulnerability analysis, capacity analysis and planning, and preparation of contingency plans and related exercises. The NRP forms part of a suite of guidance available on the DEMA web-site including:

- **Crisis management in Denmark** – a general and unclassified introduction to the tasks, organisational structure and distribution of responsibilities within the Danish national crisis management system.
- **Comprehensive Preparedness Planning** – a guide to emergency planning for "all entities that play a part in Danish society's collective emergency preparedness" including how each entity can develop emergency planning assumptions on the most critical functions needing to be protected, and the most serious threats to those functions.
- **Risk and Vulnerability Analysis** – a user guide originally published in 2005, following a 2004 study (Denmark's National Vulnerability Evaluation), which recommended that a generally applicable Risk and Vulnerability Analysis (RVA)[2] model should be developed for use by government authorities in preparedness planning.

The NRP has been designed to complement these elements of guidance. In particular, since the responsible public authorities have these other tools available to them to assist them in determining what investment to make in reducing the risks that affect their responsibilities, and since DEMA has no formal mandate to carry out central resilience capability or capacity planning even for the more serious cross-cutting risks, the NRP has been designed primarily as a risk communication tool. Within these parameters, however, DEMA is exploring the potential for development of the utility of the NRP as an instrument that can assist cross-cutting work to improve resilience to the most serious risks, for example:

- As a source of scenarios for national exercises to test the NCDMP (see above).
- To gain consensus or a common understanding of cross-cutting risks and their impacts across the sectors.
- To provide an evidence base enabling DEMA to target its resources, and in particular scientific resources, to the areas of risk that would most benefit.

- To promote a risk management culture among the public and private sector.

Definition of key terms

The use of formal risk assessment terminology by Danish public authorities varies:

- Risk and Vulnerability Analysis (RVA) – the original model drew inspiration from international risk management literature, and the 2006 version was produced following discussions with partners from the UK, Germany, Sweden, Norway and Finland. The RVA model attempts as a result to be systematic and rigorous, but also usable by people without prior knowledge of risk analysis techniques. Some key terms (for example risk and vulnerability analysis, threat, risk, probability and consequences, vulnerability) are defined in ways that are compatible with, but not identical to, those agreed in later years under ISO 3010. But the RVA model is not used in the NRP.
- National Risk Profile (NRP) – the NRP deliberately eschews the use of terminology proposed for national risk assessment in the European Commission Guidelines and in the international standards upon which these guidelines are based. In particular, the word "risk" is used in an everyday sense to mean the uncertain consequence of an event that impacts on things that are valued in Danish society; and no formal attempt is made to combine the consequence of the harmful events described in the NRP with the associated likelihood of their occurrence in accordance with the basic definition of risk proposed in ISO 30103.

The reason given for the difference in approach between the RVA guidance and the NRP is that DEMA did not wish the latter, at least in its first edition, to appear methodologically cumbersome, preferring to focus in easily readable terms on the consequences of emergencies than to speculate on the likelihood of their occurring. This is in keeping with difference in function of the two instruments.

Notwithstanding the deliberate avoidance of ISO 31000 technical definitions, the NRP contains a good deal of material that could be used to populate a risk assessment that meets the (RVA and) EC guidelines, should the Danish authorities choose to construct the profile in that way. Section 2 examines the ways in which the NRP varies from the emerging norm for national risk assessment; and section 3 speculates on the possibilities for future development of the NRP.

Transparency and accountability

A key element of accountability is that the NRP has to be formally endorsed by the Minister for Defence as the lead Minister for resilience, although there is no collective approval by Government Ministers in the Crisis Management Group. The Danish risk assessment process incorporates a number of practices in support of transparency:

- The issue of RVA guidance which, through voluntary for most (in fact all but a few) public sector organisations at national and sub-national level, and all private sector bodies making use of it, assists in establishing a consistent methodology for risk and vulnerability analysis.
- The RVA was drawn up with the aid of a focus group with representation from a number of agencies including the Danish Energy Authority and the National IT and Telecom Agency;

- The NRP though initiated and authored by DEMA is carried out in consultation with experts from government agencies with responsibilities for the different sectors, and other organisations, who provide both input and quality control.
- The NRP contains only open source information, following the recent tradition in Denmark of publishing information on societal vulnerabilities through the National Vulnerability Report issued by DEMA between 2005 and 2010, which had a similar purpose as the NRP which superseded it of promoting a preparedness culture in the public and private sector.

In addition to seeking input from and quality control by Danish experts, DEMA have also discussed their approach to the NRP in a number of international fora including the Nordic forum for risk assessment and strategic foresight, and the European Commission's expert meetings on risk assessment; and the NRP itself draws on material in similar reports in neighbouring countries, in particular the Norwegian, Swedish, Dutch and British National Risk Assessments of 2011 and 2012.

Multi-level governance and multi-actor participation

60 organisations had been consulted on the draft NRP in 2013, representing all levels of government and key infrastructure service providers. Participation by these organisations varied; some contributed substantial pieces of analysis, others much less. There was no involvement of stakeholders in the scientific/academic world.

Risk analysis

Work on the first NRP was conducted in five main phases:

1. DEMA drew a provisional list of some 30 "incident types", of which ten were to be included in detail in the first NRP, and a further twenty would be listed but not, at this stage, analysed in any detail; the issue of "multi-risks" (risks with cascading effects) was addressed at this stage.
2. DEMA drew up a set of criteria for down-selection of the ten incident types to be considered for inclusion in the first NRP.
3. DEMA drafted reports on each of the ten incident types selected, with a common structure that covered:
   - an introduction to the characteristics of each incident type, including possible causes
   - a description of possible consequences in case an incident of this type occurs
   - an account of examples of actual incidents that have previously happened in Denmark
   - an analysis of possible trends that may influence the risk associated with the incident type in the future.
4. DEMA consulted other parts of the Danish government at official/expert level on the draft; and
5. DEMA submitted the resulting draft NRP for sign-off by the Minister for Defence on behalf of the Government.

Scope

The 2013 NRP took an all-hazards approach, with both natural (extreme weather phenomena; infectious or contagious disease) and man-made (accidents; security threats) incident types being within scope of the assessment. Further criteria were that incidents should be unmanageable at a local administrative level alone but demand external emergency response assistance; and liable to manifest themselves within Denmark's borders. Exclusions include events like earthquakes that are unlikely to happen in or near Denmark. The NRP itself explains that it does not cover "risks of a more global, diffuse or long-term nature such as financial crises, international armed conflicts, proliferation of weapons of mass destruction, or scarcity of natural resources dues to population growth, urbanisation, climate change".

Hazard Identification

The NRP does not entail the identification of formal "risk owners", and the responsibility for identifying the incident types featured in the NRP – including multi-risks and multi-hazards - lay in the first instance with DEMA, who consulted responsible authorities on their initial choice of 30 incident types, and subsequent down-selection of ten. The 10 incident types shortlisted, and the remaining 20 types not shortlisted, are shown in Table 9.1.

Table 9.1. Selected incident types

Natural incidents shortlisted	
Extreme weather phenomena	*Serious contagious disease outbreaks*
1. Hurricanes, strong storms and storm surges 2. Heavy rain and cloudbursts	3. Pandemic influenza 4. Animal diseases and zoonosis
Man-made incidents shortlisted	
Accidents	*Security threats*
5. Transport accidents 6. Accidents with dangerous substances on land 7. Marine pollution incidents 8. Nuclear accidents	9. Terrorist acts 10. Cyber-attacks
Not shortlisted but may be included in updated versions of the NRP	
Natural incidents	*Man-made incidents*
• Heat waves • Hard winters • Blizzards and heavy snowfall • Sudden violent thawing with major floods • Meteorite impact in/near Denmark • Tsunami • Geomagnetic storm • Explosive volcanic eruption • Effusive volcanic eruption	• Accidental power outage • Breakdown of electronic payment systems • Pollution of drinking water • Supply failure due to strikes or blockades • Structural collapse of major buildings • Man-made fire in major buildings • Satellite crashing on Danish soil • Widespread civil disobedience, violent activism, vandalism, arson etc. • Armed clashes between criminal gangs • Act of war against Denmark

Source: Adapted from The Danish Emergency Management Agency (DEMA) 2013, National Risk Profile (NRP) 2013.

The main criteria for selection were related to the consequences of the incident types rather than the probability of their occurrence. Entry level criteria were that the consequences of incident types should be significant in terms of magnitude, geographical extent and/or duration of the harm done to:

- life, health and wellbeing of the population
- property and the economy
- the environment
- the availability of a range of critical societal functions.

Impact Analysis

Table 9.2. Checklist of possible consequences of incident types in the Danish NRP

Harm to life, health & well-being	*Harm to property & economy*	*Environmental harm*
• Dead	• Material damages	• Land pollution
• Injured	• Financial losses	• Water pollution
• Ill/infected/contaminated	• Loss of intellectual rights	• Harm to animals
• Anxiety/insecurity/fear	• Loss/destruction of cultural heritage	• Harm to plant life
• *Failure of or extreme pressure on the availability of critical societal functions*		
• Energy: Supply of electricity, natural gas, crude oil, fuel, etc.		
• Information and communication technology (ICT): Telephone, internet, information networks, data processing and transmission, navigation, satellite/radio/TV transmission, post and courier services, etc.		
• Transport: Carrying out, monitoring and controlling passenger and cargo transport (road, rail, air and sea), monitoring and controlling of infrastructure (bridges, tunnels, stations, airports, harbours), etc.		
• Water: Supply of drinking water and waste water disposal.		
• Food: Supply of food, supervision of food safety, monitoring and responding to contagious animal diseases and zoonosis		
• Finance: Money transmission and transfer services, banking and insurance, securities trading, etc.		
• Fire and rescue services, police duties, military assistance to civil authorities, etc.: Alarming and alerting, on-scene co-ordinating and technical incident command, cordoning off, firefighting, search and rescue (land/sea/air), evacuation (incl. reception, housing and catering), environmental pollution response, storm surge preparedness, snow-preparedness, public order enforcement, explosive ordnance disposal, control of production, storage and transport of hazardous materials (chemical, biological, radiological, nuclear, explosive) and response to incidents that do or may involve hazardous materials.		
• Health and social services: Pre-hospital services, hospitals, practising physicians, production and distribution of pharmaceuticals, supervisory systems, day-care and residential institutions, home care, etc.		
• Defence, intelligence and security services: Military defence and enforcement of sovereignty, counter- terrorism, counter-extremism, counter-espionage, personal protection, etc.		
• Exercise of authority (all levels): Crisis management capacity, maintenance of parliamentary, governs- mental, central administrative, judicial, municipal and regional authority.		

Source: Adapted from: The Danish Emergency Management Agency (DEMA) 2013, National Risk Profile (NRP) 2013.

The NRP is based on historical events that have affected Denmark in the past and which are therefore treated as illustrative of the risk in the future. For example, the assessment of the risks of hurricanes, strong storms and storm surges sets out a number of instances over the past century when Denmark has experienced such phenomena and no attempt is made to select a particular instance as the basis for a scenario on which to base

future planning. In this respect, the NRP approach does not go as far as other countries who similarly identify historical examples but then use these to construct a best case, worst case, or "reasonable worst case" scenario to form the basis for comparing risks and quantifying impacts, to aid prioritisation and capability building. The reasons for this difference in approach go back to the purpose for which the NRP was created, but DEMA recognise that emergency planners in responsible departments may need to base their planning assumptions and capability analysis on a scenario-based approach; the NRP accordingly refers them to the 2005 Model for Risk and Vulnerability Analysis, and associated Scenario Bank containing 22 examples of scenarios from 2006, and to other work on scenarios carried out by state, regional and local authorities and by companies responsible for critical infrastructure.

No numerical values or weighting were given to individual items on the list. Instead, these criteria were used in four ways as:

1. A checklist used by DEMA to make a qualitative judgement of which types of incident should appear in the "top 10" shortlist of risks in the first National Risk Profile.
2. A framework for a narrative description of the possible consequences of each of the ten types of incident in the body of the NRP, based partly on the examples of past occurrences given.
3. A framework for a narrative description of possible future trends and risk drivers.
4. The basis of a broad order comparison of the relative seriousness of the risks, based on a three-point scale (serious, very serious, critical) which applied to all four impact criteria.

Likelihood and Plausibility Analysis

Like many other NRA, the NRP aims to look forward 5 years but, unlike others, does not, (at this stage), attempt to put a value to the likelihood of the ten risks materialising.

Although the focus of the NRP is on the possible consequences of the 10 incident types selected for assessment, there are data from which a sense of the probability of their occurring can be derived: the narrative description outlines the numbers of occurrences and historical frequency of each type of incident, and the possible trends that might be expected to affect the future frequency as well as maximum impact of each.

For example, the description of the risk of pandemic influenza recalls that accounts of "violent and extensive outbreaks of flu-like illnesses go back to the 16th century and it is assessed that 3-4 pandemics have hitherto occurred per century". The assessment of possible trends suggests that advances in medical treatment may have lessened the health consequences of future pandemics, but that increased global mobility is likely to ensure that the risk of an outbreak will continue to feature prominently in the NRP. These assessments could be used to derive calculations of probability, at least to an order of magnitude, and the same could apply to floods and other natural disasters.

Risk evaluation, monitoring and re-evaluation

Chapter 3 of the NRP sets out a comparison of the relative impacts of each of the ten types of incident, in aggregated form (i.e., taking into account the Danish authorities' judgement across the full range of impacts, and then in disaggregated form (i.e., taking each type of impact – life/health/wellbeing; property/economy; environment; critical

societal functions – separately). A "radar" model is used to present these comparisons, using a three point scale of consequences (serious, very serious, and critical). On this basis, the incident types having the most serious consequences are: hurricanes/strong storms and storm surges; influenza pandemic; nuclear accidents (in neighbouring countries); cyber-attacks; and terrorist attacks.

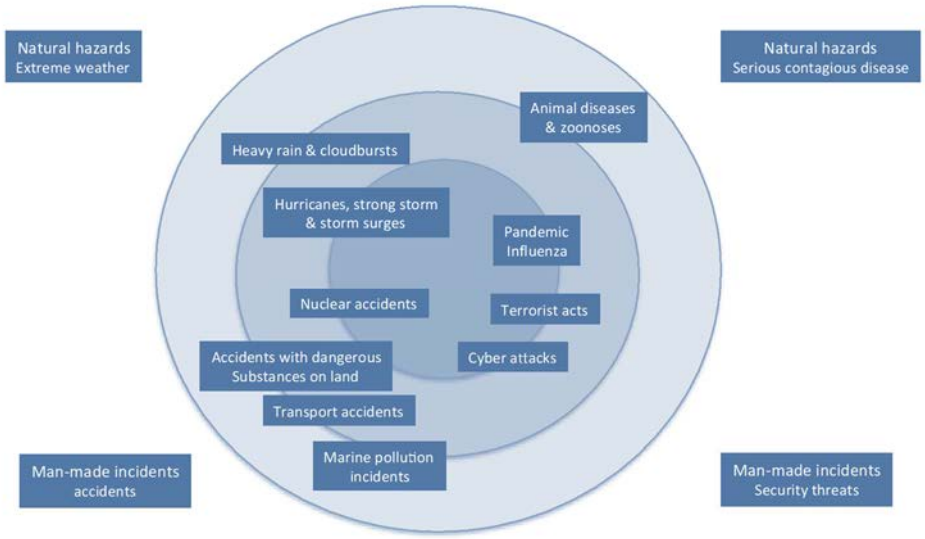
DEMA has consulted other EUMS on their NRA work, and participates in the European Commission's expert's meetings on national risk assessment. The NRP will be reviewed over the coming year with a view to making changes in methodology reflecting these consultations and the Danish Government's requirement for this kind of product. The intention is to make any necessary changes, and update the material including possibly the expansion of the initial list of 10 incident types to include some on the "reserve" list, with the next NRP due in 2016 and the following in 2019 or 2020.

Communicating the results of National Risk Assessment

Using the National Risk Profile to raise awareness about risks

The National Risk Profile is designed to be readable by organisations in the public and private sectors interested in improving their own preparedness for the kinds of incident described in it; and is published on-line for all to read, currently in Danish but in future in both Danish and English. There is at present no information available about the numbers who have read it or feedback on how useful they found it.

Figure 9.2. NRP – Overall consequence assessment



Note: Scale: Inner circle = critical consequences. Middle circle = very serious consequences. Outer circle = serious consequences.
Source: Adapted from: The Danish Emergency Management Agency (DEMA) 2013, National Risk Profile (NRP).

Tools for interpreting risk analysis

The published NRP contains a chapter showing in "radar" form the results of DEMA's analysis of the seriousness of the consequences of each type of incident relative

to each other above. There are five radar diagrams showing the relative scale of consequence in aggregated and disaggregated form; Figure 9.2 shows the first such diagram, illustrating the relative overall scale of consequences for the ten risks.

Main lessons learnt and policy outcomes

Lessons learnt, benefits, limits, and policy outcomes

The form that the National Risk Profile takes is strongly influenced by the fact that it superseded a National Vulnerability Report issued in the years 2005-2010, and is part of a suite of guidance for other players in Denmark's national crisis management system that preceded informal agreement in the EU on the form that national risk assessment should ideally take. Accordingly, DEMA has tried to find a formula that, in the first instance, meets Denmark's own needs within the resources that DEMA has available for this kind of product, but which, secondly, meets the need to be consistent and comparable with work being done by other EU Member States with whom Denmark has consulted extensively over the past decade.

The result is a hybrid: a selective catalogue of risks which adopts many of the criteria recommended in European Commission guidance but whose assessment of their importance owes more to judgement than to objective calculation; whose narrative descriptions of incident types provides plenty of information that would enable judgements to be made on what the reasonable worst case scenario and associated likelihood of occurrence are in future, but which deliberately leaves these judgements to the reader; and whose presentation ostentatiously eschews "cumbersome methodological reflections" but respects the accepted terminology and is careful to avoid the incorrect use of terms (for example, in the title of the NRP itself , and in the use of "incident types" to describe what most NRA say are "risks").

Benefits

The benefits of this approach have been educational rather than programmatic: DEMA believe that the NRP has helped to promote risk awareness and a culture of risk management, building on the more technical guidance that preceded it, and that some basis messages about the most serious risk types – and the way in which they are headed for the future – have been communicated to a broader public. DEMA does not have the means of measuring the impact that the NRP has had in these respects.

Limitations

Nationally, the primary purpose of the NRP is to promulgate information about risks that may lead to major accidents and disasters that are beyond the ability of local authorities to manage and therefore require the participation of a wide range of agencies across sectors, for which it aims to provide a quarry for emergency planning assumptions. DEMA is cautious about this, arguing that it has no remit to insist on these agencies using the NRP as an authoritative reference for emergency planning, although the NRP is already proving useful as a means of informing the national exercise programme (which this year will focus on a nuclear accident involving a foreign power). Work on the initial 2013 version therefore focused on obtaining the willing participation of as many competent agencies as possible, to maximize the chance of gaining "buy-in" to the product. These limitations are mostly linked to the governance system in place.

Policy Outcomes

Within these constraints, the aim of the review currently underway will be to consider how to improve the utility and the authority of the NRP as a risk management instrument for the voluntary use across government and the various sectors.

Notes

1. The Danish Emergency Management Agency (DEMA) published a first "National Risk Profile" in 2013

2. The RVA is referred to in Danish legislation for example on harbour security, but otherwise is for voluntary use by lead departments and agencies, and is explicitly not used for the National Risk Profile. The 2005 version was updated in 2006, and more recent guidance has been issued on methods of analysing impacts.

3. ISO 3010 (*risk management – risk assessment techniques)* is a supporting standard for ISO 31000:2009 (*risk management – principles and guidelines*) which is one of the bases, together with UNISDR terminology on disaster risk reduction, for the European Commission guidelines.

References

Danish Emergency Management Agency (2015), Crisis Management in Denmark. Available at: http://brs.dk/viden/publikationer/Documents/Crisis%20Management%20in%20Denmark_UK.pdf.

The Danish Emergency Management Agency (2013), National Risk Profile (NRP). Available at: https://brs.dk/viden/publikationer/Documents/National_Risk_Profile_(NRP)_-_English-language_version.pdf.

The Ministry of Defence (2009), Act no. 514 of 26/05 2014 to amend the Emergency Management Act.

Further reading

ISO 31000, Risk Management –Risk Assessment Techniques, supporting standard for. Available at: https://www.iso.org/obp/ui/#iso:std:iec:31010:ed-1:v1:en

ISO 31000, Technical Definitions. Available at https://www.iso.org/iso-31000-risk-management.html

UNISDR (2009), Terminology on Disaster Risk Reduction. Available at: https://www.unisdr.org/we/inform/terminology

Chapter 10. ESTONIA

Estonia's crisis management process is enshrined in the 2009 Emergency Act. The act functions as the legal basis for putting in place emergency planning policy and procedures including the national risk assessment methodology. The governance framework in Estonia comprises of committees at national, regional and local levels. This chapter outlines the overarching governance framework that applies in Estonia. Transparency and accountability is at present difficult to access as indicated in the chapter by virtue of the de-centralised nature of the risk assessment process. The chapter analyses how the risk assessment is carried out, and where (as in many countries) the hazard identification is based on past history of major emergencies. Communication to the public is achieved by the publication of a summary of the results of the risk assessment process, although the chapter discusses the fact that the NRA is primarily used as a tool to identify the need for incident management plans and to identify the most serious of risks that may affect Estonia.

Key Words: Collective policy making; Crisis committees: De-centralisation; Hierarchy of risks; Risk evaluation; Restricted all hazards risk assessment.

Introduction

Estonia has had a national risk assessment process since as early as 2003, when Government Ministries first produced assessments of risks arising in their areas of responsibility following guidelines prepared by the Ministry of the Interior in 2002. The MoI also produced an overview of the work of the Ministries in 2003/4. The next major milestone for the current NRA process was the Emergency Act of 2009 which codified the crisis management organisation for the country and the foundation of a hierarchy of emergency risk assessment and crisis planning at government, regional and local levels.

The 2009 Emergency Act establishes the Minister of the Interior as the chair of the national Crisis Committee, which is a national resilience forum in which emergency planning policy issues including risk assessment methodology are discussed and agreed, and which approves a summary of emergency risk assessments that is made available to the public. The Act also sets out "vital services regulation" for the protection of essential services and critical infrastructure in Estonia, inter alia delegating responsibility for business continuity risk assessment to the providers themselves under the supervision of sponsoring Ministries and the overall co-ordination of the Ministry of the Interior.

The 2009 Emergency Act is now being reviewed, with significant changes potentially in prospect. Key issues include the degree of consistency in application of the NRA methodology established by the Ministry of the Interior and the way in which risk assessment is reflected in risk management and associated resource planning.

Governance framework

The 2009 Emergency Act provides the legal basis for crisis management and preparations on a geographical basis but also in relation to the continuous operation of 46 named kinds of vital public services including the supply of energy, transport, communications, food, water, health and emergency services. Inspired by legislation in New Zealand and the UK, the Act governs all aspects of crisis management and preparedness that are not separately provided for in other legislation (principally the Estonian State of Emergency Act and the Wartime National Defence Act); this means that the summary of emergency risk assessments under the Act covers all kinds of emergency including malicious attacks (which come under separate State Protection legislation) but excludes risks arising from terrorism or a military threat.

The Act establishes crisis committees at national, regional and local levels. At the Government level, the Crisis Committee is chaired by the Minister of the Interior; it provides a forum for discussion and agreement on a number of aspects of emergency planning and management including organisational issues, guidance on emergency risk analysis and planning, provision of assistance to a lead authority in a national emergency, declaration/termination of such an emergency, and the need to apply for international assistance. As in a number of countries, this is not an executive body, and it cannot direct other authorities that have statutory responsibilities in respect of risk management. Its collective policy-making role and membership would enable it to fulfil a strategic crisis management role in advising the Government of Estonia on a range of command issues including the key strategic functions of declaring a state of emergency and appointment of a "head of crisis situation".

A specific responsibility of crisis committees at all levels is to analyse the probability of the occurrence of emergencies. The national Crisis Committee has in addition the responsibility to approve a summary of emergency risk assessments, defined in the Act, which are produced by responsible Ministries operating to guidelines drafted by the Ministry of the Interior and reflecting consultation in the Committee.

Similarly, providers of vital services are obliged by the Act to prepare an assessment of the risks to the continuous operation of business critical assets contributing to the vital service, in accordance with guidelines established by the Ministry of the Interior.

Aims and Objectives

There are three kinds of documents concerned with risk assessment at the national level, each with different objectives:

- **The national summary of emergency risk assessments:** this is an overview of the (currently) 27 types of emergency which are thought potentially to require government intervention. The Ministry of the Interior bases the Summary NRA on assessments submitted by lead government departments; the assessments are not subject to comparative analysis or scrutiny as part of the process of creating the National Summary. Its purpose is rather to collate assessments by lead Ministries in order to provide a brief for Government Ministers, illustrating the scope of emergency planning at the highest state levels, and seeking formal sign-off to the allocation of risks to "risk class" reflecting the severity of their potential impacts, and their likelihood. Normally this signing-off process is by correspondence but there has more recently been some discussion in Committee of the Summary, suggesting that it has a role in raising awareness, clarifying responsibilities, promoting a risk management culture and, to a limited but growing extent, establishing government level priorities for risk management. In addition, since the Summary NRA is published, it contributes to risk communication efforts from government to promote business and community resilience in the wider population.
- **Emergency risk assessments by Government Ministries:** the hazards to be analysed are handed down to those ministries and agencies that have lead responsibility for developing plans to prevent emergencies or to alleviate their consequences. The purpose of risk analysis at this level is to contribute to "ministry development plans" for those risks that have been allocated to the top "risk groups", and to inform capability development, to these ends. In addition, the 2009 Emergency Act specifies that Ministers have to take risk assessment into account in setting departmental budgets but – as is the case in many nations using risk assessment - the potential for using this in the resource allocation process has not been fully developed.
- **Emergency risk assessments by vital service providers:** under the 2009 Emergency Act, vital service regulations are set out to ensure the continuous operation of 46 different kinds of essential service (Annex 10. A1) for a list of these and the associated "organising Ministries"). Under the supervision of the organising Ministry, within the overall co-ordination of the Ministry of the Interior, some 125 named vital service providers are responsible for preparing a risk assessment including: the identification of critical elements of the service they provide ("critical operating processes"); identification of the (between 20-30)

hazards having the potential to disrupt these processes; and preparing a plan for ensuring continuous operation. The plans are not currently published. The purpose of risk assessment at this level is therefore to inform planning priorities and aid capability building by each of the 125 providers.

Definition of key terms

The 2009 Emergency Act preceded publication of the European Commission's guidelines, which recommend referral to international standards developed by the international Organisation for Standardisation, in particular ISO 31000, ISO 31010, and the corresponding ISO Guide 73. Variations of standard definitions include the following:

- **Emergency:** an event or chain of events which endangers the life or health of many people, or causes major damage to property or causes major environmental damage, or causes severe and extensive disruptions of the operation of vital services, and resolution of which requires prompt and co-ordinated action by several agencies or authorities; (it should be noted that emergencies and disasters are synonymous in Estonian, and the word catastrophe is reserved for intentional, man-made, disasters)
- **Crisis management** is a system of measures which includes preventing an emergency, preparing for an emergency, resolving an emergency, and mitigating the consequences of an emergency.
- **Emergency risk assessment** is a document that describes (on the national and, if need be, on the regional and local government level) the event itself, the threats or hazards causing the emergency, the probability of it occurring, the consequences, and other important information related to the emergency and references to models, source materials etc. on the basis of which the assessment is prepared
- **Emergency response plan:** a document that describes the organisation and management structure for resolving an emergency, the role of participants, how information is to be exchanged, how the public is to be warned and informed, and international cooperation organised.
- **Crisis management exercise:** exercises organised with the aim of assessing the procedures and capability to resolve one or more emergencies, and which include all the competent authorities. It may include command-post exercises, field post exercises, or both in combination.

Transparency and accountability

For a population of 1.3 million (and falling in the short term at least), and a relatively benign disaster risk profile, the disaster risk management system is in principle relatively de-centralized, with the responsibilities of the different actors in the national, regional, and local emergency planning hierarchy clearly set out in legislation, as are the responsibilities of providers, organisers and co-ordinators for the resilience of vital services.

Accountability for emergency risk assessment similarly is de-centralised. From the early years of the Estonian national risk assessment process, the Ministry of the Interior has sought to ensure the comparability and transparency of risk analyses carried out by other Ministries by issuing guidelines, by a degree of involvement in Ministries risk evaluation processes, by providing and obtaining collective agreement to a summary of

risk assessments at the highest level, and by publishing the summary. The onus is on responsible Ministries to assess the risks which they own and, although the Ministry of the Interior assists in this process, there is otherwise limited scope for peer review of the assessment, and the quality of assessments may be uneven.

The numbers of organisations involved in risk assessments for the 46 vital services makes it harder for the same degree of supervision and accountability to be exercised and the accountability of heads of agencies, and of providers of these services, is currently under consideration as part of the current review of legislation.

Multi-level governance- and multi-actor participation

The Act was in part based inspired by legislation in New Zealand and the United Kingdom and, like them, is on the face of it based on the principle of delegation, creating a "bottom-up" approach to resilience in which the responsibilities for organising, planning, and exercising for emergencies are distributed to local, regional and national Government level through the creation of Crisis Committees at all three levels. In practice, the risk profile of Estonia is such that most planning and risk assessment activity is in effect centralised. As a consequence, the scope for involvement by representatives of the regional crisis commissions, and of independent scientific advisers, is constrained. The involvement of the private sector is limited to risk assessment for the 46 vital services mentioned above.

Risk analysis

The Estonian risk assessment is undertaken in five stages:

1. defining the type of emergency to be assessed
2. identifying the risks through the use of scenarios
3. analysing the probability and probable impact of emergencies
4. evaluating the risks by assigning them to one of four "risk classes" (very high risk; high risk; medium risk; low risk) defined first by the potential impact and second by the likelihood of occurrence
5. identifying risk reduction measures (preventive measures or impact alleviating measures).

Scope

The Estonian risk assessment is a restricted all-hazards risk assessment in that all kinds of threat and hazard are included except for the risk of terrorism and war, which are covered by a separate State Protection Act. There are two main contributing elements:

- The analysis by lead Ministries of the risk analysis carried out by them of the major risks which pose a major risk of harm in accordance with the definition of emergency in section 1.2 above.
- Analysis of the consequences of emergencies affecting the continuity of vital services, drawn from the analysis carried out (see Aims and Objectives) by 125 named vital service providers and fed into the national risk assessment by the sponsor Ministries.

Hazards originating outside Estonia are included if there is potential for Estonian citizens to come to harm, even if they are not themselves in country. This has given rise to

difficulties in relation to the risks to Estonian nationals who are affected by disasters while travelling abroad: the sponsoring Ministry has placed this risk in the "very high" risk category on the grounds that there is a very high probability of this happening, with very serious consequences. Other national risk assessments tend to exclude these kinds of risk on the grounds that the national risk assessment should be restricted to emergencies directly affecting national territory even if they originate outside (for example a Chernobyl-type risk), or the risk to citizens when abroad are separately assessed according to criteria developed for the purpose.

Hazard Identification

The identification of hazards in the Estonian risk assessment is affected strongly by the past history of natural emergencies in Estonia, and by the variable degree of enthusiasm among Government Ministries for hazard risk analysis. This has meant that prominence is given in the NRA to the risks arising from pollution, which dominate the "very high" risk class (Table 10.1).

Table 10.1. Risk classes and risk types

Risk Class	Risk types
Very High (very severe to catastrophic impact and moderate to very high likelihood)	Incident abroad Maritime pollution Coastal pollution Maritime accidents Epidemic Pollution inland
High (severe impact and moderate to very high likelihood; or very severe to catastrophic impact but low likelihood)	Forest fire Storms Floods Road accidents Riots Epizootia Cyber incident Prison riot Sudden attack Chemical accident Fire, explosion, collapse in industrial buildings/warehouses
Medium (severe impact but low likelihood; or very severe to catastrophic impact but very unlikely)	Aircraft accident Nuclear accident Railroad accident Hazardous ice Radiological incident
Low (light to moderate impacts)	Hot weather Influx of refugees Cold weather

Source: Siseministeerium 2012 (Ministry of the Interior), National Emergency Risk Assessments

Impact Analysis

The criteria for deciding what qualifies an event as an emergency are fourfold, with differential levels of severity indicated in Table 10.2.

Table 10.2. Criteria for deciding what qualifies an event as an emergency

Impact criteria	Indicators
Human life and health	• numbers of fatalities • numbers requiring immediate medical care • extent to which number of injured exceeds regional health care resources
Asset damage	• Cost of damage to property • Harm to GDP
Natural environment	• Change in the population of any species • Change in the ecosystem function • Need for human intervention to restore environment to original state
Vital service	• Extent of disruption of vital service(s) • Duration of disruption of vital service(s)

Source: Siseministeerium 2012 (Ministry of the Interior), National Emergency Risk Assessments.

The threshold for consideration as a national risk of emergency is determined by the risk steering group, based on the guidelines developed by the MoI. Impact is measured on a scale from A (very low) to E (catastrophic), and the overall score for each risk is based on the highest level of impact, regardless of type, rather than on an average or on disaggregated presentation of the risks according to each type of impact. The scales for measuring impact are non-linear, to encourage order of magnitude differences to be identified by Ministries conducting risk assessment. The scales are tailored to the capacity of the systems affected - for example, the scales for injury proceed from 0-30; 31-170; 171-400; and over 400 for the top of the scale, all based on the capacity of hospitals, as advised by the Estonian Board of Health, to take in trauma patients. Economic damage is measured in proportion to Gross Domestic Product with the maximum of the scale being over 0.5% of GDP, the level at which foreign assistance might be required. The impact on vital services is based on the severity of the impact on any of the 46 Vital Services listed in Annex 10. A1.The only risk assessed to have potentially catastrophic impacts is an aircraft accident, which is however assessed to have a very low likelihood of happening. Most of the risks of man-made accidents or pollution are assessed to have potentially very serious impacts, as is the risk of an epidemic.

Likelihood and Plausibility Analysis

Guidance to Ministries conducting risk analysis is that an assessment of likelihood should be made using the scale presented in Table 10.3, which distinguishes between events with a relatively high likelihood of occurring from those that are much rarer, based on historical evidence informed to an extent by trend analysis of the effects of risk drivers on probability in the future.

Table 10.3. Measures of likelihood for risk scenarios

Level	Probability	Probability of occurrence within 5 years
1	Very low	<0.005 to 0.05%
2	Low	<0.05 to 0.5%
3	Medium	<0.5 to.5%
4	High	<5 to 50%
5	Very high	<50%

Source: Siseministeerium 2012 (Ministry of the Interior), National Emergency Risk Assessments.

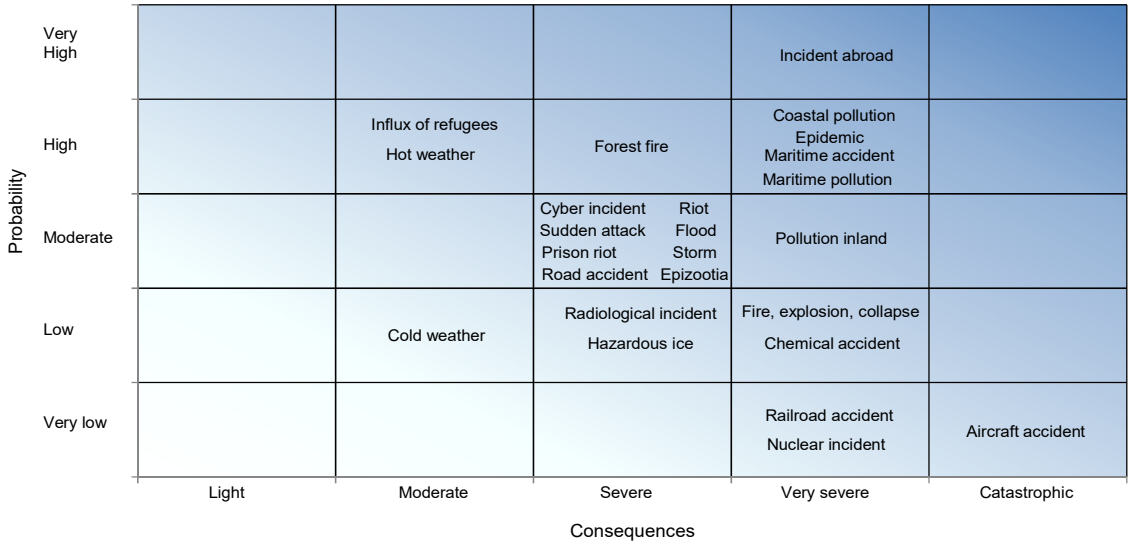
On this basis, the most likely events are assessed to be: an incident abroad; maritime pollution, coastal pollution, a maritime accident, and epidemic, and a forest fire (all assessed to have serious or very serious impacts); hot weather and an influx of refugees (relatively light impact).

Risk evaluation, monitoring and re-evaluation

The risk analysis provided by lead Ministries is plotted on a 5-by-5 matrix with impact on the vertical axis and likelihood/plausibility on the horizontal axis. As noted above, impact is based on the highest rather than the average score as assessed by the Ministry that leads on each risk, and there is no disaggregated presentation of the overall impact.

Figure 10.1 represents the risk profile for Estonia in 2013; this has one additional risk when compared with 2011 when the previous summary assessment was produced. Risk assessments are carried out as and when required – lead agencies are required by statute to keep risks under review but it is their judgement as to how frequently review is required. The national NRA summaries are produced every two years.

Figure 10.1. Risk Profile (2013)



Source: Adapted from presentation given by representative of the Estonian Ministry of interior.

Communicating the results of National Risk Assessment

The Estonia NRA process is primarily a tool to identify the need for incident management plans for the highest risks. But the Summary is published and therefore performs a secondary risk communication function to the public. We were unable to explore the extent to which it is more actively used to promote business continuity planning and community resilience self-help schemes in the wider public. There is no evaluation of the effectiveness of this risk communication approach.

Main lessons learnt and policy outcomes

Estonian government officials have used risk assessment to inform disaster risk management policies for longer than most EU/OECD governments. Those involved in the Estonian national risk assessment process believe that there have been two main benefits from the process: first, that there is a clearer understanding across government of what happens when disasters strike, and therefore better preparedness for them; second, that there is a healthy culture of cooperation arising from the collaborative nature of the process, with less institutional "stove-piping" than would otherwise be the case. These are significant benefits; the challenges facing the Estonian government are mainly to do with:

- Reinforcing the all-hazards policy framework for risk management to promote interagency planning and co-ordination across ministries, regional and local government by refining and clarifying the methodology for risk assessment, and supporting those who have to use it.
- Developing the process of translating risk assessments into risk management practice and investment in capability. Binding the necessary risk reduction activities into budget planning.

Against this background, the review under way will identify the options for further improving and exploiting the risk assessment process in order to improve civil protection.

References

Presentation given by Galina Danilišina from Rescue and Crisis Management Policy Department/advisor 20.04.2015.

Siseministeerium 2012 (Ministry of the Interior), National Emergency Risk Assessments.

Emergency Act 2009. Available at: https://www.riigiteataja.ee/en/eli/525062014011/consolide

Further reading

ISO 31000:2009, Risk management – Principles and guidelines and ISO Guide 73:2009, Risk management – Vocabulary.

Annex 10.A1

The 46 vital services, and the Ministries responsible for them, are:

Ministry of Justice	**The prison service**
Ministry of Economic Affairs and Communications	Electricity supply Gas supply Liquid fuel supply Airports Air navigation services Management of public railway Rail transport services, including passenger services Ice breaking services Ports Vessel traffic management system Main and basic road maintenance Telephone network Marine radio communication network Cable network Broadcasting network Postal network Uninterrupted communication
Ministry of the Interior	Maintenance of public order Rescue service Processing of emergency accident messages Air and sea rescue Marine pollution monitoring and control Operational radio communication network The Riigikogu, the Government, and the Presidency
Ministry of Social Affairs	In-patient specialised medical care Emergency medical care Drinking water safety control Blood service
Ministry of the Environment	Air surveillance and early warning Hydrological and meteorological monitoring and early warning Early warning of a risk of radiation
Ministry of Agriculture	Food safety
Ministry of Finance	Payment and clearing operation, including payments by state authorities
Bank of Estonia	Payment services Cash circulation
Local government	District heating system and network Rural municipality roads and city streets Water supply and sewerage, including waste water treatment plants Waste management Public transport in rural municipality or city

Chapter 11. FINLAND

This chapter on Finland's National Risk Assessment outlines the actions that Finland has taken to overhaul its risk assessment process by putting in place an NRA in 2015. The governance framework is discussed in the context of senior level government leadership beginning at the Prime Minister's office cascading down to ministerial responsibility by various departments with responsibility for emergency response. Synergies with neighbouring countries and the European Union methodologies are also discussed in the development of the NRA process as good practice and cross border requirement in the event of a national incident with cross border dimensions. Transparency and accountability is ensured by a collaborative approach at senior government level. This occurs on regional and local levels and with public and private entities although independent validation of the process has not taken place at the time of writing. Communication is facilitated by the involvement of a large number of stakeholders within the process. Public access to the NRA is currently restricted.

Key Words: Core vital functions; Generic risks; Harmonisation; Identification of vulnerabilities; Strengthening of co-ordination mechanisms.

Introduction

The peer review of Finland's risk management policy[2], conducted during October 2013 by the European Commission, the OECD, and the UNISDR, noted that the risk assessment process in Finland would benefit from a more comprehensive approach and better co-ordination from the national to the local level. Indeed, the 2010 National Security Strategy for Society was based on a well advanced risk identification process, combining the definition of the core vital functions of Finnish society that have to be secured in all situations, and the identification of their vulnerabilities to a series of 13 generic threat scenarios. However, the impacts and the likelihoods of these different threat scenarios were not evaluated and quantified, and could then not allow comparing them in order to define priorities in risk management, which is the essence of a National Risk Assessment process.

In the two years since then, the government has overhauled its risk assessment process and will have put the finishing touches to its first National Risk Assessment in the autumn of 2015. This will identify the top risks facing the country as a whole, and the most common "generic" risks which for the most part should be managed at regional or local level, in line with the responsibilities for emergency management devoted to the regional and local level under the Rescue Act. Over 60 risks have been identified and analysed by the multi sectoral working group established by the Ministry of the Interior at the request of the National Security Committee for this NRA process. The list has been nailed down to 21 risks after several rounds of consultations. The assessment of the impacts of risks scenarios is underway for all these risks, but the probability/likelihood analysis will only be done for the most common generic risks and not for the top risks, for which there is no historic records. These two series of risks will be represented then differently, with a target style diagram for the top national risks focusing on impact criteria and a classic risk matrix for the 15 other important risks falling under the responsibility of regional rescue services.

Following discussion of the thresholds that should be applied, the top risks to be recommended to Government Ministers are likely to be in the following areas:

- nuclear power plant accident causing radioactive hazard in or near Finland
- geopolitical threat directed at or affecting Finland
- infectious disease pandemic
- severe Solar Storm
- cyber- attack
- disruption in supply of energy (electricity, oil or fuel).

The NRA process has generated a significant multi-stakeholder engagement and allowed the initiation of a large whole-of-government dialogue on risks, including with local governments and the private sector. These efforts come at the right time as they will constitute the basis for an updated version of the National Security Strategy for Society that may possibly be renewed in 2016.

2. The Review was carried out in October 2013 and published in 2014.

Governance framework

For this first NRA, a Working Group was set up consisting of members of the preparedness secretaries of the ministries with responsibilities for emergency response at the national level including: the Prime Minister's office, Ministries for foreign affairs, the interior, health and social affairs, agriculture and forestry, transport and communication, employment and the economy, the environment, the education and culture and defence as well as the Security Committee. The private sector was represented through the national emergency supply agency and regional authorities with the Regional State Administrative Services, and Centre for Economic Development, Transport and the Environment. The Ministry of the Interior (Department for Rescue Services) co-ordinates the work of this Working Group and the work is steered by the Security Committee.

When agreed at this level, the Finnish NRA will be submitted to the Security Committee at Permanent Secretary (top official) level, and then to the Ministerial Committee that is responsible for European Union issues for its final endorsement at Ministerial level.

Aims and Objectives

The Peer Review of Finland's risk management policy noted that, prior to 2013, these policies operated at two levels:

- A national level, where the 2010 Security Strategy for Society had adopted an approach based on the identification of the vital functions of Finnish society that have to be secured in all situations, and their vulnerabilities to disturbance illustrated in 13 scenarios. This provided a uniform basis for strategic preparedness of all Finnish institutions but was not sufficient to be used operationally for capability or emergency planning, or for risk reduction purposes. This is because the threat scenarios had not been assessed in terms of their likelihoods and impacts.
- Regional risk assessments carried out and updated regularly by the (22) rescue authorities for the purpose of capability and emergency planning as required by the Rescue Act. Tools and guidance developed by the Ministry of the Interior provide a consistent basis for this regional assessment, which is used to determine the standard of service to be provided by the rescue authorities and the capabilities they need to reach this standard. Risk zones are defined for the whole country, and mapped on a 1 kilometre grid which indicates the level of exposure to risk, and response times required for the emergency services.

The Review noted that methodologies for risk assessment under these two approaches were being harmonised, under the co-ordination of the Ministry of the Interior, so that probabilities and potential impacts of emergencies at the strategic national, and at the regional, level could be assessed on a comparable basis, for the purpose of building on the already advanced risk management policies and capacities present in the country. This would enable Finland to keep pace with developments in its risk profile arising from its high dependence on critical infrastructures and global supply chains, and the exposure of its widely distributed population to its Nordic climate conditions. It would also constitute the Finnish Government's response to the European Council Decision on a Union Civil Protection Mechanism.

Harmonisation of risk assessment methodologies is being designed with a four-fold purpose:

- To aid development of risk management strategies and capabilities, to fill gaps that may be emerging due to evolution of the country's risk profile.
- Promotion of a consensus with Government and with stakeholders outside on the priority to be accorded to the risks.
- Promotion also of a risk management culture.

By drawing on elements of the European Commission guidelines, and by maintaining comparability with the methodology being developed by Norway in its national risk assessment, the Finnish approach also maintains the objective of facilitating cross-boundary comparison of risks with neighbouring countries.

Definition of key terms

The first Finnish NRA will have a list of definitions, based broadly on those in the European Commission guidelines. This will include a definition of "risk" which takes account of the likelihood of emergencies occurring, and the probable impact in four broad areas (human, economic, environmental, and social/political impacts) taking into account the robustness or vulnerability of assets in these areas.

Transparency and accountability

A key element of the changed process for national risk assessment since 2013 has been strengthening of the arrangements for collaboration across administrative boundaries and the strengthening of co-ordination machinery. Thus, although it remains the responsibility of each Ministry to undertake risk assessment in its area of responsibility, the resulting "risk cards" are assessed in the Working Group to ensure that the scenario, and the evaluation of risks that it illustrates is understood within the group. Since the Working Group includes not only the Ministries but also the National Emergency Supply Agency (which has links to private sector representative bodies for each of the main service sectors, known as "clusters"), the Regional State Administrative Agencies, and the Centre for Economic Development, Transport and the Environment, it includes in one body – directly or indirectly – all the main stakeholders in national resilience. Subject-matter experts can be consulted from Government agencies such as the Meteorological Office, and transport agencies.

The Finnish NRA will be agreed by the government at the political level, through the senior ministerial committee that deals with European issues. When agreed and published, the NRA will explain the methodology, enabling stakeholders not directly represented in the process to understand the basis on which judgments have been made. Independent validation of the methodology, bias control, and the creation of an independent challenge function within the Working Group may follow once there has been a chance to review the first NRA, including by further involving the scientific community in the process.

Multi-level governance and multi-actor participation

At present the risk assessment process is conducted as collaboration between authorities at the national level, with participation by some representatives of the regional level. At the regional level, provinces are likely to carry out their own Regional Risk Assessment as a next step following agreement to the NRA, and 2 of the 6 provinces were reported to be participated in the NRA process. In due course, the Finnish government expects the NRA to steer the development of more regional and local risk assessment by

rescue services in support of their responsibility under the Rescue Act to co-ordinate planning for emergencies. In that case, the main outcomes of the first NRA will be:

- The development of risk management strategies at the national level for the handful of top (tier 1) risks accepted as such by the Government
- The development of Regional Risk Assessments covering those (tier 2) risks delegate to regional level by the Government
- Development of Local Risk Assessments covering tier 3 risks deemed to be for local management

Risk analysis

This first Finnish NRA will be designed to be able to support the first two of these three required outcomes, in its scope, and the analysis of impact (for all risks) and likelihood (for tier 2 risks).

Scope

The Finnish NRA will be an all-hazards assessment, including risks of intentionally harmful acts such as terrorism and cyber-attacks. The only exclusions – to be explained in the public version of the NRA - are the risks of financial crises. It will aim to be comprehensive from the start.

Hazard Identification

The initial stage of the risk assessment process has been the preparation of "risk cards" by each administrative sector (Ministries) covering the risks of emergencies arising in their own area of responsibility. The risk cards describe the nature of the risk and the expected outcome in terms of the impact in each of the areas of interest (human, economic, social/political and environmental impact). Over 50 of these risk cards were produced but many of these overlapped in scope and these were reduced during the initial phase of assessment to around 20 generic risk types to be the subject of detailed analysis

Detailed analysis was carried out in a number (21) of working groups, which developed scenarios covering the scope of the risk cards that contribute to the generic risk types, resulting in an agreed set of "reasonable worst case scenarios" describing the historical background to the risk, an outline description of the likely outcome, and actions already in place to prepare for and respond to the event described in the scenario. The scenarios will cover the risks in Table 11.1.

Table 11.1. Risks covered in risk scenarios

1	Major Flood
2	Strong winter storm
3	Severe weather
4	Pandemic
5	Multiple forest fires near settlements/communities
6	Interruption of water supply
7	Large maritime accident in the Baltic sea
8	Large chemical accident or explosion near settlement
9	Nuclear power plant accident causing radioactive discharge in or near Finland
10	Major fire affecting critical infrastructure
11	Major forest fire
12	Disruption in energy supply (electricity, oil, fuel)
13	Severe transport accident (air, road or rail)
14	Security political threat directed at or threatening Finland
15	Terrorist attack against Finnish people abroad
16	Violent attack on people (e.g. school shooting)
17	Major public disorder
18	Disruption in data systems caused by cyber attack
19	Space weather/ solar storms

Source: Ministry of the Interior Finland (2016).National Risk Assessment 2015.

Of these generic risk types, those highlighted in **bold** are considered being "tier 1" risks for the State to manage; in the NRA they are likely to be plotted mainly on impact rather than on likelihood. Other scenarios provide the basis for tier 2 risks which would in the first instance for regional authorities to manage although, in the reasonable worst case scenario, they may need recourse to capabilities and capacity held in neighbouring regions or at the national level; these will be plotted both on impact and likelihood.

Impact Analysis

There are five main criteria for assessing the impact of emergencies in the Finnish NRA Table 11.2.

Table 11.2. Criteria for assessing the impact of emergencies

Main criteria	Sub-criteria
Human impact	Fatalities Seriously injured Numbers Evacuated
Economic impact	Material damage Property damage Interruption damage
Environmental impact	Affected area (kilometers2) Duration
Impact on critical infrastructure	Energy production and distribution system Information and communication technology systems Financial services Transport and logistics Water supply Building and maintenance of critical infrastructure Waste management Food supply Health care system Industry Production that supports military defence
Impact on vital functions	Management of government affairs International activity Defence capability Internal security Functioning of the economy and infrastructure Public income security and capability to function Psychological resilience to crises

Source: Ministry of the Interior Finland (2016).National Risk Assessment 2015.

Measurement of impact is done on a 5-point scale (Table 11.3). For example, human casualties numbering less than a dozen would count as a low impact, with thresholds for subsequent points on the scale increasing by an order of magnitude to a high impact exceeding a thousand casualties. The social/political impacts of disruptive challenges are much more a matter of judgement of the extent and duration of the disruption. In the overall assessment, no particular weight is given to any particular criterion.

Table 11.3. Impact scale for tier 2 events

	I	II	III	IV	V
Dead (number)	<= 5	6-15	16-50	51-200	> 200
Injured (number)	<=15	16-45	46-150	151-600	> 600
Evacuated (number)	<= 50	51-200	201-2000	501-2000	> 2000
Material damage (M. euros)	< 1	1-10	100-500	100-500	> 500
Interruption damage (M. euros)	< 1	1-10	100-500	100-500	> 500
Environment (square Km)	< 1	1-10	100-1000	100-1000	> 1000
Duration	< week	<month	6 moths - 1 year	6 months - 1 year	over 1 y
Critical infrastructure (number of affected ones)	0-2	3-4	7-8	7-8	9-11
Duration	< day	1 day - 6 days	2 weeks - month	2 weeks - month	over month
Vital functions (number of affected ones)	0-1	2-3	5-6	5-6	7
Duration	< day	1 day - 6 days	2 weeks - month	2 weeks - month	over month

Source: Ministry of the Interior Finland (2016).National Risk Assessment 2015.

Likelihood and Plausibility Analysis

As noted above, for the top risks, the Government has decided that they do not need to calculate probability because all of these risks are plausible, and they intend to accord an equal priority to all.

Accordingly, an assessment of the likelihood or plausibility of hazards and threats is made only in respect of the 15 or so "tier 2" risks (i.e., those that engage the regional level of administration) for which a sense of likelihood is needed to establish priorities for emergency response planning. The calculation of probability is made according to the scale in Table 11.4, which relates to the expected likelihood and return period for risks in the near future (i.e., there is no specific time horizon for the assessment of probability):

Table 11.4. Likelihood values and description

Value	**1**	**2**	**3**	**4**	**5**
Description	Very low	Low	Average	Significant	Catastrophic
Criteria	Once every 1000 years	Once in 500 – 1000 years	Once in 100 – 500 years	Once 10 - 100 years	Once in 10 years

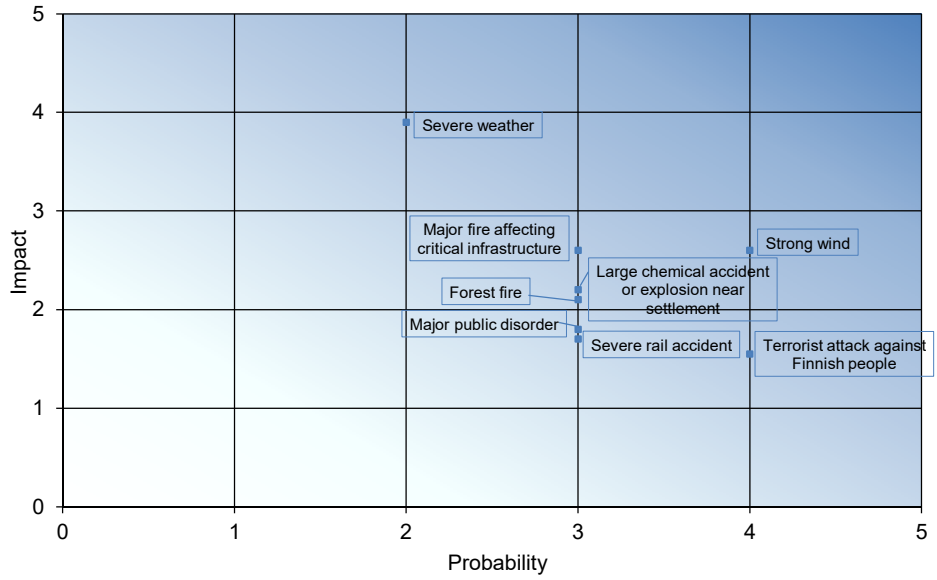
Source: Ministry of the Interior Finland (2016).National Risk Assessment 2015.

Risk evaluation, monitoring and re-evaluation

It is expected that the risk evaluation process will result in the production of two different representations: the top-level risks (tier 1) will be represented independently in a 4 axis radar graphic highlighting only the impacts around the 4 types of impact criteria, as the likelihood will not be evaluated; for the 15 tier 2 risks a matrix representation plotting

them in terms of their potential impact and likelihood will be developed along the following lines in Figure 11.1.

Figure 11.1. Serious regional accidents shown in a risk matrix



Source: Adapted from Ministry of the Interior Finland (2016). National Risk Assessment 2015.

The initial intention for the evaluation of this first NRA and potential updating has been stated to be of 3 years.

NRA Excursions

The Finnish NRA process takes account both of the cascading effects of risks, notably through the disruption of critical infrastructures, and of the potential for cross-boundary risks, such as in the scenarios of Nuclear power plant accident causing radioactive discharge in or near Finland or "Large maritime accident in the Baltic sea".

Risk mapping has been a feature of the Finnish approach to risk management for many years, as noted in the Peer Review which reported that risk zones are defined for the whole country based on the national incident data-base and other information, and that these data are aggregated through a high-technology GIS-based mapping of the country on a 1 kilometre resolution grid.

In addition, the Finnish Government is carrying out longer-term risk assessment in support of the development of a national climate change adaptation plan. At the other end of the time horizon, a horizon-scanning risk matrix is maintained to identify the most likely sources of emergency over the next 6 months.

Communicating the results of National Risk Assessment

Using the National Risk Profile to raise awareness about risks

The involvement of regional authorities in the NRA process is intended to facilitate the adoption of the NRA by regional emergency planners and, in due course, local

planners for their own purposes, including in the formulation of regional and local risk assessments reflecting regional/local conditions. The intention is that there should be a public version of the NRA, which contains no classified information but includes both tier 1 and tier 2 threats and hazards.

Tools for interpreting risk analysis

The Ministry of the Interior has developed tools and guidance for regional risk assessment, to enable the 22 rescue services of Finland to decide on the standard of service that should aim to provide to comply with the Rescue Act, and what capabilities they may need to meet the standard. The NRA when agreed by the Government and promulgated, will provide information enabling the rescue authorities and other authorities obliged to participate in rescue work to differentiate between the different kinds of impact that the tier 2 risk types may have within the overall risk assessment.

Main lessons learnt and policy outcomes

Lessons learnt

There were a number of recommendations for improvement to the national risk assessment process in the 2013 Peer Review, all of which have been addressed in the new approach to this first NRA:

- A more comprehensive approach and better co-ordination from the national to the local level, which has been partly addressed in the composition of the NRA Working Group.
- Improved systems for monitoring and assessing larger-scale risks that, although less likely, would cause severe impacts: these have been separately identified by applying a higher threshold for impact assessment that would distinguish them from (tier 2) risks whose management can more effectively be delegated to regional rescue administrations.
- More coherent criteria for determining the consequences of major disasters, so that the criteria for fatalities are more directly equivalent to those for measuring economic impact and environmental impact.

The first NRA will be circulated, first to the Security Committee and then to Ministers, before promulgation to all authorities who have a stake in the outcome of the assessment. Comments from this circulation will also provide a basis for a review as necessary of the NRA methodology before work starts on the next edition expected to be produced in three years' following this action.

Benefits

At this stage, the first observable benefits of the NRA has been the reinforcement of already strong patterns of collaboration between the main actors in the NRA Working Group, and a growing interest among them in the potential of risk assessment to help formulate a forward-looking national risk management strategy for the top risks which are by their nature complex and cross-cutting. The strengths of the Finnish approach (which is less stove-piped than other national administrations and finds it easier to work to a common methodology and to resolve disputes over risk ownership) have been reinforced and extended beyond central Government to the regional administrations and, indirectly, to the private sector.

Limitations

There remain constraints on the involvement of some key stakeholders in the NRA process, and the government will be examining further improvements in governance, and in the engagement of stakeholders in the private, academic and NGO sectors, as well as at regional/local level, to promote the desired outcomes:

- The development of risk management strategies at the national level for the handful of top (tier 1) risks accepted as such by the Government.
- The development of Regional Risk Assessments covering those (tier 2) risks delegate to regional level by the Government.
- Development in due course of Local Risk Assessments covering tier 3 risks deemed to be for local management.

Policy Outcomes

It is expected that this National Risk Assessment would form a good basis for the development of the possible upcoming update of the National Security Strategy at the time of writing presumed to be 2016.

References

Ministry of the Interior Finland Publication (2016), National Risk Assessment 2015.

Further reading

OECD, UNISDR EUR & EC (2014), Finland peer review report 2013 - Building resilience to disasters: implementation of the Hyogo Framework for Action (2005-2015). Available at: https://www.unisdr.org/we/inform/publications/38523

Chapter 12. GERMANY

This chapter on Germany outlines how the governance framework functions in national and regional risk assessments. At a Federal level the risk assessment process for civil protection makes a clear distinction between risk analysis and risk evaluation. The Federal Office of Civil Protection and Disaster Assistance (BBK) consulted internationally when compiling the NRA and applied good practice and ISO standards throughout. Transparency and accountability is widespread in the case of Germany with exposure in public forums such as the Federal Parliament and to the public online. This chapter discusses the methodology for hazard identification and analysis, in addition to vulnerability and impact analysis in some detail. There is substantial ongoing exposure for the NRA at the highest level of government which serves to keep it up to date and relevant.

Key Words: Collaboration; Cross disciplinary approach; Expertise; Joint responsibility; Interconnection; Transparency.

Introduction

Further to a "new strategy for the protection of the population in Germany" (Standing Conference of the Minister and Senators for Internal Affairs agreed in 2002), the federal states (Länder) each conducted a first uniform estimation of hazards (technical, man-made and natural) faced by the civil populations in their areas of responsibility, in 2004-2005. These sixteen hazard estimations were combined with information on national level hazards (such as epidemics, failure of national infrastructure) to form the first national Joint Hazard Estimation in 2006. As the next step in fulfilling the 2002 civil protection strategy, the Federal Office of Civil Protection and Disaster Assistance (BBK) was invited to propose a method of analysing both the probability and the impact of these hazards so that risk analysis could be conducted in a consistent fashion at all administrative levels including at the Federal Government level, the Länder level and at the level of municipalities. Accordingly, the BBK developed a risk analysis methodology for civil protection which is constantly reviewed, updated and improved in line with new developments. BBK has also developed guidelines for the implementation of the methodology to provide more tailored guidance to the particular needs of different administration levels. These guidelines explain how to employ the method, including instructions on how the specific levels need to proceed in the area of risk analysis and risk management (BBK, 2015). BBK has also identified 18 hazardous events with potentially national significance, and used the methodology to conduct its own analysis of several risk scenarios. The results of these analyses have been reported to the Federal Parliament (Deutscher Bundestag, 2012-2015).

Governance framework

In accordance with the 2009 Federal Civil Protection and Disaster Assistance Act1, the Federal Government in cooperation with the Länder compiles a nationwide risk analysis for civil protection. The Federal government is responsible for protecting civilians from hazards and risks arising out of military conflicts and wars; in all other cases the responsibility lies with the Länder. But, in the 2002 "new strategy for civil protection", it was agreed that a narrow partitioning of responsibilities would be inadequate in the event of a disaster on a national scale, and that it should be a joint responsibility (in a pragmatic, political sense rather than as a matter of law) of the Federal Government and the Länder to overcome such a large scale contingency. To give effect to this, a core element of the 2002 strategy was to promote better interconnection, fine-tuning and collaboration between officials at the federal level on the basis of hazard and risk analysis: the Federal Government would conduct an inter-departmental risk analysis for civil protection, looking in a generic way at hazards that have the potential to be nationally relevant within the scope of the Government's constitutional and legal responsibilities; the analysis of these types of risks would be supplemented by corresponding analysis at the Länder and municipality of how such hazards might impact in their geographic area of responsibility; and these national, state and municipal risk analysis would provide an integrated (both inter-jurisdictional and inter-departmental) system of risk analysis to inform civil protection planning. At the Federal Government level, risk analysis arrangements are conducted through a structure of committees with cross-government representation as follows:

- A Steering Committee of representatives from federal ministries, co-ordinated by the Ministry of the Interior, is charged with decisions on the overall methodological framework for risk analysis at federal level (damage parameters, classification+), selection of hazards to be assessed, the tasking of subordinate groups and evaluation of their results.
- A Working Committee of representatives from federal agencies chaired by BBK ("Riskoanalyse BevS Bund") is charged with developing scenarios for specific hazards, carries out risk analyses, and preparing reports for the Steering committee, including an annual report to the Bundestag.
- Hazard-specific sub-groups of subject-matter experts, led by specialised lead agencies and BBK, carry out the risk analysis for these scenarios.
- BBK participates directly in the work of the hazard working groups and the Working Committee, inter alia, to control for bias in their deliberations.

Aims and objectives

Civil protection authorities are responsible for providing reliable information about hazards, risks and available capabilities for crisis management. This information is supposed to provide such authorities with a neutral and transparent basis of decision-making about the handling of risks. These decisions relate to risk management (e.g., prioritisation of measures for the minimisation of risks), emergency planning (e.g., preparation for incidents that cannot be avoided) and crisis management (e.g., provision of resources for response) (BBK, 2011, p.46).

At the Federal Government level, the risk assessment process for civil protection encompasses but makes a clear distinction between:

- Risk analysis, which is an objective-dispassionate inventory of what would have to be reckoned with upon the onset of a hazardous incident in Germany and which pre-empts neither the prioritisation of individual risk scenarios nor the evaluation of risks or provision to be made for risk management, from a policy perspective.
- Risk evaluation which is a political or policy-making process in which social values and risk tolerance levels are factored in by ministers and officials, in order to decide upon the objectives of policy, what measures can or must be taken to achieve those objectives, and whether the residual hazard is tolerable.

On this basis, the purpose of the national risk assessment is to provide a risk analysis which is fit for the purposes of informing risk evaluation and policy decisions at federal level, in accordance with the Government's constitutional and legal responsibilities, and to inform risk analysis at state and municipal level as part of the interconnected system of risk assessment in Germany.

Definitions of key terms

In developing the risk analysis methodology, the BBK took into consideration existing international standards (ISO31000 and ISO 31010), and consulted a number of other nations including the Netherlands, the United Kingdom, United States, Norway and Sweden. As a consequence, several definitions are used (Annex 12.A.1) (BBK, 2011).

Transparency and accountability

The pragmatic approach to collaboration between departments and agencies in the risk analysis process promotes transparency within government and between the different levels of government. For example, the analysis of the risk posed by severe winter storms was conducted in a working group led by the German Weather Service but with over twenty federal agencies involved.2 BBK also ensures that the results of work on NRA scenarios are continuously communicated to the federal states (Länder) during the analysis phase to ensure transparency between national and federal governments (Deutscher Bundestag, 2012, p.3).

Transparency and accountability are also built into the national risk assessment process through an annual report delivered to the Federal Parliament on risk analysis for civil protection, which is discussed in select Committees of the Bundestag, and has also been discussed in plenary. These reports are available online.

Multi-level governance and multi-actor participation

The BBK envisages the intensification of cooperation between "all players and administrative levels to concentrate and communicate the respective findings in an appropriate way", this includes "the inclusion of interdisciplinary expertise from various authorities from the start of the procedure, to ensure coverage of as many aspects of the variety of risks as possible" (BBK, 2011, p.51). The BBK guidance encourages the use of supplementary expertise from scientists, economists and other subject matter expertise, through "Network Risk Analysis in Federal Agencies" that operates at federal level, and through the equivalent of this network approach at other administrative levels (BBK, 2011, p.21).

Beyond the risk analysis phases, the methodology calls for the evaluation of identified risks to take place "in a dialogue between analysts and politically responsible persons by comparing the identified risks to the desired levels of protection (i.e., the definition to what extent and in what quality the subjects of protection should be protected or to what extent capabilities for crisis management should be provided). Additionally, there will be a discussion needed between public authorities and citizens about risk analysis results and their evaluation. This is a dialogue on legitimating social negotiations" (BBK, 2011, p.46).

Risk analysis

So far, at federal level the following risk analyses have been carried out since 2012: Floods (2012); Extraordinary epidemics (2012); Winter storms (2013); Storm surge (2014); Release of radioactive substances from a nuclear power plant (2015). At present, the risk analysis "Release of chemical substances" is being finished.

The risk analysis methodology first sets out a number of "framework conditions" for successful analysis:

a. The need to address both of the integral elements of risk (likelihood and impact).
b. The need to balance a scientifically sound approach with pragmatism given that uncertainty is one of the determining characteristics of risk.
c. The need for careful documentation of the risk analysis process, to provide an "evidence trail" for the conclusions.

d. The need to consider impact thresholds governing the escalation of risk management from one administrative level to another.
e. The need to consider trans-boundary risks originating in a neighbouring territory and, therefore, to consult neighbour administrations.
f. The need to re-iterate risk analysis over time.
g. The need to distinguish risk analysis from risk evaluation (see above).
h. The need to consider risk analysis as one part of a risk management process that proceeds from establishing the context through risk identification, analysis, evaluation, and risk treatment.

The work process and methodology for the National risk assessment is conducted in the following steps:

1. description of reference area
2. selection of hazard and description of scenario
3. assessment of likelihood
4. assessment of impact
5. visualisation of risk.

Scope

The risk analysis at federal level takes into account major hazards/events that could potentially affect the entire federal territory i.e., that would need to be managed by the Federal Government in a special way within the framework of its responsibility enshrined in the Basic Law. In principal, the risk analysis is of all hazards: technical, man-made, and natural.

The methodology for risk analysis emphasises the importance of defining the geographic scope or "reference area" such as the Federal Republic of Germany, a federal state, an administrative district, or a rural district or a community. If a hazardous event occurs in the chosen reference area, impacts are determined according to the expected consequences. A detailed description of the reference area is compiled as the first step of the risk assessment. This includes information related to the general geography of the reference area (e.g., climate, land use) its population (e.g., number of inhabitants, population density), environment (e.g., protected areas), economy (e.g., economic performance, business tax receipts) and supply (e.g., main infrastructures of electricity and drinking water supply).

The methodology directs its users to include the variables in Table 12.1, which describes the main elements of exposure to risk and therefore help in determining an event's expected impact. These reflect the ultimate aim of Germany's national risk assessment, which is to improve the protection of five national values that are a 'subject of protection' and set out in the Basic Law (people and animals, the economy and environment, vital infrastructure and facilities, and 'Non-material' subjects of protection (e.g., the political system and cultural assets). Decisions to include or exclude a risk from the analyses are based on an estimate of what an event would, in the reasonable worst case scenario, entail for national interests. Risks are identified for analysis on the basis of at least one of these subjects of protection at the national level being exposed and vulnerable to a hazard.

Table 12.1. Description of the reference area

Category	Information	Possible sources of Information
Man	Number of inhabitants	Statistical offices
	Population density	Federal institute for building, Urban and Rural Research
	Number of households	Registry offices
Environment	Protected areas	Federal Agency for Nature Conservation
		Environmental offices
	Agricultural land	Statistical offices
		Offices for agriculture
Economy	Economic performance	Statistical offices
	Business tax receipts	Economic authorities
Supply	Infrastructure of water supply	Economic authorities
		Infrastructure suppliers
	Infrastructure of electricity supply	Economic authorities
		Infrastructure suppliers
	Infrastructure of gas supply	Economic authorities
		Infrastructure suppliers
	Infrastructure of telecommunication supply	Economic authorities
		Infrastructure suppliers
Immaterial	Cultural assets	Authorities for preservation

Source: Adapted from: BBK (2011)

Hazard identification and analysis

The second step of the risk analysis process defines the type of hazard for which risk is assessed and develops a risk scenario. The so-called "Joint Hazard Estimation" is provided as a reference to identify hazards (infectious diseases, various types of extreme weather, disruptions of critical infrastructure, earthquakes, wildfires and the release of hazardous substances), and the Working Committee develops a risk scenario describing the event in detail to provide a basis for the assessment of likelihood and impact.

The scenario parameters should describe the type of hazard, its spatial dimension, intensity and the duration of the expected incident. To help ensure the design of realistic scenarios, any scientifically proved assumptions/prognoses about the expected intensity of a hazard that are already available should be used in the scenario. The justification concerning the selection of the scenario parameters is meant to be documented. Annex 12.A2 provides examples of parameters and central questions used for designing an appropriate scenario.

The usual units of measurement of the intensity of events that can be measured are applied (e. g. Richter scale Magnitude 6). But, where there is no usual unit of measurement and a qualitative description is necessary, reference to real incidents is recommended in order to allow third parties to understand the assumptions and to make the further analysis more illustrative (e.g., "Release of hazardous substances on 12 December 00 in the city of XY") (BBK, 2011, p. 25). The guidance is silent on whether the scenarios are best case, worst case or "reasonable worst case", but this is implied in the Joint Hazard Estimation and in the selection of the scenario by the Working

Committee. An example is the scenario description given in the 2013 report to the German Parliament (Deutscher Bundestag, 2013, p.30) for the risk of a severe winter storm impacting at the national level:

"This scenario describes an extraordinarily severe winter storm situation. In the frontal zone vectored from the North Atlantic between 45° und 55° N over Germany to East Europe a very intense low pressure system develops, which coming from the westerly direction with its centre over the North Sea moves away to the east. In this process the storm and low pressure field meet at the southern flank of the cyclone, almost covering Germany entirely. A quick subsequent secondary depression intensifies into a storm front over the East Atlantic and moves with its centre from the western exit of the English Channel, temporarily intensifying further, eastwards via North Germany. South Germany is in full grip of a storm and hurricane field on the southern side of the cyclonic storm approximately a day after the previous storm."

Vulnerability and impact analysis

The negative impacts, or damage, of the risk scenarios are meant to be assessed according to a two-step process: the selection of "damage parameters" and "threshold values" that help to classify impacts related to each parameter so that they are comparable across different types of risks. The BKK methodology presents a selection of damage parameters to carry out a risk assessment on a five point scale from A to E in Table 12.2. Table 12.3 shows as an example, what the threshold values are for livestock impairment.

Table 12.2. Example: 2013 Impact Assessment for "Winter Storm"

Subject of protection		Damage parameter	Impact				
			A	B	C	D	E
People	M1	Fatalities	■	■	■	■	
	M2	Injured	■	■	■	■	■
	M3	Persons in need of public aid	■	■	■	■	■
	M4	Persons missed	■				
Environment	U1	Impairment of protected area	■	■	■	■	
	U2	Impairment of water bodies	■	■			
	U3	Impairment of forests	■	■	■	■	■
	U4	Impairment of agricultural land	■				
	U5	Impairment of livestock	■	■	■	■	■
Economy	V1	Impact of public administration	■	■	■	■	
	V2	Impact on private economy	■	■	■		
	V3	Impact on private households	■	■	■		
Immaterial	I1	Impact on public order & safety	■	■	■	■	■
	I2	Political implications	■	■	■	■	■
	I3	Psychological implications	■				
	I4	Damage to cultural assets	■	■	■	■	■

Source: Adapted from BBK (2011).

Table 12.3. Example: Threshold values for livestock impairment

Damage parameter: Impairment of livestock (U_5)
Extent of damage-types: A: ≤ 1,500 animal units impaired B: > 1,500 - 15,000 animal units impaired C: > 15,000 - 150,000 animal units impaired D: > 150,000 - 1.5 million animal units impaired E: > 1.5 million animal units impaired

Source: BBK (2011).

Likelihood and plausibility analysis

The likelihood of risk scenarios is determined using a five-step scale ranging from 1 (“very unlikely”) to 5 (“very likely”), and a corresponding statistical likelihood is assigned. Table 12.4 shows an example of a risk scenario classification. The hazard specific working group identifies a reasonable worst case scenario and the likelihood of the event is assessed according to a logarithmic scale in which an event that is likely to take place at least once in ten years is regarded as very likely. In addition, the lowest scale of likelihood is accorded to events that take place once in more than 10,000 years. Using the logarithmic scale reflects the degree of uncertainty attending some risks, by according them an "order of magnitude" in likelihood. If there is no objective evidence of the return period of particular risks, the alternative qualitative method of describing risks as "very likely", likely etc. is recommended to users and a correlation is assumed which preserves the advantage of the logarithmic scale.

BBK does not consider it useful to attempt a forward projection of risk, but rather calculates a current probability expressed as a return period for risks. The reasoning behind the likelihood assessment is meant to be documented in order facilitate the retracing and/or adaptation of the assumptions, if the analysis is updated/checked (Deutscher Bundestag, 2013, p.28).

Table 12.4. Likelihood scales

Value	Classification	per year	1x in … year
5	very likely	≤ 0.1	10
4	likely	≤ 0.01	100
3	likely to a limited extent	≤ 0.001	1 000
2	unlikely	≤ 0.0001	10 000
1	very unlikely	≤ 0.00001	100 000

Source: BBK (2011).

Time horizon

BBK considers it unnecessary to establish a time horizon beyond which risk scenarios will not be considered for inclusion in the National Risk Assessment. It considers that the likelihood assessment that any risk scenario will occur within one year is sufficient to cover this methodological step that is followed by many countries.

Uncertainty

The risk analysis methodology is premised on recognition that the level of knowledge about hazards and vulnerabilities is persistently insufficient. Assumptions on which decisions and analyses are based can be questioned, and can become outdated over time. The methodology does not provide any structured approach to take account of such uncertainty in the analyses, but rather prescribes (the majority) of society to decide the extent to which it can live with uncertainty at the moment. It directs users of the methodology to clearly state which results are verified and reliable. These caveats are meant to warn that that absolute certainty cannot be guaranteed, and citizens should undertake precautionary preparedness measures.

Updating the National Risk Assessment

No information was collected during the interview with BBK about the frequency or plans update the results of the National risk assessment. There is also no mention of the regularity of NRAs in the annual report to the parliament. The BBK does stress, however, the importance of conducting NRAs for multiple hazard types for future projects to the parliament; a point discussed in further detail in section 4.4.

Communicating the results of National Risk Assessment

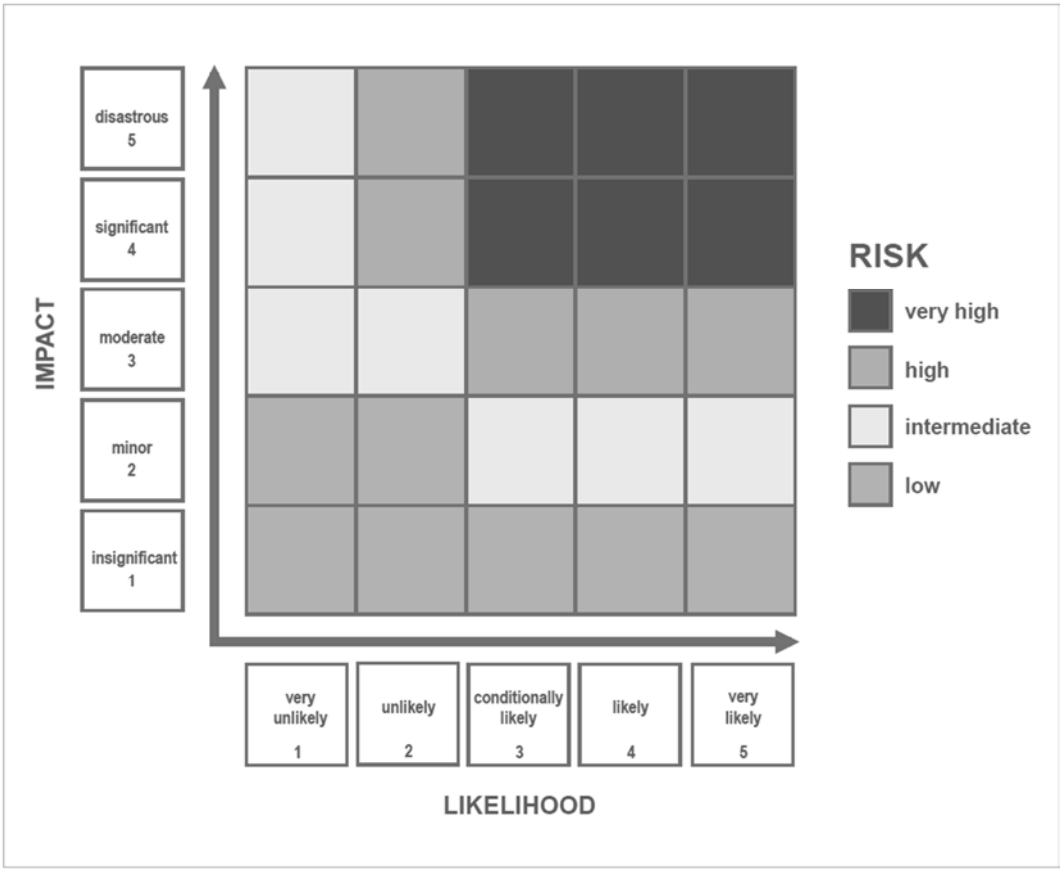
Using the National Risk Assessment to raise awareness about risks

The results of the risk analysis serve to raise awareness about risks and capabilities amongst public authorities and the participants in the process. According to Section 18 subsection 1 sentence 1 of the Federal Civil Protection and Disaster Assistance Act (Zivilschutz- und Katastrophenhilfegetz, 2009) The Federal Ministry of the Interior reports annually about the results of the latest risk analysis and the latest developments in risk analysis at international, national and federal state level to the German Federal Parliament (Deutscher Bundestag, 2012-2015). These reports (to which the risk analysis are normally attached) are published and are accessible to the public (Deutscher Bundestag, 2012-2015).

Tools for interpreting risk analysis

The results of the NRA can be visualised with a risk matrix, which depicts the risk scenario as a point determined by the factors “likelihood” and “impact”. According to the BKK methodology, this information “can serve as decisions basis in risk management, emergency planning and crisis management, including the prioritisation of measures for the minimisation of risks as well as the preparation for inevitable incidents and their handling” (BBK, 2011, p. 40). However, BKK does not intend to use the risk matrix at this point as a tool to aid in decisions about prioritisation.

Figure 12.1 Assessing likelihood and impact of risks



Main lessons learnt and policy outcomes

Lessons learnt

At the time of interviews, Germany had completed work on three risk scenarios, but expected shortly to conclude a fourth, on the risk of a “Storm Surge”. Although BBK has not completed enough scenario analyses to describe a comprehensive "risk profile" for Germany, the first attempts to analyse risk scenarios have helped it to identify key factors driving societal vulnerability in the future, namely: demographic changes and in particular the uneven distribution of elderly citizens; and urbanisation, with young people in particular leaving rural communities for jobs in cities.

BBK considers geo-coded information to be potentially useful for risk assessment and for civil protection preparedness planning. Risk maps that describe the social and economic vulnerabilities present in geographic locations would enhance future NRA, as will the law on access to geocoded information under the European Inspire initiative.

Benefits

The German civil protection system is considered to be efficient and well integrated and to have proved its worth. But the German government believes that the country may be faced by risks that would prove challenging. The NRA system (encompassing distinct processes of risk analysis and evaluation; and supporting effective inter-connectivity

between different levels of administration each with its own competence in law) is a work in progress, but has produced several intermediate benefits so far, including:

- Enabling a cross-disciplinary approach to understanding risks by bringing together all agencies with an interest in risk analysis. This includes engagement of the private sector in the risk analysis, which is helpful to gauge impacts of civil contingencies on the economy, and improved knowledge of risks is the enhancement of understanding damage monitoring and damage analysis (Deutscher Bundestag, 2012).
- Achieving consensus on what the reasonable worst case risk scenarios facing Germany are.
- Raising awareness at all levels of government (parliamentary; Federal government ministers and a wide range of civil servants).
- Leveraging the results in the design of crisis simulations/exercises, and using the risk maps that informed part of the risk analysis process to prioritise areas for emergency protective measures during flooding events.
- Providing insights for other security related initiatives such as the national strategy of critical infrastructure protection or the strategy to climate change adaptation (Deutscher Bundestag, 2012), and to international platforms aimed at enhancing information exchange.

Further benefits expected from the NRA should be expected as the process initiated in 2006 reaches a conclusion, enabling the German government to answer the two questions set out in the 2013 report to the Bundestag:

- What are the hazards/incidents that Germany has to reckon within Germany (by implication involving the federal Government level)?
- Is the German civil protection system adequately prepared for these contingencies?

Given the impossibility of total mitigation of the risks, this requires an understanding of the tolerability of the residual risk after measures have been taken and a setting of "protection goals" reflecting what is factually and politically feasible (Deutscher Bundestag, 2013). This suggests the need for a strategic-level audit of resilience capabilities of the government, reflecting the joint sharing of responsibility for national emergencies between the federal and state government levels agreed in 2002.

Limits

Among the challenges encountered in conducting the National risk assessment is the need to balance the practicability of analysis with the reliability of its results. There seems to be a trade-off between the resource requirements for detailed analyses on the one hand and an undesirable level of residual uncertainty on the other when analysis is less than thorough. This trade-off raises the issue of the availability of resources for conducting an NRA and the difficulty of engaging the expertise found in departments and agencies on a continual basis.

In addition, BBK found that it lacked data with regard to critical infrastructure and economic loss assessments, which required it to rely heavily on expert appraisals. BBK suggests close cooperation with critical infrastructure operators and private enterprises to

obtain more concrete information for future risk assessments. It also found the geocoded data available provided an insufficient level of granularity as protection values could not be viewed at a more detailed level than local municipalities.

With this information, BKK would be in a better position to include the cascade effects of complex disasters in its NRA. BBK hopes to be able to obtain information on a more granular level after the national census data of 2011 are entered into the relevant data bases.

Policy inputs and outcomes

The BBK submitted its report on risk analysis in civil protection to the Bundestag in 2013. It includes a detailed overview of two risk scenarios: extreme floods due to snow pack melting in low level mountains, a pandemic due to a SARS-like virus. It is not clear whether the Bundestag has used this information for any decision in particular, but it has been observed that political debates have referred to it to argue for more resources for the civil protection services. It acknowledged the importance and timeliness of NRA and sees the BBK report as seminal for its own work as a legislative body. The parliamentary report by BBK stresses the importance of making NRA a regular activity, with close horizontal as well as vertical cooperation within the government, and states that national risk management would benefit also complementary NRA conducted by the federal states in close cooperation with the central government (Deutscher Bundestag, 2012).

Notes

1. http://www.gesetze-im-internet.de/zsg/

2. Federal Institute for Materials Research and Testing, Federal Office for Building and Regional Planning, Federal Office of Civil Protection and Disaster Assistance, Federal Office for Goods Transport, Federal Agency for Nature Conservation, German Maritime and Hydrographic Agency, Federal Office for Information Security, Federal Agency for Public Safety Digital Radio, German Federal Institute of Hydrology, Federal Institute for Real Estate, Federal Institute for Agriculture and Nutrition, Federal Highway Research Institute, Federal Federal Agency for Technical Relief, Federal Institute for Risk Assessment, Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway, Federal Police, Deutsche Bundesbank, DFS Deutsche Flugsicherung GmbH, Federal Railway Authority, Johann Heinrich von Thünen- Institute, Federal Aviation Office, Robert Koch-Institute, Federal Environment Agency, Bundeswehr Geoinformation Office.

References

Federal Office of Civil Protection and Disaster Assistance (BBK) (2011), Section II.1 – "General Policy Issues of Civil Protection, Risk Management, Emergency Preparedness", Provinzialstraße 93, D-53127 Bonn. Available at: http://www.bbk.bund.de/SharedDocs/Downloads/BBK/EN/booklets_leaflets/Method_of_%20Risk_Analysis.pdf?__blob=publicationFile

Federal Office of Civil Protection and Disaster Assistance (BBK) (2015), Risk Analysis for Civil Protection A stress test for general hazard prevention and disaster management. Available at: http://www.kritis.bund.de/SharedDocs/Downloads/BBK/EN/booklets_leaflets/Praxis-BS_Bd16_RiskAnalysis.pdf;jsessionid=A02B438D0847C4305C6EE5D8A8682498.1_cid330?__blob=publicationFile

Deutscher Bundestag (2012), Drucksache 17/12051, Bericht zur Risikoanalyse im Bevölkerungsschutz. Available at: http://dipbt.bundestag.de/dip21/btd/17/120/1712051.pdf

Deutscher Bundestag (2013), Drucksache 18/208, Bericht zur Risikoanalyse im Bevölkerungsschutz. Available at: http://dip21.bundestag.de/dip21/btd/18/002/1800208.pdf

Deutscher Bundestag (2014), Drucksache 18/3682, Bericht zur Risikoanalyse im Bevölkerungsschutz. Available at: http://dip21.bundestag.de/dip21/btd/18/036/1803682.pdf

Deutscher Bundestag (2015), Drucksache 18/7209, Bericht zur Risikoanalyse im Bevölkerungsschutz. Available at: http://dip21.bundestag.de/dip21/btd/18/072/1807209.pdf

Further reading

ISO31000 and ISO 31010

Standing Conference of the Minister and Senators for Internal Affairs agreed in 2002.

Risikoanalyse im Bevölkerungsschutz – Ein Stresstest für die Allgemeine Gefahrenabwehr und den Katastrophenschutz, Bd. 16 Reihe, Praxis im Bevölkerungsschutz, Bundesamt für Bevölkerungsschutz u.

Katastrophenhilfe (Hrsg), Bonn 2015.

Annex 12.A.1 Terms in Use in the German NRA process

Terms	Definitions
"Event"	The spatial and temporal conjunction of subject of protection and a hazard.
"Hazard"	A condition, circumstance or process that can result in damage to a subject of protection.
"Risk	A measure for the likelihood of a particular damage to a subject of protection under consideration of the '*potential damage extent'* [sic].
"Risk analysis"	Systematic procedure to determine the likelihood of … damage to a certain subject of protection under consideration of the potential damage extent [sic].
"Risk evaluation"	Procedure to: (1) ascertain the extent to which a previously defined protection goal will be achieved in case of a certain event; (2) decide which remaining risk is acceptable and (3) decide whether measures for mitigation can/have to be taken.
"Risk management"	Continuously ongoing systematic procedure for the goal-oriented treatment of risks including analysis and evaluation of risks as well as planning and implementation of measures for risk mitigation/-minimisation and risk acceptance.
"Damage"	Negatively perceived consequence of an event to a subject of protection.
"Subject of protection"	Anything that is to be protected from damage due to its ideal or material value.
"Protection aim"	The aspired condition of protected property which has to be maintained when an incident happens.
"Scenario"	An assumed possible event or sequences of events and their effects on subjects of protection.
"Vulnerability"	A measure for a subject of protection's assumable [sic] susceptibility to damage with regard to a particular event.

Source: Adapted from BBK (2011)

Annex 12.A2. Parameter and central questions for the description of risk scenarios

Parameter	Central Question
Hazard	Which type of hazardous event is considered?
Scene of occurrence	Where does the event take place?
Spatial dimension	Which area is affected by the event?
Intensity	How strong is the event?
Time	When does the event take place? (Time of year/time of day. If applicable)
Duration	How long does the event and its direct impact last?
Development	How does the event evolve?
Notice time for warning	Is the event expected? Is the population able to prepare for the event? Are public authorities able to prepare for the event?
Who is affected	Which subjects of protection are affected by the event? (persons, environment, objects etc.)
Reference incidents	Have there been comparable events in the past?
Further information	How well prepared are the responsible authorities/relief units/helpers? Findings concerning the damage susceptibility and/or robustness of the affected persons/elements. What else is important for the scenario but has not yet been gathered?

Source: BBK (2011).

Chapter 13. HUNGARY

Hungary began the process of disaster risk identification by carrying out an initial pilot in 2011 and as a result followed on by completing a National Disaster Risk Assessment (NRA) in 2014. One of the most important aspects of this assessment is the adherence to good practice in its compatibility with European Commission guidance on risk assessment practices and time horizon milestones in adapting to climate change. In respect to governance, a lead agency (National Directorate General for Disaster Management NDGDM) is designated to co-ordinate the process assisted by working groups comprising of subject matter experts. The national risk assessment process is seen as evolving in Hungary with some work still to be completed. This chapter contains an outline of this effort and main lessons and policy outcomes to date.

Key Words: Consistency; Cascading events; Common terminology; Impact of climate change; Societal vulnerabilities; Shared understanding of concepts; Subject matter experts.

Introduction

As of October 2013, Hungary was in the beginning phase of developing its full scale National Risk Assessment. It had conducted a pilot initiative in 2011 that revealed several paths for improvement, and it has been elaborating incrementally upon the initial assessment. In July 2014 Hungary completed the National Disaster Risk Assessment report (hereafter referred to as the NRA). This project specifically aims to be compatible with guidance set-out by the European Commission on the topic (European Commission, 2010). It includes both the assessment of impending risks of emergencies (within a 5 year short term horizon) and a long term (20-25 year) outlook of the challenges for national adaptation to climate change.

A report summarising the process and method of analysis for the NRA presents and documents the methods used for development of risk scenarios that could impact upon national safety and security and how to assess their likelihood and impacts (NDGDM, 2011). It compares the results of worst case risk scenarios developed according to a standard template. The scenarios describe the context and causes of the risk, including climate change factors and causal inks to other risks, chains of events and likely risk outcomes. The threshold qualification for inclusion of a risk is that it affects at least one "societal value" and requires government action to manage it.

Hungary elaborated a risk profile in July 2014 by comparing risks in these areas. This takes into account the possibility of "cascading events" – the triggering of multiple events by the interaction of natural hazards with other societal vulnerabilities. Subsequent developments will focus on operationalising the risk assessment, e.g., to implement a GIS mapping of risks, and leveraging the disaster risk assessment results to support policy making.

Governance framework

The development of a National Disaster Risk Assessment (NRA) is a direct result of Hungary's effort to comply with duties shared by all Member States of the European Union[1], according to which they are required to begin developing national risk assessments, through scenarios for a number of risk factors, to analyse them and to provide the Commission with this evaluation.

The Ministry of Interior takes lead responsibility for the NRA, and within it the National Directorate General for Disaster Management (NDGDM) is the co-ordinating body in accordance with their responsibilities for civil contingencies preparedness, planning and disaster management.

The NDGDM led an Ad Hoc Expert Group on Disaster Risk Assessment, which included three thematic subgroups: a Natural Disaster Working Group, a Man-made (major) Disasters Working Group, and an Intentional Incidents Working Group. The Working groups comprise subject matter experts from ministries, public authorities and research institutes. The groups met every 2-3 weeks to work on their assigned tasks of selecting the individual risks for analysis and describing them. These tasks are performed according to a standard process to ensure the assessments are comparable.

Aims and objectives

Hungary initiated work on its National Risk Assessment during the Hungarian EU Presidency, in response to EU Council conclusions 8068/1/11 of April 2011 on "further developing risk assessment for disaster management within the European Union". The overarching policy objective is to improve safety and security in each of the areas of vital national interest (see “Hazard identification and analysis”).

A final edition of the first NRA was submitted to the European Commission at the end of 2011, but it was deemed incomplete. Subsequently, the Hungarian government decided to revise, fine tune and further improve upon the NRA to satisfy the EU guidelines, in pursuit of access to EU funds for thematic operational programmes in 2014-2020. Such access imposes a so-called ex ante conditionality, which requires conducting a comprehensive disaster risk assessment. Hungary aims to develop an operational programme called Joint Disaster Management Risk Assessment and Preparedness in the Danube Macro-Region (SEERISK)) that promotes climate change adaptation and risk prevention. The NRA under development will therefore cover both a near term (5 year) perspective and a much longer term (20-25 year) forward look taking into account the potential effects of climate change.

A short term objective is to improve the consistency of risk assessment in Hungary and other EU Member states enabling these risk assessments to be more comparable across countries. In the long term the objective is to make an assessment of the impacts of climate change which is, again, broadly comparable with the assessment made by other EU Member States.

Definitions of key terms

The NRA "Methodology and Process" report states that “common terminology and shared understanding of concepts will greatly facilitate consistency and comparability (with NRA conducted by different EU Member states) (NDGDM, 2011, p.4). While it provides only a few specific definitions, it does state that the definitions used in the report comply with those in the ISO 31000 standard[2]. The only specific definition put forward is for "Undesirable incidents/ accidents", which are incidents with negative consequences for fundamental societal values.

The NRA "Methodology and Process" report states that “common terminology and shared understanding of concepts will greatly facilitate consistency and comparability (with NRA conducted by different EU Member states) (NDGDM, 2011, p.4). The paper does provide definitions for some key terms, and further states that the definitions used in the report comply with those in the ISO 31000 standard.[3] Among the specific definitions put forward is for the term "Scenario", which is important given that the NRA incorporates a scenario based approach. A scenario is a detailed and specific description of an undesirable incident/ accident with negative consequences for fundamental societal values.

Transparency and accountability

The National Directorate General for Disaster Management has published an article on its website announcing the initiation of the NRA. The outcome of the NRA has been published on the official website of the Government of Hungary. The process is overseen by the Ministry of the Interior, which can make relevant information available to different government departments upon their request.

Multi-level governance and multi-actor participation

The National risk assessment process involves many different actors from more than 20 institutions and authorities including the insurance industry, external consultants, multiple scientific research institutions as well as several national ministries.

The NRA process is designed to take into account the fact that threats to safety and security are changing and increasingly interconnected. "Relatively simple threats can lead to societal disruption due to increasing dependencies. Consequently, a response to existing and new threats is harder to formulate and implement by a single ministry or organisation" (NDGDM, 2011, p.12). The National Directorate for Disaster Management, the Ministry of Interior and Ministry of National Development pay attention to ensure a cross-sectorial perspective.

In Hungary the mayors and local disaster management committees have competence to intervene in emergency management. A Government Decree[4] requires every local municipality to perform a disaster risk assessment and, eventually, to classify risk exposure on a three-point scale. According to the National Directorate General for Disaster Management, all the municipalities have implemented the provisions of the Decree.

Risk analysis

There are three stages in the process to conduct a National disaster risk assessment: definition of societal values; the identification of threats and risks; and execution of risk analysis (NDGDM, 2011, p.9).

Scope

The scope of risks included in the National risk assessment comprises three main categories: natural incidents, major accidents and intentional incidents. This all-hazards approach to risk assessment supports the effort to conduct multi-risk analysis and to consider knock-on effects, as the occurrence of one hazardous event may trigger the occurrence of a different type of event. The addition of such knock-on events to the scope of the NRA is novel, and merits some description in its own right:

> The likelihood of the knock-on event is assessed with reference first to the likelihood of preceding trigger event. The assessment of consequences then considers the cumulative impact of all the various impacts occurring at the same time or shortly following each other. In this way the frequency of the multi-risk scenario was determined by the arithmetic sum of the triggering events and/ or triggering scenarios. In the framework of this analysis only one step multi-risk effect is taken into account, which means that only the direct causal events (first order triggered events) are considered. Second order multi-risk analysis are considered to require a more complicated assessment method and specific analysis software (NDGDM, 2011, p. 47).

Hazard identification and analysis

The starting point for analysis is identification of events or situations that could threaten any one of five vital national interests, or societal values, in such a way that there is potential for societal disruption. The so-called modified Preliminary Hazard Assessment tool (PHA) is used to filter insignificant and/ or local hazards from further

consideration and to focus resources on the analysis of those risks that affect one of the five following societal values:

1 human- compromised by loss of human life and health
2 nature/ Environment
3 finance/ Economy
4 stability of society
5 ability to govern and territorial control.

Since the range of severity of hazardous events that pose risks are too numerous to analyse in detail, scenario development follows guidance that they should be designed according to a "realistic worst-case scenarios" (serious, but credible). The general scenario description gives factual supporting information, including: context/casual connections; progress/evolution of the events, occurrences; potential consequence (impact) areas; potential domino effects to support the multi-risk approach (NDGDM, 2011, p.15-16).

Before selecting a general scenario for further analysis, a determination is made whether government action would be required and at least one of the societal values would be impacted. Each hazard type has been investigated with its associated risk scenario from a so-called "triggering" perspective, that identifies the mechanism and routes (processes, events, failures) that initiate the scenario. The PHA tool takes into account the possible future effects of climate change, and attempts to reflect the possibility of cascading (or domino) effects. Hungary has provisionally identified twelve risk areas upon which to build associated risk scenarios for assessment:

1 extreme weather
2 flooding
3 geological hazards
4 epidemics
5 space weather
6 hazardous substances
7 traffic accidents
8 nuclear accidents
9 terrorism
10 cyber attack
11 security policy crisis
12 energy supply deficiency.

Vulnerability and impact analysis

The risk scenarios are assessed for impacts upon the 5 societal values (Life and health, Nature and Environment, Finance/Economy, Stability of society, and Ability to govern and territorial control), according to eight impact criteria:

- deaths
- illness and injuries
- long term damage to nature and the environment
- financial and material losses

- social unrest
- disturbance to daily life
- weakened national ability to govern
- weakened control of territory.

Each impact criteria is assessed according to specified thresholds (NDGDM, 2011, p.25-28), and graded from A (limited consequences) to E (catastrophic consequences). The scoring thresholds for the impact criteria "deaths" and "injuries" were formulated in accordance with observed practice in Hungary.5 The other impact thresholds substantially use the Dutch interval values (NDGDM, 2011, p.24). In addition, to aid accurate scoring in scenarios where critical infrastructure might be affected, a detailed checklist is provided to assess the impact criteria "Financial and material losses" and "Disturbance to daily life" (NDGDM, 2011, p.30).

To derive an aggregate, or overall, impact score that reflects the scores for each impact criteria, two different approaches to weighing criteria are followed. First, is to give equal weight to each criteria, i.e., each of the eight impact criteria scores is given 0,125 weight in the overall impact score. The second approach is to assign different weights to different criteria. This flexibility enables some quasi-sensitivity analysis that could prove informative to discern whether intangible values (such as environmental quality and cultural assets) are attributed more, or less, importance than is desired.

Likelihood and plausibility analysis

Likelihood is expressed as the probability of occurrence of the risk scenario occurring within five years. Like the impact assessment, it is also measured on a scale from very unlikely to very likely (represented by scores of A to E in Table 13.1). Threats are measured in a different fashion from hazards because of the human factors involved. In assessments both of likelihood and impact the scales are logarithmic, facilitating clear ("order of magnitude") differences to be shown between risks on both axes. The interval between each of the five categories is a factor of ten.

Table 13.1. Likelihood categories for hazards

Category	% per 5 years		Quantitative (%)	Qualitative description
A	<0.05	A-low A-medium A-high	<0.005 0.005 – 0.02 0.02 – 0.05	Very unlikely
B	0.05- 0.5	B -low B-medium B-high	0.05 – 0.1 0.1 – 0.25 0.25 – 0.5	Unlikely
C	0.5- 5	C-low C-medium C-high	0.5 – 1 1 – 2.5 2.5 – 5	Possible
D	5- 50	D-low D-medium D-high	5 - 10 10- 25 25- 50	Likely
E	50-100	E	50-100	Very likely

Source: Report on Hungary's National Disaster Risk Assessment. Methodology and its Results (2014)

Likelihood of occurrence for threat scenarios is referred to as plausibility assessment, and its determination is based on the available knowledge and data from competent organisations about the capacity to act and the likely success of an intentional act, e.g., a terrorist attack. There are two components to this analysis: the likelihood that a specific threat leads to an attack, which is determined by the type of threat and the capabilities and intentions of the attacker; and the likelihood that the attack will be successful due to the vulnerability of the targets. Specific guidance in the NRA methodology is provided for the determination of vulnerability (NDGDM, 2011, p.38-39). In addition, separate tools are used for the assessment of likelihood for risk scenarios related to climate change (NDGDM, 2011, p.42).

Time horizon

The risk scenarios selected for assessment are a combination of events that could occur within the next 5 years as well as emergencies that could occur within the next 20-25 years when taking into consideration the national challenges that could arise due to climate change.

Uncertainty

The NRA methodology accounts for uncertainty through likelihood assessments. Estimates of likelihood for a risk scenario are assigned a lower, upper and expected value using available quantitative data (e.g., incident data, failure data, probability design data and climatological data). There are at least two elements that compose the likelihood of a hazard scenario; the probability of occurrence of the hazard and the likelihood that the hazard will result in the impacts described. Upper and lower limit likelihoods are assessed by looking at the greatest deviation from the forecast value.

Updating the National Risk Assessment

Hungary is undertaking the assessment of likelihood and impacts for the first time. Plans for reassessment and review will be developed at a later stage in the process.

The validity of NRA results is supported by a review or cross-check process, which is conducted by subject matter experts involved in the process. This measure is meant to control for a bias in view or hidden agenda amongst any of the participating experts.

Communicating the results of National Risk Assessment

Using the National Risk Assessment to raise awareness about risks

The intention is to report and interpret the results of the NRA within government and the working group participants. Extracts of the results of NRA analysis are supposed to feed into this report that describes the risk assessment process, its methodology, the supporting literature and software used. The report will include production of a "risk diagram" that indicates the risk scenarios with relatively high likelihood and impact (see Tools for interpreting risk analysis). Much of the underlying data and information used in the NRA is sensitive or classified, and therefore there is no plan to make them publicly available.

Tools for interpreting risk analysis

Three risk diagrams will be produced to visually illustrate and help interpret the results of the assessments of the risk scenarios. The risk diagram will represent the results

of analysing the risk scenarios as a plotted dot representing its relative impact (vertical axis) and likelihood of occurrence (horizontal axis), adjusted to the logarithmic (ln-ln) structure of the diagram (NDGDM, 2011, p.49). It will contain 5 vertical rows denominated from A (lowest impact) to E (highest impact), and 5 horizontal columns denominated as "very unlikely" on the far left to "very likely" on the far right.

The difference between the three diagrams (basic, uncertainty, sensitivity) resides in how each portrays the results of the scenario analysis. The basic diagram assigns equal weight to the eight impact criteria and points representing the scenarios. The uncertainty diagram presents the points on the matrix with uncertainty bounds for both impact and likelihood. The sensitivity diagram depicts the points representing the results of the scenario analysis with defined weightings for each of the eight impact criteria.

The risk diagram provides a general indication of the relative likelihood and impact of the risk scenarios. The National Directorate General for Disaster Management does not consider it possible to represent an exact comparison due to the nature of the risks contained within each grouping related to the identified risk area, but only to give an idea of the position of each group of risks relative to each other.

Main lessons learnt and policy outcomes

Lessons learnt

The National Directorate General for Disaster Management identified several lessons identified in the course of the work carried out so far:

- The need for sustained collaboration of experts from a wide range of disciplines.
- The need for sustained cross-government collaboration.
- The need therefore for a permanent risk assessment machinery – the Ad Hoc Experts Group is to be transformed into a permanent Risk Assessment Steering Committee in the future. It will produce recommendations regularly for decision makers and also reviews and updates of the NRA framework.

Benefits

In advance of the first full NRA, Hungary has nevertheless been able to use data on the risk of flooding of the Danube to assist in prioritising the national response to such flooding in 2011-2013. The benefits of derived from this work so far have included:

- Raising awareness of national risks throughout the government.
- Initiation of cross-departmental cooperation, in particular among subject-matter experts, and the use of cross-disciplinary approaches in risk analysis.

Limits

The National Directorate General for Disaster Management identified several challenges for the NRA going forward, including the following:

- The difficulty to frame the outcomes of the risk assessment process into policy recommendations that can be understood by non-experts.
- The communication of risk and risk assessment to design strategies and policies to mitigate risks.
- Resource limitations (e.g., the availability of experts and financial funds to conduct risk assessment, on a sustainable basis).

Policy inputs and outcomes

The outcome of the first full NRA in 2014 will be used to inform a programme for the financial period 2014-2020 to operationalise risk assessment at local level, to use GIS applications to map risks and integrate the concept into spatial planning and disaster risk preparedness. This will require legislative change and changes to the organisational code of conduct of the NDGDM.

Notes

1. Conclusion No. 8068/1/11 of the Council as of April 7, 2011, on "the further development of the disaster risk assessment in the European Union

2. See: ISO 31000:2009, Risk management – Principles and guidelines and ISO Guide 73:2009, Risk management – Vocabulary.

3. See: ISO 31000:2009, Risk management – Principles and guidelines and ISO Guide 73:2009, Risk management – Vocabulary.

4. Decree 234/2011.

5. Decree 219/2011.

References

European Commission (2010), Staff Working Paper: Risk Assessment and Mapping Guidelines for Disaster Management SEC 1626, Brussels.

National Directorate General for Disaster Management (NDGDM) (2011), "National Disaster Risk Assessment Framework and Strategy, Hungary: Methodology and Process of the National Risk Assessment", unpublished.

European Council (2011), Conclusion No. 8068/1/11 of the Council as of April 7, 2011, on *"The further development of the disaster risk assessment in the European Union"*.

Further reading

ISO 31000:2009, Risk management – Principles and guidelines and ISO Guide 73:2009, Risk management – Vocabulary.

Government Decree 234/2011 passed in October 2011

Government Decree 219/2011 on control and prevention of major accident hazards involving dangerous substances.

(2014), Report on Hungary's National Disaster Risk Assessment. Methodology and its Results

Chapter 14. KOREA

This chapter on Korea reflects information gathered from an OECD workshop held in Seoul on a National Risk Assessment Process. The information was updated following the Sewol Ferry accident in 2014 and the subsequent re-structuring of Korea's crisis management system. Since 2016, Korea has been developing relevant institutional framework to introduce NRA and preparing risk analysis tools, such as risk assessment techniques for implementing the scenario-based NRA and scenario-based disaster models. The chapter also provides a brief outline of the National Disaster Management System (NDMS,) which is an information management support system used to manage crisis preparedness and response in Korea. There is substantial effort to communicate information on risk and the warning of potential disasters to the public, which support some of the same operational purposes as National Risk Assessments.

Key Words: Administrative re-structuring; National consensus; National Disaster Management System; Outreach programmes; Risk communications; Technical capacities;

Introduction

In April 2013 the OECD held a workshop on National Risk Assessment (NRA) At the time of the workshop, the Korean government was considering whether to set-up a multi-hazard, national risk assessment drawing on the risk assessments, data and research already produced by line ministries and responsible government departments, agencies and research institutes. The workshop convened several major public bodies with expertise in risk assessment to consider how their individual parts could be co-ordinated into a comprehensive whole that would use a consistent methodology to compare different types of emergency risks. Government officials from the following ministries and agencies presented their roles in conducting risk assessments: Ministry of Security and Public Administration, the National Emergency Management Agency, the National Police Agency, the Ministry of Environment, the Ministry of Science, Information and Communication Technology and Future Planning, the Ministry of Agriculture, Food and Rural Affairs, and the Ministry of Health and Welfare. The risk assessment presented ranged from those associated with natural hazards, social unrest, disruptions to infrastructure, cyber-attacks, and human or animal diseases.

The workshop presented examples of NRA from different countries where this approach has proven to be a useful support for setting priorities in civil contingency planning. At the time of compiling this information, no decision had been taken on whether to implement such a national risk assessment in Korea. This summary reflects information that the participants provided to OECD about various risk assessments conducted across government departments at the time of the workshop, including floods, typhoon, landslides, industrial accidents and infectious disease outbreaks. Some sections of this summary have been updated with more recent information following the Sewol Ferry crisis in 2014, which precipitated a re-structuring of Korea's crisis management system.

Governance framework

At the time of the OECD workshop, the National Emergency Agency (NEMA) had direct responsibility for natural and human induced disasters, whereas the Ministry of Security and Public Administration had direct responsibility for social disasters. Responsibility for assessing these types of risks was therefore administratively separated. Following the ferry crisis, the Ministry of Public Safety and Security was established as the primary organisation at the national government level with responsibility for crisis management.[1] NEMA, the Korean Coast Guard and the safety branch of the Ministry of Security and Public Administration (MOPAS) were merged under its authority, as part of this administrative restructuring. In 2017, Korea carried out another reshuffle in order to foster the disaster and safety management system in the wake of the inauguration of the new government. As a result, the Ministry of Public Safety and Security (MPSS) and the Ministry of Interior were merged into the Ministry of the Interior and Safety (MOIS). Through such restructuring, the Korea Coast Guard and the National Fire Agency became independent government agencies.

While there is currently no NRA in Korea, the various line ministries present at the OECD workshop displayed the technical capacities to identify and assess the risk of major disasters. Korea conceives of these risks under three broad incident types: 1)

natural disasters (e.g., typhoon, flood, torrential rain, high wind, tsunami, storms, earthquakes, landslides, etc.), human induced disasters (fire infrastructure collapse, traffic accidents, chemical spills) and social disasters (e.g., disruptions to critical infrastructure networks such as energy, transportation, telecommunication, medical, and human or animal diseases).

The strong technical capacities of public bodies for risk assessment are enhanced through the National Disaster Management System (NDMS). This information collection and management tool for natural hazards, human induced disasters and social disasters, connects numerous government departments at central and regional levels as well as cities. Information on natural hazards in particular, such as typhoon, heavy rainfall, flood, wind storm, drought, heavy snow, extreme temperature, earthquake, land slide, tsunami, wild fire, storm surge and yellow dust are integrated into a web based system to support government decision making. The information on exposures to natural hazards are used to draw-up local and provincial hazard maps, which help to inform the design of evacuation plans, government compensation following disaster declarations and the determination of flood insurance rates.

Aims and objectives

As discussed with Korean officials in the 2013 OECD workshop, the objective of a national risk assessment would be in part to support decisions on the optimal allocation of resources for disaster risk management by comparing different types of risk scenarios according to standardised criteria. Many countries that conduct an all-hazards national risk assessment find that it fosters a "whole-of-government" or "whole-of-society" consensus to civil contingencies planning and enhances community resilience. The potential benefits include:

- Building national consensus on priorities for risk management, in an inherently complex risk environment encompassing threats, natural hazards, and man-made accidents.
- Support for the adoption risk management strategies.
- Informing the objective quantification of risk analyses – both in terms of likelihood and consequence – to aid decisions on investment in capability and capacity.
- Assisting in risk communication to citizens to mobilise self-help preparedness among business and social communities.

Multi-level governance and multi-actor participation

At central government level, within the Ministry of Public Safety and Security, the Special Disaster Management Office (hereinafter SDMO) was established to manage and respond to all disasters, national and international, natural or man-made, including: large-scale environmental pollution, infectious diseases, nuclear energy and major road accidents. It provides professional analytical and technical support to the disaster response capabilities of government departments. The SDMO is also responsible for building partnerships with stakeholders such as domestic and international disaster related private organisations, associations and research institutes. As such it is, in theory, well placed to provide a platform at the central government level for co-ordinating a NRA.

Among the relevant capacities in Korea that could support the realisation of a national risk assessment is the NDMS, which includes information support systems at central and

local levels of government to take actions for the preparedness and response both to natural and human-made disasters. The NDMS is jointly operated by the national government, local governments, and related authorities. It is a nationwide information system put in place to promptly respond to emergency situations and to support recovery and restoration.

The NDMS consists of a web based central system at the NEMA and local systems that are installed in 16 cities and provinces nationwide. The NDMS includes a hazard data collection capability that gathers up-to-date information from a number of sources, including the National Meteorological Administration (NMA) and Flood Control Offices (FCO), which are located at major rivers. Using the database, the NDMS processes and produces relevant data for users in the central government. The local systems are for users in the local governments in 231 cities and provinces nationwide. The NDMS information system would provide much of the raw data needed to develop risk scenarios for a NRA. Such a tool could eventually help inform the design of a disaster risk reduction plan and mitigation programmes for natural hazards such as river and coastal floods, forest fire, landslide, earthquake and tsunami.

Risk analysis

Scope

At the time of the OECD workshop government efforts to assess major risks focused on three categories of risks: natural hazards, human induced disasters and social disasters. Table 14.1 provides an illustrative table of the types of events that belong to each category.

Table 14.1. Typology of disasters in Korea

Natural Disasters	Human Induced Disasters	Social Disasters
Typhoon	Fire	Energy disruption
Flood	Building collapse	Transportation disruption
Torrential rain	Traffic incident	Telecommunication disruption
High wind	Environmental disasters	Infectious disease outbreak
Tsunami		Animal Infectious Disease outbreak
Storms		
Earthquakes		

Source: Ministry of Public Administration and Security (2013)

Hazard identification and analysis

In 2013, the Korean government had not yet considered whether a National Risk Assessment should be based on a comparison of deterministic scenarios (which is the basis for NRA in most OECD countries), or on a probabilistic basis, however. It has been implementing a modified version of NRA for some types of natural disasters, however, and its government departments, agencies and research institutes collectively possess the information and data needed to develop well informed risk scenarios. Korea gradually accepted the necessity of introducing scenario-based and probabilistic-based NRA through workshops with OECD and studies on best practices of other countries. Accordingly, it has been developing NRA analysis tools and models through a series of research projects.

Extensive data has been collected on natural disaster events (Table 14.3), man-made incidents (Table 14.4) and the number of fatalities (Table 14.5). Data has been collected also on hazard exposure and vulnerability that supports disaster risk analysis, including changes in population density, and observed effects of climate change such as changing patterns of rainfall and temperature. Korea also possesses extensive data and information about risks that most OECD countries are not exposed to, for example "yellow dust" events (Box 14.1). Historically flood risk has been the most significant of all risks, especially from typhoons that Korea faces each summer. Information is also collected on the economic losses arising from the main kinds of natural hazards (i.e., typhoon, rainstorm, heavy snow, etc.) and the numbers of fatalities in recent years. Information has been collected on the frequency and damages from human-induced incidents, such as: public transport accidents, forest fire, maritime accidents, gas incidents, oil pollution, cyber-attacks, and the number of animals affected by animal disease.

Box 14.1. Yellow dust storms

Korea is periodically exposed to yellow dust storms that originate from the dry desert regions of China and Mongolia. Low-pressure systems combine with strong winds and cold air fronts to raise dust into the atmosphere and carry it across the continent. The consequences of this trans-border environmental risk range from visibility reduction to a variety of human health problems.

Over the past decade, the yellow dust phenomenon has become a serious problem due to industrial pollutants and intensified desertification in these regions. Table 14.2shows that the phenomenon has impacted Korea up to 15 times a year, lasting up to 25 days in 2010. The socio-economic impact of yellow dust, stemming from increased medical treatment, decreased industrial and agricultural production, complications in aviation transport and product purchase for preventing the damage, were estimated at 0.8% of Korean GDP in 2002 (Jeong 2008). Moreover, yellow dust has negative effects on environmental assets such as water, air, soil and animals.

Source: Ministry of Public Administration and Security (2013)

Table 14.2. Frequency of annual yellow sand

Year	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Frequency	2	6	11	9	13	10	10	15	7	5
Duration (day)	3	14	17	21	22	20	18	25	15	6

Source: Korea Meteorological Administration (national weather forecast system); Jeong, D. Y. (2008). Socio-economic costs from yellow dust damages in South Korea. Transborder Environmental and Natural Resource Management, 185-198.

Table 14.3. Disaster events (2002~2011)

	Economic losses in average during last decade (2002~2011) (M. Won)	Economic losses in average since the establishment of NEMA (2004~2011) (M. Won)
Typhoon	₩1,046,413	₩130,626
Torrential rain	₩464,256	₩442,269
Heavy snow	₩136,761	₩170,952
Others	₩10,883	₩13,604
TOTAL	₩1,658,314	₩757,452

Source: NEMA's Main Statistics issued in June, 2012

Table 14.4. Man-made incidents in a period of 2008~2010

	Man-incurred incidents as of 2010					
Types of incidents	No. of occurrences	Number of casualties				Economic losses (M. Won)
	Total	Subtotal	Death	Injured	Other	
Total	280607	366911	6758	359840	313	₩321,850
Public Transport	226878	357963	5505	352458	NA	NA
Fire	41863	1892	304	1588	NA	₩266,776
Mountain fire	282	2	2	NA	NA	₩4,451
Train	181	177	73	104	NA	₩395
Subway	136	173	62	111	NA	₩138
Explosion	41	65	1	64	NA	₩11
Maritime accidents	1627	153	85	68	NA	₩25,558
Gas	134	206	10	196	NA	₩119
Maritime transport	1	1	1	NA	NA	NA
Pollution (oil leakage)	102	NA	NA	NA	NA	NA
Industrial facilities	22	31	10	21	NA	₩1,414
Mine	34	34	7	27	NA	NA
Electric shocks	585	585	47	538	NA	NA
Elevator accidents	129	176	10	166	NA	NA
Boiler accidents	NA	NA	NA	NA	NA	NA
Air transport accidents	7	2	1	1	NA	₩7,270
Structure collapse	284	168	19	143	6	₩5,197
Waterside accidents	57	58	58	NA	NA	NA
Drowning accidents	2195	800	302	425	73	₩5,209
Climbing	3079	2251	88	2034	129	NA
Falling down	1365	977	104	793	80	₩300
Agricultural machines	645	602	60	541	1	₩3,557
Bicycle	599	335	6	323	6	₩455
Leisure and daily sports	282	235	3	217	15	NA
Playground facilities	79	25	NA	22	3	NA
Amusement parks						NA
Etc.	NA	NA	NA	NA	NA	NA

Source: NEMA's Main Statistics, accessed in June 2012.

Table 14.5. Number of Fatalities (2002~2011)

	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Total	400158	363031	394950	363495	359726	359795	354133	358559	379289	368504	1943
Natural disasters	NA	270	148	14	52	63	17	11	13	14	78
Man-made hazard	400158	360526	391969	361177	357332	357552	351657	355832	376835	366598	NA
Fires*	NA	2235	2833	2304	2342	2180	2459	2716	2441	1892	1865

Note: Fire casualties are already included in the figures of the man-made hazards
Source: Korea Meteorological Administration (national weather forecast system)

Vulnerability and impact analysis

At the time of the OECD workshop the National Emergency Management Agency had put in place several programs aimed at disaster risk reduction, which were informed by vulnerability analyses carried-out at local level. Among these programmes is the "Local Jurisdiction Safety Index", which identifies vulnerability factors at the local level and assesses its safety on a scale of 1-10 in face of natural hazards. This project looks at population density and demographic distribution, the record of disastrous events over the past 10 years, and the magnitude of those events in terms of the hazard exposure, damages, fatalities and injuries.

The Government of Korea has shown capacity to take a longer looking perspective on major risks through its strategic approach to adapt to climate change. The central government set-up a National Government Adaptation Committee (NGAC) composed of the representatives of 13 ministries to implement a National Climate Change Adaptation master Plan, which includes the development of policy tools to support climate change impact, conduct hazard identification and analysis and vulnerability assessments. The Korean Government have designated 13 Government Departments to take responsibility for the ten vulnerable sectors and regions identified due to climate change (see Table 14.6).

If Korea were to put in place a National Risk Assessment it would likely have the information necessary to conduct impact assessments on the basis of:

- Harm to life (measured in numbers of fatalities arising from harmful events over a period of time) and health (numbers being injured or falling ill, over a period of time).
- Disruption of essential services (measured as the extent, intensity and duration of disruption to services provided through national infrastructure).
- Economic damages, whether measured as the cost of damage repairs or as a proportion of gross domestic product (GDP), and possibly.
- Non-material impacts such as a measure of public confidence, an indicator of impacts on reputation of the government or effectiveness of the political system.

Table 14.6. Climate change impact sectors and risk criteria

Climate Change Impact Sectors	Risk Criteria
Health	Protection of the population from Heat waves and Infectious Diseases
Disaster	Minimizing damage through the consolidation of the disaster prevention strategies
Agriculture	Switching to adaption based agricultural systems and new opportunities
Forestry	Improvements of forestry health and a reduction in forest fires
Coastal /Marine Resources	Responding to sea level rise and security in marine resources
Water Resource's	Building secure water management systems from the threat of flood and drought
Biodiversity	Securing biodiversity through restoration and protection
Climate Change Monitoring and Projection	Monitor climate change over time and provide scientific knowledge of climate change projections
Adaptation Industry/Energy Publication	Create new business for adaptation and minimise damages in industry and provide energy stability
Publication Education International Cooperation	Raise public awareness and expand international partnerships for climate change adaptation

Likelihood and plausibility analysis

The OECD workshop on National Risk Assessment presented the trend in many OECD member countries of measuring the likelihood of risk scenarios occurring over the next 5 years on a logarithmic five-point-scale, starting with the most likely ("as likely as not") and proceeding by (generally four or five) orders of magnitude to the least likely (<1/20,000). A more linear approach would be as presented in Table 14.7.

Table 14.7. Measures of likelihood for risk scenarios

Value	Classification	…per year	1x in ….years
5	very likely	≤ 0.1	10
4	likely	≤ 0.01	100
3	likely to a limited extent	≤ 0.001	1000
2	unlikely	≤ 0.0001	10000
1	very unlikely	≤ 0.00001	100000

Source: Authors

Communicating the results of National Risk Assessment

Information sharing

Korea has established numerous initiatives to share information about risk exposures to the public. Individual agencies, such as the National Police Agency, communicate

directly with the public and cooperate with other agencies through outreach programmes, and publicity campaigns at a national level through newspapers, magazines, news programs and various websites. At the time of the OECD workshop in Seoul, this proactive strategy was carried out under the auspices of the disaster emergency management bureau, which also possesses a typhoon warning system through which information is shared with the National Emergency Management Agency, the Ministry of the Environment and the Metrological Office. Another concrete example is the three-tiered warning system managed by the Korean Meteorological Administration and carried by local media:[2]

1. At the lowest level of warning, the elderly, children and people with respiratory issues are advised to stay indoors. Everyone should avoid strenuous physical activity outdoors.

2. At the second warning level, kindergarten and elementary students should also remain indoors, and all strenuous outdoor activity should be avoided. All people should remain indoors if possible.

3. At the highest warning level, the general public is advised to remain indoors. It is recommended that outdoor events be postponed. People who must go outside should wear protective glasses, a mask and long-sleeves.

NEMA utilises commercial telecommunications companies to communicate with the general public by a text alert system. In addition, the Ministry for Health and Welfare uses a number of public information websites to communicate to the public on various areas of concern such as climate change, travel disease, pathogen infection, quarantine, vaccinations and virus surveillance. The MOIS (the then MPSS), since 2014,has put in place a strategy for public communication which includes a publicly available website (http://www.safekorea.go.kr), the use of Blogs, Facebook, Twitter and a broadcasting facility. The public are also encouraged to report threats to safety via the website (http://safepeople.go.kr/) and a mobileapp (Safety e-Report).

Main lessons learnt and policy outcomes

Lessons learnt

The Republic of South Korea has a long history of dealing with large scale disasters, which have led to numerous policy changes and administrative reforms. Since the 2014 reform to vest responsibility for crisis management in one ministry, Korea is better placed to adopt a National Risk Assessment if it commits to a strategic approach to risk assessment that breaks down the silos between technical services. All the technical ingredients are in place for a comprehensive national risk assessment in the overall context given the proliferation of tools for data collection and analysis. What is currently missing is a mandate and leadership willing to co-ordinate a wide range of experts within government and the scientific community in private companies and academia.

Benefits

The benefits of a whole of government approach are numerous and can create an even greater level of protection to citizens than already prevails by virtue of the current system that functions in operational silos. These benefits include optimisation in the allocation of

resources in dealing with the most serious risk that have been identified as affecting the country. Additionally this will lead to the reduction in unpredictability of risks and the identification of the highest risks which may require special treatment by government and experts in this particular subject matter. The adoption of a strategic approach specifically focused on a better strategy for managing risk would provide an objective and systematic evidence base for government-level emergency planners.

The wider benefits of an effective all-encompassing national risk assessment would enable the Korean Government to build on the existing structure in addition to the following wide strategic benefits:

- Build consensus and facilitating cross-cutting collaboration between Departments and agencies,
- Avoid the need for speculation in an unpredictable risk landscape,
- Prioritise risks according to the likelihood,
- Identify the highest risks requiring special programmes of mitigation by the government,
- Adopt strategies for managing and highlighting priority areas for preventive action,
- Communicate accurate information on the risks to those who need to know,
- Provide a basis for horizon-scanning for imminent emergencies, and longer-term strategic assessments of risk trends on a medium to long term basis.

Policy outcomes

A comprehensive national risk assessment could provide crucial support to an effective strategy for the governance of critical risks in Korea. It would draw from existing technical capacities in risk assessment, and provide an overarching framework across different fields of expertise to conduct analyses according to common criteria. This would help to prioritise investments in the mitigation of risks and their consequences and improve overall preparedness and consequence management. This could also support the stated goal in Korea to redirect investment from restoration to prevention or reduction of disaster damages. By engaging the whole of government and the wider stakeholder community, the establishment of a national risk assessment would also likely enhance the support of citizens for policy decisions, and encourage communities and businesses to take greater responsibility for their own safety. Engagement with the private sector in risk assessment would also tend to present the additional advantage of broadening partnerships that are useful to mitigate risks to critical infrastructure.

Notes

1. http://www.mpss.go.kr/en/

2. The Korean Meteorological Administration website, available at: http://www.kma.go.kr/eng/weather/asiandust/intro.jsp;

3. Jeong, Dai-Yeun 2008, "Socio-economic costs from yellow dust damages in South Korea." Transborder Environmental and Natural Resource Management 185-198.

References

Korea Meteorological Administration (national weather forecast system).

Jeong, D. Y. (2008). Socio-economic costs from yellow dust damages in South Korea. Transborder Environmental and Natural Resource Management, 185-198. Available at: http://www.kossrec.org/wp-content/uploads/2015/04/Socio-Economic_Costs_from.pdf

NEMA's Main Statistics issued in June, 2012.

Chapter 15. THE NETHERLANDS

This chapter on the Netherlands outlines how the governance framework functions from a national perspective led by the Ministry of Safety and Justice and through a de-centralised structure involving a myriad of stakeholders. The methodology presented in this chapter has been tried and tested for many years by the Netherlands and the involvement of subject matter experts from the public, private and academic sectors in the NRA process is seen as good practice. This chapter also discusses the methodology for hazard identification, impact analysis and, likelihood and plausibility analysis. The Government subscribes to transparency in the process in both the detailed results and methodology used for the NRA which is under constant review given the changing threat landscape.

Key Words: Collaboration; Capability and capacity building; Cross disciplinary approach; Risk tolerance; Subject matter experts; Social and political stability.

Introduction

The Netherlands has conducted an annual National Risk Assessment (NRA) for many years now – the latest (2014) version is the sixth in a row. The NRA supports development of a cross-government National Safety and Security Strategy, providing an evidence base for determining priorities for risk reduction through prevention and through investment in capabilities for response and recovery. The 6th iteration (NRA 6) of the NRA provides a risk matrix covering 45 risks of all kinds, analysed by a Network of Analysts for National Security on behalf of the National Steering Committee for National Safety and Security. The Netherlands is a pioneer in the use of expertise from the private and academic sectors to carry out NRA analysis. It is also, famously, a country where a 55% of the territory is below sea level or flood prone, and it is acknowledged as a global reference for water management in terms of ensuring protection from floods and freshwater supply: 1.2% of the GNP is invested in prevention and since 1953 there has been no flood disaster (OECD, 2014). Flooding apart, The Netherlands has in recent times enjoyed a relatively benign risk environment

Nevertheless, 2014/2015 have been years of reflection for the Netherlands on what the next steps for national risk assessment should be. Proposals have been made to Parliament to replace the current annual National Risk Assessment with a National Security Profile, to be released every four years from 2016, setting out a comprehensive analysis of the most salient risks and threats to national security and an overview of relevant technological and social developments that are likely to affect those risks in the future. The National Security Profile will complement regional risk profiles, and the two levels of assessment will inform each other.

Governance framework

The Governance Framework for the Netherlands' National Security and Safety Strategy, and for the National Risk Assessment (NRA) that supports it, is set out in a publicly available document called "The Guide" (Leidraad Nationale Veiligheid, 2014), which also explains in considerable detail the methodology used to carry out the NRA. The Guide explains that:

- The Cabinet is responsible for the implementation of the National Safety and Security Strategy.
- The Minister of Security and Justice holds the portfolio, with implementation being carried out in collaboration with other ministries, the Network of Analysts for National Safety and Security, decentralised governmental departments, the business community, knowledge institutions and planning offices.

At the start of the annual cycle of the Strategy for National Safety and Security decisions are made within the interdepartmental Steering Group for National Safety and Security as to which scenarios will be elaborated. The Network of Analysts for National Safety and Security, which comprises a collaboration of knowledge institutions and scientific establishments, is then responsible for the development of the scenarios and assessment of the scenarios. The results of these risk assessments are included in the National Risk Assessment.

Aims and Objectives

The main purpose of the NRA is to provide a consistent evidence base for decisions to be made by the Government on the priorities for and approaches to risk management, and investment in capabilities. For each of the main risks assessed, a capability analysis is carried out and research done into whether the Netherlands has sufficient capacities available (people, machinery, knowledge, skills, agreements) to stand up to the threat and which capacities should be increased. The capability analysis is carried out under the responsibility of the professional area that is most involved, with support from the Ministry of Security and Justice. The process concludes with the compilation of a report for the Cabinet in which proposals are made for increasing capacities, and a decision by the Cabinet decides on the priorities for increasing capabilities and capacities, and responsibilities for this. The results of the National Risk Assessment and the capability analysis are reported annually to Parliament.

In fulfilling this primary aim, the NRA also contributes to the following aims:

- preventing or reducing the risk of hazards occurring
- reducing the effects, through both capability and capacity building
- monitoring risks over time
- communicating risks to others with risk management responsibilities in the public sector but also more generally to stakeholders in the private, public, NGO, and voluntary sectors, and to communities; and alerting the population to imminent threats through the national crisis management website3 promoting an understanding of risk and a risk management culture
- determining risk tolerance levels within government and among other organisations using the NRA
- providing a basis for risk mapping of selected risks (floods, fire, chemical hazards, radiation hazards) which is done mainly by the regions
- assisting identification of cross-boundary risks with neighbouring countries.

Definition of key terms

Comprehensive definitions are given throughout the Guide of what is meant by risk, scenarios, likelihood (of both hazards and the realisation of threats) and impacts (of all the 6 main kinds and the sub-categories within each). As well as definitions, examples are given showing how to interpret the definitions, and giving the format of the various reports contributing to the risk assessment and capability programmes. These are consistent with ISO 31000 and the EC Guidelines, but are much more extensive and detailed.

Transparency and accountability

The arrangements for development, implementation and maintenance of the risk assessment process are set out in exhaustive detail in the Guide. This includes the names and parent organisations of those involved in the method group for the National Safety

3. National crisis management website available at: http://www.crisis.nl/

and Security Steering Group, who compiled the Guide. This unusual degree of openness includes: identification of the organisations participating in the national risk assessment process, their roles, and the documents to which they are expected to refer in varying out their roles, and the extent to which and terms under which some kinds of information are withheld for reasons of cost, privacy, confidentiality and national security.

These arrangements ensure that there is a high degree of consistency and comparability of results in the Netherlands NRA, reinforcing what is reputedly a high degree of trust among the population generally in the competence and reliability of the government in matters of emergency risk management. The use of a Network of Analysts for National Safety and Security, including experts from outside government, is unusual for NRA and helps to counteract criticism – to which countries with less advanced NRA processes are vulnerable – that policy rather than science is being allowed to drive the risk analysis.

Multi-level governance and multi-actor participation

The Netherlands national risk assessment process both feeds and is fed by risk assessment at the regional level. The concept of risk ownership operates both with national government and in the safety/security regions, as well as in communities/cities; and the practice of engaging safety/security regions both in the process of identifying risks and in the Network of Analysts that carries out the development of scenarios and related risk assessment, ensures that the process engages both subject-matter experts and those who have the responsibility for emergency risk management. It also helps, through discussion at the assessment stage, to clarify responsibilities where there are overlapping jurisdictions.

Risk analysis

The Netherlands NRA is an all-hazards risk assessment, which takes into account all risks – of events or developments – that can lead to societal disruption. The assessment is based on scenarios and is both qualitative and quantitative; enabling it to help in the analysis both of the capability needed to manage particular risks or risk types, and of the amounts of capability needed, across the board, to reduce the risks to a level that the Government deems tolerable.

Scope

The Netherlands NRA has grown from 13 risks in 2007 to 46 in 2014. The range and scope of the assessment is very wide, including as it does not only internal risks of natural hazards, man-made accidents, malicious damage and attacks on cyber-space, but also external risks to the security of the state including the proliferation of mass-effect weapons in failed states, and a crisis outside the territories of EU Member States that affects national security. The risks posed by extremism of various kinds (religious extremism, animal rights extremism and right-wing extremism are included), as are the disruptive potential of confrontation between communities within the Netherlands, and the risk of criminal subversion of critical businesses. In this sense, the Netherlands NRA is far more open about the socio-political risks than are most other NRA so far examined. The breadth of the NRA reflects the fact that it serves not only the national civil protection strategy but its broader international security policy.

Hazard Identification

The National Safety and Security Strategy and associated NRA are based on the identification and exploration of risks through the use of scenarios. These describe events or developments that, on their own or in combination with others, can cause harm to the safety and security of key assets at a national level. The origins of the risk are described, together with the trigger event causing the incident or development to materialise, and the broader societal context including the extent of exposure of people, property and society. Consequences, and consequence management measures already in place, are set out. These combine to form an outline description both of the risk and of its possible outcome.

Proposals for risk themes are approved by the Steering Committee for National Safety and Security but may originate in one of three ways:

- Members of the Steering Committee may make proposals.
- The Steering Group may ask the Network of Analysts for National Safety and Security to elaborate on a theme, and to offer alternative scenarios for consideration by the Steering Group.
- Safety/security regions can propose themes from their own work on regional risk profiles.

Decisions on the risks and scenarios to be subject to further analysis will include the following aspects:

- Timeframe: the normal timeframe for the NRA is 5 years but the Steering Group may specify that the analysis should look not at the next five year period but at a period in the longer term future.
- Whether the scenario to be analysed is a worst case (and therefore less probable), a probable (and therefore less harmful) case or somewhere in between.
- Whether the scenario should be tied to a specific geographical area or be independent of location.
- Which kinds of events should be included in the scenario?

The treatment of impacts on critical infrastructure and vital services is given particular attention both in developing the scenarios, and in scoring impacts during the assessment phase. For these purposes, the Table 15.1 is used to provide a checklist of services whose disruption may have an impact on either the economy or everyday life, or both.

Table 15.1. Critical infrastructure and vital services

Sector	Product or Service
Energy	1. Electricity 2. Natural gas 3. oil
Telecommunications	4. landlines for telecommunication 5. mobile telecommunications 6. radio communication and navigation 7. broadcasting services (crisis communications) 8. internet access
Drinking water	9. drinking water
Food	10. provision and security of food
Health	11. emergency care and other hospital care 12. medicines 13. serums and vaccinations 14. nuclear medicine
Financial	15. payment services/payment structure 16. government financial transfers
Surface water flows	17. managing the water quality 18. controlling the flow and managing the quantity of water
Public order and security	19. maintaining public order 20. maintaining public safety and security
Legal system	21. dispensation of justice and detention 22. law enforcement
Public administration	23. diplomatic communication 24. provision of information from the Government 25. armed forces 26. decision-making in public administration
Transport	27. main port Schiphol 28. main port Rotterdam 29. main roads and main sailing routes (government infrastructure) 30. railway system
Chemical and nuclear industry	31. transport, storage and production/ processing of chemical and nuclear substances

Source: Ministry of Security and Justice (2014) "Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherland", P.O. Box 20301 | 2500 eh The Hague.

Impact Analysis

The Netherlands NRA assesses the impact on five "vital interests":

1. Territorial Security: the undisrupted functioning of the Netherlands as an independent state, and more specifically the territorial integrity of the country.
2. Economic Security: the undisrupted functioning of the Netherlands as an effective and efficient economy.
3. Ecological Security: sufficient self-recovery capability/adaptability of the living environment due to climate changes and other events or developments.
4. Physical Safety: the undisrupted functioning of inhabitants (and nature) in the Netherlands and its (living) environment.
5. Social and Political Stability: the undisrupted continued existence of a social climate in which groups of people live together without major conflict within the framework of the democratic state and shared core values.

In each case, a five point scale is used to represent the range of possible impacts, from A (representing a scenario with very low impact) to E (representing a scenario with a catastrophic impact). In translating this alphabetical scale into numerical values, an impact score of E carries 3 times the weight of D, which carries three times the weight of C etc., so that the impact scale is in effect logarithmic. This makes it easier for the Netherlands to manipulate the scoring so as to give proportionally greater weight for example to elements of national infrastructure which are most critical to the economy or society than to others that are less critical. In carrying out the scoring, equal weight is given to the 5 main types of impact (here defined in italics).

Table 15.2. Vital interests and impact indicators

Vital Interest	Impact indicator
Territorial Security	1.1 Encroachment of Territory: *the actual or functional loss, or out of action and/or access or the loss of control over parts of the Kingdom of the Netherlands (including territorial areas overseas and territorial waters and airspace).*
	1.2 Infringement of International Position: *damage to the reputation or the influence or appearance of the Netherlands abroad.*
Physical Security	2.1 Fatalities: *Fatal injuries, immediate fatality or early fatality within a period of 20 years*
	2.2 Injuries: Cases of injury in the [triage] categories T1 and T2, and people with long-term or permanent health problems such as breathing difficulties, serious burns or skin disorders, damage to hearing, suffering post-traumatic stress syndrome (PTSS). Victims in the categories T1 or T2 need immediate medical assistance and should be treated immediately (T1) or must be kept under continuous observation and be treated within 6 hours (T2). Chronically ill people who experience limitations over a long period (> 1 year): needing medical care, being wholly or partially excluded from participating in their work, experiencing difficulties in their social functioning due to their illness.
	2.3 Physical suffering: Exposure to extreme weather conditions, as well as a lack of food, drinking water, energy, housing, basic sanitary provisions or other primary necessities of life.
Economic Security	3.3 Costs and impairment of the economy: a. repair costs for damage suffered, extra costs and lost income. b. impairment to the vitality of the Dutch economy
Ecological Security	4.1 Long-term impact on nature and the environment: long-term or permanent impairment to the quality of the environment, including contamination of the air, water or ground, and long-term or permanent disturbance of the original ecological function, such as the loss of diversity of types of flora and fauna, loss of special ecosystems, being overrun by foreign types.
Social & Political stability	5.1 Disruption of everyday life: infringement of the liberty to move about freely and to gather in public places and spaces, whereby participation in the normal social existence is hindered.
	5.2 Violation of the Democratic System: impairment of the functioning of the institutions of the Dutch democratic system and/or infringement of rights and liberties and other core values bound to the Dutch democratic system as set out in the Constitution.
	5.3 Social psychological impact & social unrest: negative emotions and feelings (such as fear, anger, dissatisfaction, sadness, disappointment, panic, disgust, and resignation/apathy) of citizens. This concerns the population as a whole, therefore besides those people directly affected also citizens who experience the incident or process via the media or other means. The expressions of these emotions and feelings may or may not be perceptible (i.e., audible, visible, readable).

Source: Ministry of Security and Justice (2014) "Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherland", P.O. Box 20301 | 2500 eh The Hague.

Likelihood and Plausibility Analysis

An estimate is made of the likelihood for every scenario. As in the case of impact analysis, the uncertainty in the assessment is catered for by calculating three values:

- The expected or forecast value: this is the most likely score.
- The lower limit: the score is almost certainly equal to this or higher.
- The upper limit: the score is almost certainly equal to this or less.

For each of these, the likelihood score of between A (highly unlikely) and E (highly likely) is estimated according to Table 15.3, which also shows a further sub-division of each of the five points for likelihood into low, medium and high.

Table 15.3. Likelihood scores

Class	% likelihood over 5 years	Sub-division	Quantitative (%)	Qualitative description
A	< 0.05	A-low A-medium A-high	<0.01 0.01 - 0.025 0.025 - 0.05	Highly unlikely
B	0.05 – 0.5	B-low B-medium B-high	0.05 – 0.1 0.1 – 0.25 0.25 – 0.5	Unlikely
C	0.5 - 5	C–low C–medium C-high	0.5 – 1 1 – 2.5 2.5 - 5	Likely to a certain extent
D	5 - 50	D-low D-medium D-high	5 – 10 10 – 25 25 - 50	Likely
E	50 - 100	E-low E-high	50 – 66 66 - 100	Highly likely

Source: Ministry of Security and Justice (2014) "Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherland", P.O. Box 20301 | 2500 eh The Hague.

Determining the likelihood for the individual scenarios is based on a variety of sources of information including, for a quantitative judgement, historical data and reasoning based on case histories, modelling and design calculations, and data on the failure of individual components of the hazard combined with network analysis where (as is often the case) networked risk is concerned. For risks where more qualitative judgements are concerned, and in particular in the case of threats of malicious harm, the Dutch methodology uses expert opinion, trend analyses, and threat analyses, combined with vulnerability analysis. Calculations of the plausibility of the terrorist threat are based on the capabilities and intentions of terrorist group to carry out particular kinds of attack successfully, and the vulnerability of their intended targets; on the first set of criteria, qualitative judgements are made of the extent to which the scenario is credible and there are concrete indications that terrorist groups have the capability and intent, on a scale from A to E; and these scores are compared with a vulnerability assessment on a three point scale to give an overall score.

Risk evaluation, monitoring and re-evaluation

The Steering Group on National Safety and Security is responsible for approving the final report and determines in which form this can be published. The basic principle hereby is: "open if possible, confidential if necessary". The final product of the NRA is a report from the Network of Analysts for National Safety and Security, in which the following parts, provided with substantiation, are included: 1) the scenarios; 2) a short description of the way in which the scenarios and the risk assessment were carried out and which parties were involved; 3) the scores (i.e., the calculated impact and likelihood values) of the scenarios used in the risk assessment, with an explanation and substantiation risk diagrams in which the scores of all the scenarios are set out against an impact and likelihood axis; 4) one or more sensitivity analyses.

Communicating the results of National Risk Assessment

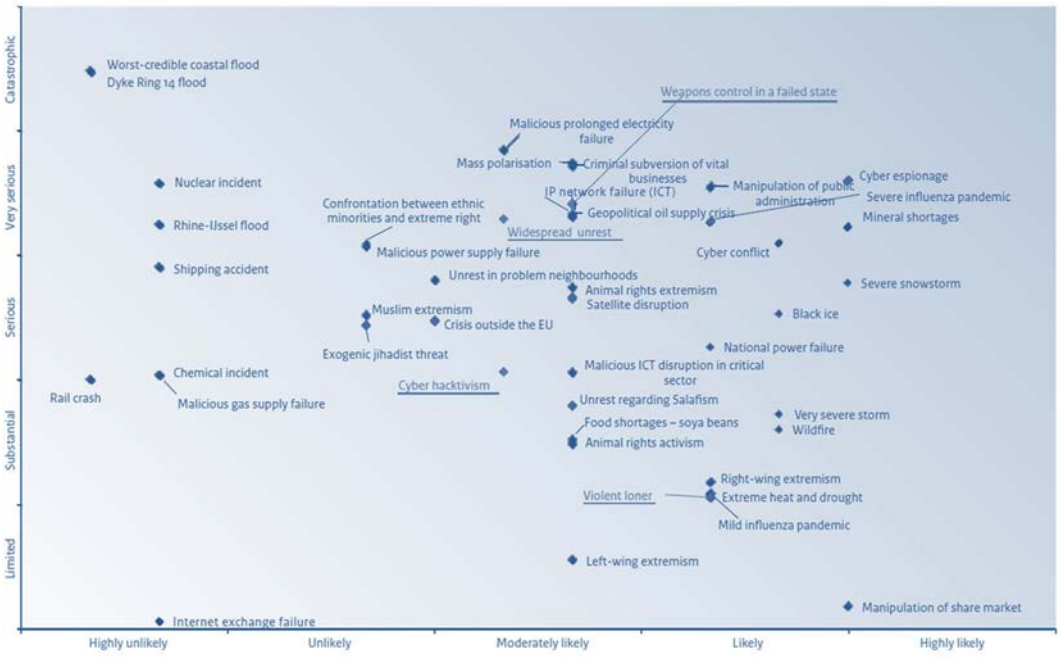
Using the National Risk Profile to raise awareness about risks

The Netherlands Government gives out considerable detail about its NRA, both in the detail supplied in open forum about the methodology and about the outcome of the assessment. Thus, the sixth edition of the NRA, which reports the outcome of work to assess three risks (1) far-right extremism; 2) Lek Dyke breach and flooding of Lopiker and Krimpenwaald; 3) foreign enterprise unmasked as a criminal Trojan horse) sets out the detailed assumptions underpinning the scenario as well as the detailed scores for likelihood and impact, with explanations for each. NRA 6 also provides a chart showing the frequency with which each of the impact criteria are scored as A, B-C, or D-E, providing an explanation of the priority adopted by the Government for investment in generic risk management capabilities. The NRA also supplies details of the organisations in the National Network involved in assessing each of the three risks.

Tools for interpreting risk analysis

The main tools for interpreting risk analysis are the risk matrix in the published NRA (Figure 15.1). These are based on equal weighting being given to each of the ten impact indicators, but sensitivity analysis is also carried out, exploring the effects of using different weightings (for example, by applying the weighting to the 5 'vital interests'). Similarly, the effects of using the worst case or best case scenarios can be explored and the effects displayed on a diagram specifically designed to show the degree of uncertainty in the analysis of the risks. The Netherlands also carries out capability analysis in relation to the risks in the NRA and systematically compares the capabilities required in order to make calculations of capacity (the amount of capability required) in each of the main capability areas.

Figure 15.1. The Netherlands Risk Diagram with logarithmic axes for the 2014 National Risk Assessment



Source: Ministry of Security and Justice (2014), Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherland", P.O. Box 20301 | 2500 eh, The Hague.

Regional risk assessment is carried out according to similar methodology, although not for purely national risks (like space weather); and risk mapping (for fire hazards, floods and chemical/radiation hazards) is also carried out at regional level. Amongst the other tools available for risk management is an application for mobile phones ("crisis.nl") which provides information to citizens on common hazards, in particular flooding.

Main lessons learnt and policy outcomes

Lessons Learnt

The Dutch NRA is a thorough, mature assessment which has strong buy-in from the Network of Analysts that produces it and a strong link to policy formulation in the National Safety and Security Strategy. The collaboration between public/private sector stakeholders means that the NRA can assist in securing consensus on priorities, in determining an effective balance between prevention and resilience in national strategy, and in quantifying the most important impacts in need of mitigation. In a country that has, in general, a comparatively benign risk environment, and whose people show themselves to have a high degree of trust in the authorities, the quality of legislation and tradition of risk management, the government's openness about the national risks helps contribute to risk awareness and the avoidance of complacency.

Policy Outcomes

In a 2015 letter to the House of Representatives, the Minister of Security and Justice outlined changes that the Government of The Netherlands proposed to make to the National Safety and Security Strategy, which is based on the analysis of threat and risks. The government will replace the current annual National Risk Assessment with a

National Security Profile (NSP) to be released every four years, with the first edition due in 2016. The National Security Profile will be a comprehensive analysis of the most salient risks and threats to national security, based on an all-hazards approach, but will also contain an overview of relevant technological and social trends and developments that are likely to affect the country's risk profile in the foreseeable future. The expectations is that the first NSP (2016) will contain 8-10 threat themes describing developments and future trends that are assessed to be the main drivers of risk in the future. Work will continue in the Network of Analysts for National Safety and Security to identify the risks arising from these themes, updating existing risk assessments or adding new scenarios accordingly, to inform future work on capability.

The benefits of this new approach are likely to be that it maintains the momentum already achieved through the 6 editions of the NRA since 2007 by:

- Providing strategic early warning of future developments in the risk profile of the country, to help the government decide on its priorities for longer-term investment in safety and security of citizens of the Netherlands.
- Re-engaging the interest of policy-makers and of citizens, so embedding a risk management culture more firmly in the body politic.
- Capitalising on the very extensive work done, through partnership with stakeholders in the public, private and academic sectors, to assess the current risk picture in the Netherlands, reducing the effort required to maintain the current risk portfolio on an annual basis.

References

OECD (2014), Water Governance in the Netherlands: Fit for the Future*?*, OECD Publishing, Paris
DOI: http://dx.doi.org/10.1787/9789264102637-en

Ministry of Security and Justice (2014), Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherland, P.O. Box 20301 | 2500 eh The Hague.

Further readings

ISO 31000:2009, Risk management – Principles and guidelines.

ISO Guide 73:2009, Risk management – Vocabulary.

European Commission staff working paper (2010), Risk Assessment and Mapping Guidelines for Disaster Management Guidelines. Available at: https://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf

Chapter 16. NEW ZEALAND

This chapter discusses the broad concept of New Zealand's national risk management strategy as a framework for a comprehensive collaborative approach to deal with a full range of national security challenges. From a governance perspective national security issues are overseen by the cabinet and involve oversight of a system of Domestic and External Security Co-ordination (DESC) which is integrated at all levels. The ongoing management of these risks has been influenced by the catastrophic Christchurch Earthquake that the country suffered in 2011 and the potential for further seismic activity in the future. This chapter discusses the methodology used in New Zealand for hazard identification, impact analysis and, likelihood and plausibility analysis. An all hazards approach is used in the risk analysis process with involvement by public and private entities such as government agencies, critical infrastructure owner/operators, SME's and academia.

Key Words: Accountability; Active partnership; Comprehensive concept of national security; Indicative national risks; overlapping levels of responsibility; Subsidiarity.

Introduction

New Zealand's national security system has evolved over the past 20 years, shifting from threat-based assessments to the more active management of risks of all kinds, over time. Emphasis is now put on a comprehensive layered management, building local preparedness, and encouraging resilience in communities, organisations, networks, and critical infrastructure. A national risk management strategy provides a framework for this collaborative approach.

Taking such a broad approach to risk identification and risk response has required a more open and transparent national security architecture. New Zealand's capacity to deal with the full range of national security challenges requires the system to be integrated at all levels, and able to leverage partnerships between government agencies, local government, private companies, and individuals.

Governance framework

Since 1987 New Zealand's arrangements for dealing with national security issues have evolved through a system of Domestic and External Security Co-ordination (DESC) overseen by Cabinet. The public policy document that sets this out defines national security in terms of a risk management strategy, observing four main principles (New Zealand's National Security System, 2011)[1:]

- That the system should address all significant risks to New Zealanders and the nation.
- That national security goal should be pursued in an accountable way, respecting civil liberties and the rule of law.
- The principle of subsidiarity should be applied, meaning that responsibility and authority for decision and the use of resources ordinarily rests at the level of those closest to the risk and best able to manage it.
- That New Zealand should strive to maintain independent control of its own security, while acknowledging that it benefits from norms of international law and state behaviour which are consistent with the nation's values, global and regional stability, and the support and good will of its international partners.

The National Security System document is likely to be updated in 2016, and the indications are that the trend will be towards more resilience and adaptive management of risks. A central feature of thinking about the risks in New Zealand is that the most serious are also the least predictable or understood; and therefore that the best policy is to invest in improving the general resilience qualities of the nation, its infrastructure and its citizens.

Aims and Objectives

The policy context for New Zealand's security is set out in its planning document (New Zealand's National Security System, 2011) which outlines the main elements influencing the country's current risk profile (generally benign but with some significant natural hazards, and potential for interaction between these and new vulnerabilities arising as a by-product of economic and social development), and the – generally global – trends and factors driving change for the future. New Zealand's national security system,

as much a matter of policy as of law, provides a framework for managing these risks and, increasingly following the significant damage done by the Christchurch earthquake disaster of 2011, building the resilience of communities and infrastructure.

Within this system, the primary purpose of the Riskscape is to:

- Illustrate the spectrum of risks from those affecting individuals and communities, those affecting security of the State, to those that are clearly in the international domain.
- Identify overlaps of responsibilities, as illustrated in Figure 16.1.

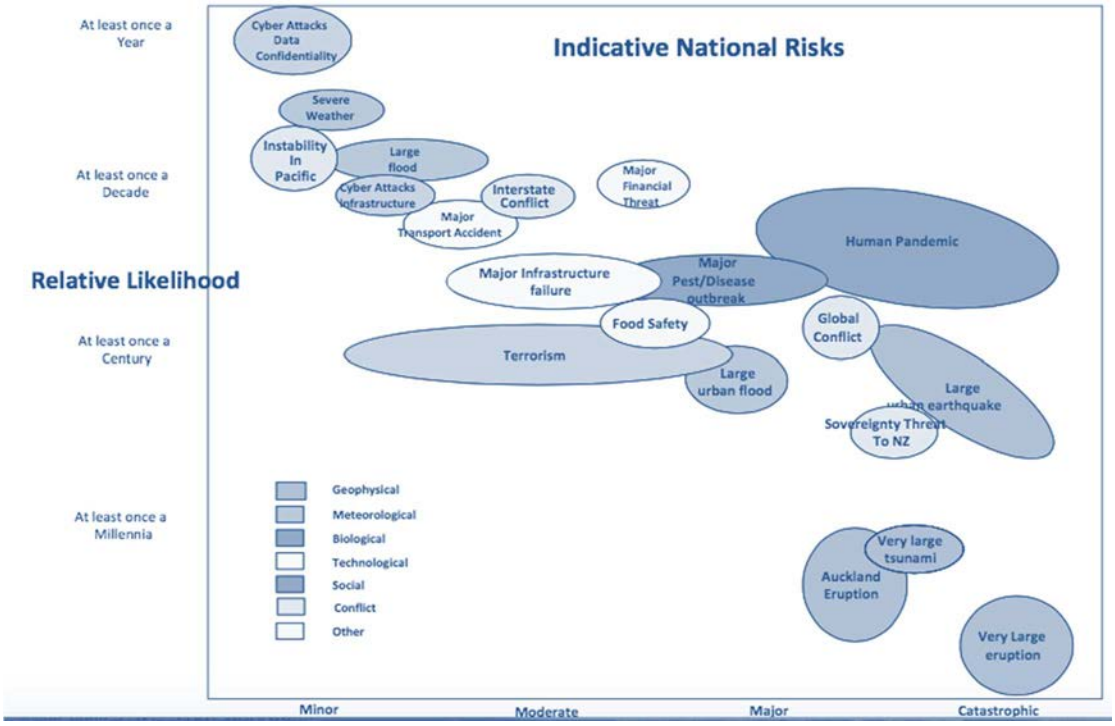
Figure 16.1. Overlapping levels of responsibility for risk management action

Source: Department of the Prime Minister and Cabinet of New Zealand (2011).

To provide a visual comparison of the approximate scale of the main components of significant risks – likelihood and consequence – in order to indicate for planning purposes the relative importance of the risks.

The matrix presented in Figure 16.2 shows indicative national risks. It comes with caveats (that it is not meant to be a precise portrayal of risks; that it does not depict worst case scenarios but averages across the whole of New Zealand; and that it should not therefore be used for regional planning). The assessments are qualitative rather than quantitative, particularly for large-scale and rare events, and the intention is that it be used for capability planning rather than for calculations of the capacity needed for those risks that are accepted as the responsibility of the national government.

Figure 16.2. Indicative National Risks



Source: Department of the Prime Minister and Cabinet of New Zealand (2011).

Definition of key terms

National security is defined as a "condition which permits citizens to go about their daily business confidently, free from fear, and able to make the most of opportunities to advance their way of life", with seven key objectives that underpin a comprehensive concept of national security:

- Preserving sovereignty and territorial integrity - Protecting the physical security of citizens, and exercising control over territory consistent with national sovereignty.
- Protecting lines of communication - These are both physical and virtual and allow New Zealand to communicate trade and engage globally.
- Strengthening international order to promote security - Contributing to the development of a rules-based international system, and engaging in targeted interventions offshore to protect New Zealand's interests.
- Sustaining economic prosperity - Maintaining and advancing the economic well-being of individuals, families, businesses and communities.
- Maintaining democratic institutions and national values - Preventing activities aimed at undermining or overturning government institutions, principles and values that underpin New Zealand society.
- Ensuring public safety - Providing for, and mitigating risks to, the safety of citizens and communities (all hazards and threats, whether natural or man-made).
- Protecting the natural environment - Contributing to the preservation and stewardship of New Zealand's natural and physical environment.

"Risk" is expressed as a product of likelihood and consequence of events affecting objects of value in the physical environment and the social (including health), economic and built/infrastructure environments. Systemic risks are those that arise from the interactions between interdependent elements of the economy and society.

Transparency and accountability

The DESC system provides a practical means of overseeing implementation based on the four main principles of national security. In particular, the principle of subsidiarity, and the need for active partnerships between multiple stakeholders at local level, is underpinned by a Co-ordinated Incident Management System (CIMS)[2], which is a set of international protocols adapted for local use and agreed by all New Zealand emergency services. CIMS provides a consistent methodology which can be applied both to local emergency response and to larger events (for example a health emergency) – requiring a layer of regional co-ordination.

The role and function of Central Government, and the threshold for Central Government engagement (and expectations of when emergencies will be handled by first-line responders or local authorities/lead agencies) are set out, together with the three elements of the national security governance structure:

1. The Cabinet Committee on Domestic and External Security Co-ordination – DES[3], which is the key decision-making body of executive government in respect of all issues involving security, intelligence, and crisis management. DES is chaired by the Prime Minister, and includes senior Ministers with relevant portfolio responsibilities. The membership of DES is flexible depending on the nature of the emergency (for example, pandemic, natural disaster, biosecurity emergency etc.).
2. The Officials' Committee for Domestic and External Security Co-ordination - ODESC, which is a forum of central government chief executives with security responsibilities, chaired by the chief executive of the Department of the Prime Minister and Cabinet.
3. Watch Groups and Working Groups of senior officials as required.

In the 2011 version of the national security system policy guidelines, a number of new measures were announced, affecting governance of the system overall and designed to strengthen strategic prioritisation, resource co-ordination, leadership and accountability within the central government security and resilience community. The new arrangements strengthened the role of ODESC, supported inter alia by policy and operational directorates within the Department of the Prime Minister and Cabinet. The National Security Process is illustrated in Annex 16.A2.

Multi-level governance and multi-actor participation

Risk identification and analysis is carried out at regional and local level in accordance with the principle of subsidiarity and various legislation. There are arrangements for involvement of actors outside government (infrastructure owners/operators/ academics/other SMEs) in risk assessment and management. These are largely voluntary, although there is legislation pending that will require owners of infrastructure (electricity, telecommunications etc.) to provide reliable services.

Risk analysis

Scope

The matrix showing indicative national risks identifies national security risks on an "all-hazards" basis. This means that all risks to national security whether internal or external, human or natural, are included within the ambit of the national security system.

Hazard Identification

Identification of hazards is done by means of scenarios. These are assessed on a comparable basis by setting out the average severity of the hazard across all of New Zealand. National risks are identified in central government; local risks by local government. Officials (local and central) work together to identify risks that may not have a single (or any) owner; often central government has to pick up risks that have no owner.

Risk analysis sometimes uses scenarios to illustrate risk types, sometimes empirical evidence, and sometimes scientific research. There is no single template in use for all scenarios, and no set number of scenarios. The scenario selection process draws on multi-disciplinary expertise, especially where the analysis involves any physical, social, economic or environmental risks.

In general terms, the criteria for issues to be managed at the national level tend to fall into two broad categories relating to the **characteristics** of the risks or the way in which they have to be **managed**. As Annex 16.A2 suggests, the government takes a particular interest in risks that have the following risk characteristics:

- unusual features of scale, nature, intensity or possible consequences
- challenges for sovereignty, or nationwide law and order
- multiple or inter-related problems which when taken together constitute a national or systemic risk
- a high degree of uncertainty or complexity such that only central government has the capability to tackle them
- interdependent issues with the potential for cascade effects or escalation.

The Government is also interested in risks where

- response requirements are unusually demanding of resources
- there is ambiguity over who has the lead in managing risk, or conflicting views on solutions
- there are cross-agency implications
- and/or where there is an opportunity to contribute to conditions that will enhance overall national security.

The most serious risks are, in the experience of those involved in drawing up the national security strategy, those about which least is known. As can be seen from Figure 16.1, considerable attention is given to those risks which begin outside New Zealand, but which can harm assets of value or produce disruption on the domestic front.

Impact Analysis

Consequences were considered across the physical, social (including health), economic and built/infrastructure environments. A four point logarithmic scale is used, in which each succeeding step is ten times more severe than the previous; the four steps are described as "minor", "moderate", "major" and "catastrophic". In some cases, for example, terrorism, the impacts can range from minor to major and this uncertainty is indicated by the use of “balloons” (Figure 16.2). The scales are both quantitative and qualitative; in the New Zealand experience, the most serious risks usually lack reliable quantitative data, so that qualitative means of understanding the risk have to be used. No systematic weighting is given to particular kinds of impact because of the inevitably complicated cascade effects or ill-defined combinations of (e.g., economic, societal, environmental, reputational) effects. As the experience of the Christchurch earthquakes demonstrated, such contextual elements can greatly amplify the predicted effects. No single threshold is used for identifying the risk of disaster or catastrophe. The assessment of impact takes account of preventive or preparatory measures employed to reduce the risk.

Likelihood and Plausibility Analysis

There are four points also on the scale for relative likelihood, from 0.1% likelihood in any one year (at least once a millennium) to 1% (at least once a century), to 10% (at least once a decade), to (at least once a year). The assessment is forward looking and some of the risk trends can be inferred from the description of the context in Annex 16.A1 of the policy. As is the case for impact analysis, the presentation of risks takes account of the degree of uncertainty attaching to estimations of likelihood through the use of "balloons".

Risk evaluation, monitoring and re-evaluation

Figure 16.2 (Indicative national risks) is an unclassified version of the matrix used by the New Zealand government to evaluate risks and determine priorities for national policy towards risk and impact mitigation for those risks that are not delegated to sub-national levels. The assessment of likelihood and impact of risks is an ongoing process at national and local levels, as is the identification of new risks.

Communicating the results of National Risk Assessment

Using the National Risk Profile to raise awareness about risks

Each department of central government tends to have its own close connections with industry counterparts or non-government agencies (for example in the agriculture and health sectors), and these links are used to promulgate suitable information from the national risk profile to enable mitigation and resilience to be improved in those sectors.

The government aims to be as open as possible to the general public; the presentation of indicative national risks is a redacted version of an internal Government assessment designed to inform all stakeholders of the government view of risks. This was prepared in 2010 as part of the May 2011 document on New Zealand’s National Security System, which aims to explain how the risks are managed.

Main lessons learnt and policy outcomes

Lessons learnt

The New Zealand government aims to ensure that lessons about the national risk assessment process are learnt and that new data are incorporated into its analyses. This is regarded as a critical area, but obstacles to effective learning of lessons arise from staff "churn" among agencies, and new knowledge or understanding of risk may not always get the continuing attention that it needs.

Benefits and limitations; Policy outcomes

The Government is in the process of assessing the strengths and limitations of the risk assessment process, and its translation into improved risk management, as part of ongoing reviews of the national security system. Strength is that, as a small country, New Zealand finds it easier to identify and involve the relevant stakeholders in the process and, as in other countries in a similar position, the tradition of cooperation between departments and agencies is relatively strong. A weakness, however, is the tendency to under-appreciate uncertainty, complexity and ambiguity – and to recognise that the most serious risks are the least well known, and the worst are not known at all.

The New Zealand Government believes that in a small well-connected country there are relatively straight-forward pathways between a meaningful assessment and having something done about the problems that are revealed.

Notes

1. An updated version was planned for 2016.

2. The Coordinated Incident Management System was adopted in New Zealand in 1998 following the Emergency Services Review conducted in the mid-1990s. It is a simple and widely-used system to define roles and responsibilities for command, control, and coordination of resources at incidents and emergencies. It is used in one form or another every day in multi-service situations such as major road accidents, search and rescue, and other civil contingencies. Over time it has evolved to become the basis not only of first-line response but of higher level coordination arrangements, such as those used in the emergency operations centre of the Ministry of Health during the H1N1 epidemic in 2009. It is used widely throughout the world, which has allowed New Zealand to respond quickly with well-integrated contributions to emergencies in other countries (eg, the Australian bush-fires in 2009, and similar events in North America).

3. Since 2011 this Cabinet Committee has changed its name to the National Security Committee, a change which is reflected in the 2016 update of the national security strategy.

Reference

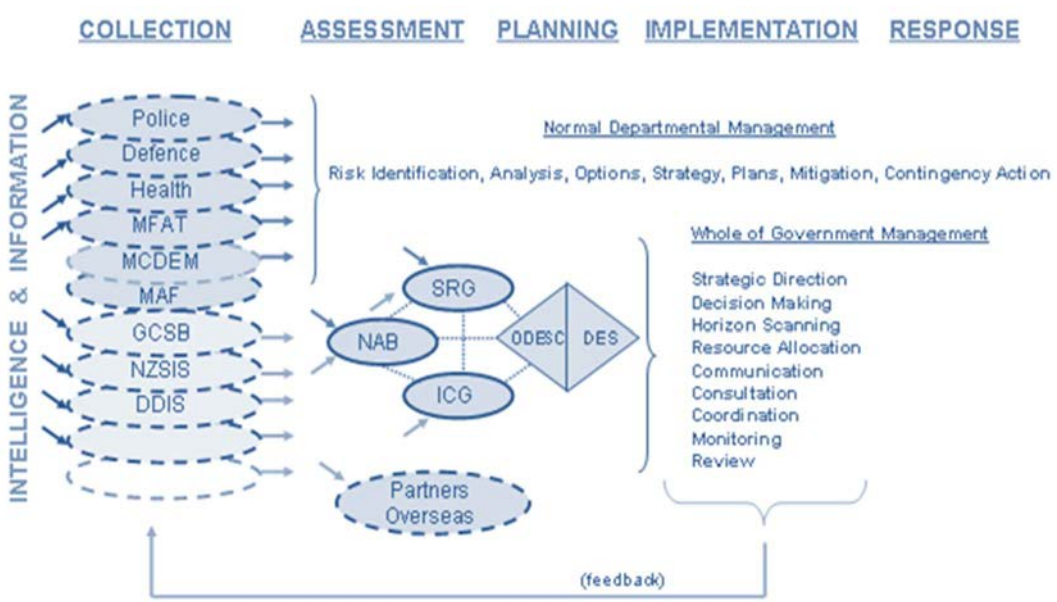
Department of the Prime Minister and Cabinet of New Zealand (2011), “New Zealand’s National Security System”.

Annex 16.A1. Risk Response Thresholds

Risk response thresholds			
Responsibility	First-line responders	Local authority or local lead agency such as DHB	Central government led: - lead agency alone - multi-agency - whole-of-government co-ordinated
Characteristics	- Small scale - Local - Single events - Limited impact - Occur regularly - Boundaries known	- Small-middle scale - Occur periodically - Local or Regional effects - Community impacts	- Large scale and/or complex - Occur occasionally - Boundaries may be ill- defined - Unfamiliar impacts - Little recent experience - Multivariate & interconnected - Unpredictable cascade effects - Serious societal impacts - Wide-spread apprehension - May get worse before better
Resources	- Local Responses - Standard resources - Straightforward to mitigate & manage	- Integrated local and regional resources - National assistance may be required	- Needs significant resources - Requires adaptive responses - Difficult to predict or mitigate - Manage by building resilience - Co-ordinated response required - Resource intensive & high cost - Long-duration recovery

Source: Department of the Prime Minister and Cabinet of New Zealand (2011).

Annex 16.A2. National Security Process.



Source: Department of the Prime Minister and Cabinet of New Zealand (2011).

Chapter 17. NORWAY

Norway has developed and analysed a set of crisis scenarios (ACS[1]), and a methodology for making such analyses. The work is co-ordinated by the Directorate for Civil Protection (DSB). The ACS are firmly rooted in legislation outlining the roles and responsibilities of government bodies and municipal authorities. Subject matter experts are included in the process from the beginning with wide consultation taking place. The ACS process and outcomes are available to the public online. This chapter discusses the methodology for hazard identification/analysis and vulnerability and impact analysis in some detail.

[1] The scenarios were originally called National Risk Assessment. In 2016 the name was changed to "Crisis scenarios – analyses of serious events that may affect Norway" (in short: ACS). In this document, the term ACS is used consistently, although it also refers to scenarios developed previous to the change of names.

Key Words: All significant risks; Accountability; Broad national security considerations; Comprehensive layered management approach; Independent control; Overlapping level of responsibility; Subject matter experts.

Introduction

The Norwegian Ministry of Justice and Public Security commissioned a 'National Risk Assessment' from the Directorate of Civil Protection (DSB), and the first edition was published in 2011. The fourth edition called 'National Risk Analysis 2014' is publicly available online, providing broad information on 15 risk areas and 20 analyses of specific disaster scenarios that can affect the Norwegian society. The interest in producing an analysis of crisis scenarios stems from the recognition that a broad systems perspective helps to analyse the complex nature of modern risks.

The purpose of the ACS is threefold:

1. To provide decision makers an easily accessible comparative overview of disaster risks
2. To provide input to risk analyses and emergency planning in the ministries, sectors, and authorities at regional and local level.
3. To contribute to capacity planning for worst case scenarios that might occur in the future.

DSB regularly involves experts in the scenario development. Emphasis is placed on the identification and assessment of cross-sectoral incidents with serious consequences, requiring extraordinary efforts by the sectoral authorities. The most recently published ACS describe hazard and threat scenarios for a selection of "undesired incidents that would present disastrous consequences for society", be they natural events, major accidents or malicious acts. Risk is generally assessed according to their consequence, probability and uncertainty, although probability is not determined for scenarios that entail deliberate acts. A risk matrix is produced that plots risk scenarios according to their likelihood and consequence. The scenario with the highest risk is a pandemic flu. The highest ranking risk scenario in terms of consequences is an earthquake in a city.

The next edition of ACS will be published in 2018. The report will contain risk analyses of 25 scenarios – five more than the 2014-edition. The new analyses are Foodborne diseases, School shooting, Urban flooding, Resistance to antibiotics and Shortage of drug supply. Individual reports are made with in-depth analyses of each of these scenarios.

Governance framework

According to the Norwegian Royal Decree of 15 June 2012 the instructions for public security in the ministries should be "based on an overview of the risk and vulnerabilities in their own sectors and DSB's National Risk Analysis, must assess the risk, vulnerabilities and robustness of critical social functions in their own sectors as a basis for continuity and emergency planning". On September 1th 2017 the decree was replaced by new instructions for the ministries, with similar requirements.

The Act relating to Municipal Emergency Preparedness, which entered into force on 1 January 2011, states that the "Municipalities are required to survey the disruptive events that may occur in the municipalities, assess the probability of these events occurring and

how their possible occurrence may affect the municipalities. The results of this work must be assessed and collated in a comprehensive risk and vulnerability analysis" (DSB, 2014).

The legal duty for government bodies for all sectors and at all levels to conduct risk assessment is thus firmly rooted in legislation. The remit to co-ordinate a national risk assessment comes from the Ministry of Justice and Public Security to DSB as the agency responsible for civil protection and planning. DSB has consulted widely in devising a risk assessment methodology and has created expert environments involving subject matter experts in each risk area both within and outside DSB, to identify the main risk areas, to agree scenarios, and to carry out risk analysis. DSB has used expertise from the Norwegian Defence Research Establishment and from the University of Stavanger in an advisory capacity in all this work.

Aims and objectives

The overarching policy contexts of the ACS are civil contingencies planning, national security and public safety. The objective is to provide a shared basis to understand key risks for civil protection planning across sectors such as health, transport and energy. Norway operates according to a 'Principle of responsibility' whereby each sector conducts an analytical overview of risks and vulnerability within its own area of competence. Report to the Storting no. 29 (2011-2012) on Civil Protection states that the "Government has decided that DSB's National Risk Analysis should form the basis for a common planning foundation across the sectors and sectoral authorities in society. (…) The enterprises should base their planning upon this, as a supplement to the overview of risk and vulnerabilities that the enterprises have within their own areas of responsibility. All actors must therefore evaluate what the risk analysis may mean to their area of responsibility."

The aims of the ACS vary according to the target groups (DSB 2014, p. 16):

- Politicians and leaders may have a need for an overall risk analysis across sectors.
- Municipalities, counties and sectoral authorities can use the ACS to survey what national events might affect them and require preparedness measures
- At the operational level, the scenarios in the ACS can be used for exercises and emergency planning.

The objectives for the Norwegian ACS are to aid:

- Emergency planning, by promoting a consistent method of risk analysis across government and agencies including local authorities.
- Emergency planning in particular for cross-sectoral incidents requiring extraordinary efforts across government.
- Risk information to all societal sectors and the public.

Definitions of key terms

The ACS include several definitions of key terms used in the risk analysis.

- "Likelihood" is used as an expression of how likely we think it is that a specific event will occur, given our knowledge base.
- "Consequences" are the effects of an adverse events on given societal assets.

- The “risk analyses” in the ACS are assessments of the likelihood that the scenario will occur, the societal consequences the events may have, the vulnerability of the systems involved d and the uncertainty related to the knowledge base of analysis results.
- “Vulnerability” is conceived as the capacity for society to continue to function when exposed to the extraordinary effects of the scenarios in the ACS. The barriers to prevent disruptive events and their consequences influence the vulnerability of the society. A robust society has the capacity to resist and withstand adverse events, and to quickly restore critical societal functions.
- “Risk management” is the entire process of defining in what areas and for what adverse events risk analysis should be conducted, conducting the risk analysis, evaluating the risk results (whether the level of risk is acceptable or not) and implementing any risk-reduction measures.
- The term 'catastrophic events' is based on a definition of disaster: A disaster is a major upheaval, accident or destruction in which many persons are involved simultaneously and which entail extreme consequences for the population and society. Disaster is also used to refer to events that exceed the capacity and resources of the local community and ordinary support systems to manage the event.

Transparency and accountability

Information about the ACS procedure is open to public on the Directorate for Civil Protection's website and in print. DSB gives presentations of the ACS for ministries and other authorities, including the regional and county government level. User surveys have been conducted among major stakeholders in order to improve the ACS.

Risk analysis

The five step process of conducting an ACS:

1. definition of the societal values to be protected
2. hazard identification and selection
3. development of scenarios
4. risk analysis of selected scenarios through expert workshops
5. consolidation of information and establishment of a risk overview.

Scope

In 2014, the ACS included 20 scenarios of catastrophic events that could occur in Norwegian society. These were identified on the basis of how they affect five paramount societal values with two associated consequence types for each value. This gives 10 consequence types to qualify the adverse consequences that an incident could have. (Table 18.1). DSB recognises that these risk scenarios are not all the catastrophic events that could occur and it foresees the development of new risk scenarios in future. The next catastrophic event may be a type that has not been seen before or analysed and therefore it may be completely unexpected when it occurs. The prevailing view at DSB is that by preparing Norwegian society to meet the events that have been analysed in the ACS, high levels of preparedness can be supported for the consequences of many unanticipated events.

Table 17.1. Societal values

Societal assets	Associated adverse consequences
Life and health	- death - injuries and illness
Nature and the environment	- long-term damage to nature and the environment
Economy	- financial and material losses
Societal stability	- social unrest - impact on daily life
Capacity to govern and maintain territorial control	- weakened national capacity to govern - weakened territorial control

Source: Adapted from: DSB, 2014.

Hazard identification and analysis

The ACS process entails identification of potential adverse incidents. Among these a selection is made for development as full-fledged risk scenarios – a specific course of events surrounding the adverse incident. The scenario description includes factors contributing to the event, geographic location, time and duration of the event, strength of the event and consequential events. A scenario is defined as a "detailed and specific description of an undesirable incident; a description of a future condition and the series of actions and incidents leading up to the incident" (DSB, 2011, p.11). Any type of incident, such as a flood, can have a broad range of possible consequences. To facilitate the analysis the incident is developed into a conceivable worst case scenario, which illustrates the most severe consequences the event could have on the entire range of societal assets. The worst-case scenario is not so extreme as to be unrealistic (its occurrence should be possible in the course of a year), nor should it be so mundane as to encompass day-to-day accidents.

Common to all the scenarios are the following characteristics:

- The events have consequences affecting several important societal assets.
- It must be conceivable that they could occur in the course of a year.
- They must threaten one or more of the societal assets.
- They must have cross-sectoral consequences and require cross-sectoral management.
- They must require extraordinary input from the public authorities.
- They must be based on an event that has actually occurred.

To begin work on a risk scenario, DSB contacts agencies whose experts would be most involved in management of an actual incident depicted in the scenario. Relevant knowledge and experience from similar events in Norway and abroad is collected, and a scenario is developed in close cooperation with these experts. A working seminar is held to conduct a qualitative expert analysis in which relevant competence is gathered from various sectors and academic communities to assess likelihood of the event and its consequences.

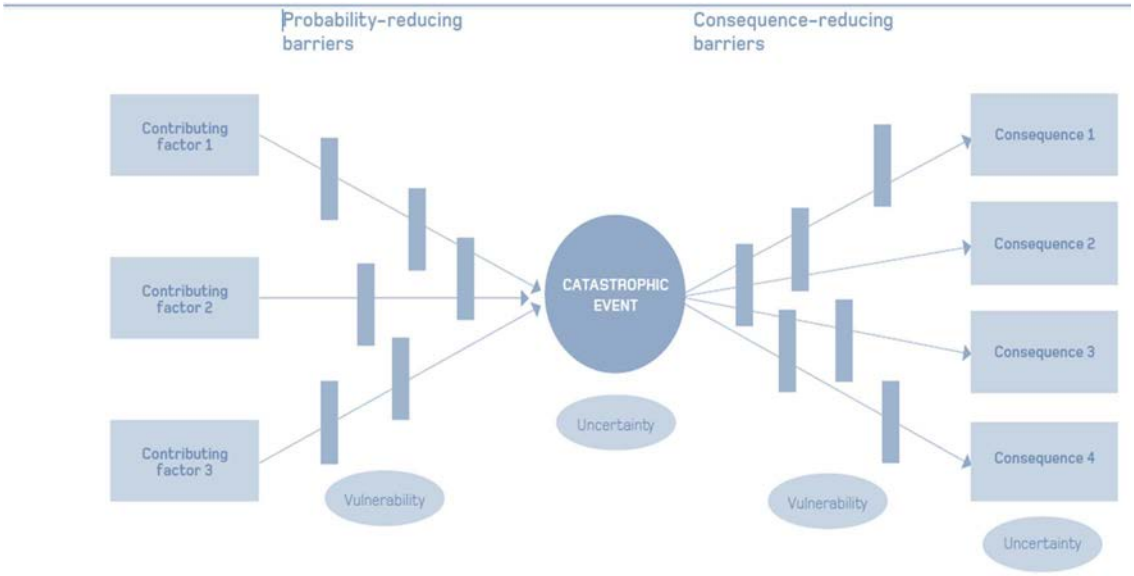
In addition to the groups consulted to help develop specific scenarios, a reference group of five or six experts from the most relevant agencies meets with DSB two times a

year to discuss practical problems, methodology and choice of scenarios. DSB also consults with independent experts from universities and research institutions. DSB recognises the risk that experts may attempt to push their own agenda, but has not experienced this as a problem. It has also established a common process for experts to follow to ensure consistency in the scenario analyses.

The risk analyses conducted at the working seminars described above produce qualitative expert analysis in accordance with the bow-tie model (cf. figure 17.1), which describes the course of an incident before and after a disruptive event.

The bow-tie model distinguishes trigger events that take place before the disruptive event, which are the prerequisites for the main event occurring. Concurrent events take place at the same time as the main event and affect the subsequent course of events. There are also second and third order effects that take place in the wake of the disruptive event, which can contribute to the consequences. An illustrative example is the flood risk scenario: a warm front is a contributing factor, a heavy snowmelt is a trigger event, and a breached flood defence is a concurrent event. Damaged transmission line masts and roads are cascading events, which contribute to the final consequences of the disruptive flood event .

Figure 17.1. Bow tie model for risk analysis



Source: DSB (2014).

The experts at the working seminars provide opinions both about the likelihood of the incident occurring, and the magnitude of its various consequences. They score the likelihood and consequences in quantified terms to the greatest possible extent, and not just classified qualitatively as high/low and large/small. The likelihood is stated as the period of time over which the adverse event is expected to occur, and this is converted to a percentage of likelihood that the event will occur within one year (DSB, 2013, p.32).

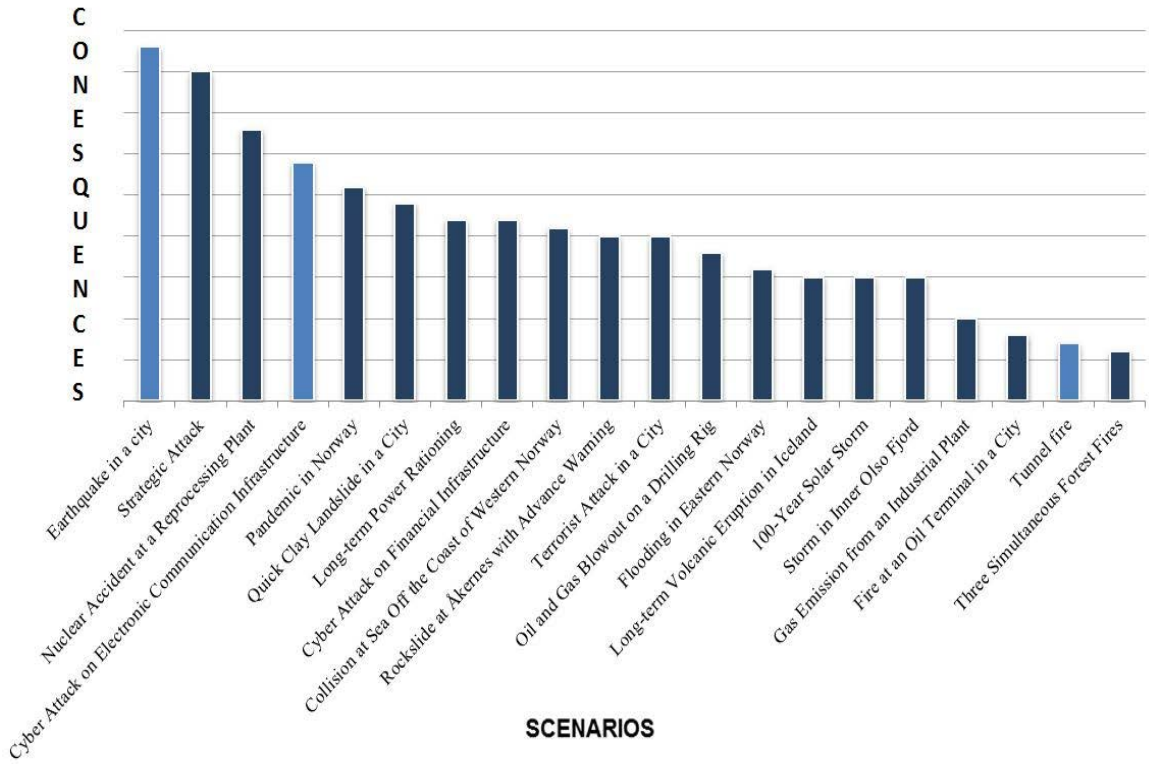
The perceived strengths of expert analysis are the transfer of knowledge and efficiency. DSB recognises, however, that the quality and precision of the assessments of

probability and consequences depend on the quality of the expertise represented during the process. Potential disagreement among experts is expressed in the uncertainty dimension of the risk analysis.

Vulnerability and impact analysis

The consequences described are based on ten consequence types in the risk analysis (Figure 17.2). Each consequence type is assigned a score (A-E), which depends on the quantities indicated in the risk analysis (e.g., number of fatalities, costs, etc.). Scoring of consequences overall is done by giving a quantitative value for each consequence type and then totalling the scores on the basis that all 10 of the types are weighted the same. After assigning a score for all the consequence types , these are aggregated to produce the total score for the scenario.

Figure 17.2 Distribution of consequence types – all scenarios



Note: The bars illustrate the overall consequences for each scenario, broken down by the ten consequence types mentioned in Table 17.1

In order to assess likelihood and consequences, it is necessary to have knowledge of both the event that occurs and the vulnerability of the systems or society that are affected. Sources of vulnerability in a system may be interdependencies between critical functions, complexity and an inadequate overview, inadequate barriers and the lack of redundancy.

Likelihood and plausibility analysis

The likelihood that a chosen scenario will occur is assessed on a scale from very low to very high likelihood, where very low likelihood is less than once every 10,000 years and very high likelihood is once or more every 10 years. The likelihood that a natural event or major accident will occur is also expressed as a percentage. The category very low probability means that the likelihood of the event occurring during the course of a year is less than 0.01 per cent, and very high likelihood means that the likelihood of the event occurring is more than 10 per cent (DSB, 2013, p.172).

None of the analysed scenarios are assessed to have a very high likelihood. Similar to the consequence analysis, the likelihood of risk scenarios is estimated and scored. Comparison of likelihood is made on a logarithmic scale, illustrating differences of an order of magnitude in the estimated return periods for the different risk scenarios. There are separate criteria for intentional and non-intentional acts. *Time horizon*

The Norwegian national risk assessment considers near term risks, using a one year time horizon for the selection of scenarios. This short length implies some challenges to consider possible severe consequences of risks that are more likely to occur over the longer term such as those due to climate change or its impact on food security. If the NRA time horizon were extended, the scenarios selected might be altered. The practice of creating and monitoring a list of future events interests the Norwegian authorities, however a lack of resources makes it difficult for DSB to move forward with longer-term planning and assessment of risks.

Uncertainty

The uncertainty is described through an evaluation of the knowledge base for the analysis and of the sensitivity of the results to changes in the assumptions. Results that are sensitive to small changes in the scenarios or assumptions on which the conclusions are based, are less generalisable. Three indicators are used to evaluate the strength of the knowledge base :

1. Access to relevant data and experience.

2. Comprehension of the event/phenomenon that is being analysed (how good is the explanatory model?).

3. Agreement among the experts participating in the risk analysis.

Risk monitoring and re-evaluation

DSB recognises there will be a need to revise the scenarios in order to incorporate new knowledge and experience, which may perhaps change the assessments of risk. This will be contingent on a process in which the responsible authorities and specialist groups are involved. This will be a key purpose of the new 2018 overview of all scenarios developed hitherto.

Communicating the results of National Risk Assessment

Meeting authorities and stakeholders and giving presentations is an effective way of communicating the results from the ACS. The results have been presented to the Minister of Justice and Public Security to provide an overall picture of national risks. The assessment results also inform a wide range of government work, particularly in areas where security or safety issues are important. The method and process used for conducting risk analysis in the NRB is becoming a reference method for conducting risk analysis and presenting an overview of risk and vulnerabilities also among sector authorities, county governors and municipalities. In combination with the decision made by the Government that the NRB should form the basis for a common planning foundation across sectors and sectoral authorities, this also contributes to systematic analysis of risks and increased risk awareness.

Lessons learnt and policy outcomes

DSB have over the last years conducted several surveys that confirm that the ACS are used by stakeholders at both central, regional and local level in their work with societal security. The ACS are used as a knowledge base for given risks and scenarios and provides terms and methods for risk analyses at a societal level. In addition, the process contributes to important arenas for the exchange of information and understanding between stakeholders. The national risk assessment also provides an overview of the situation, a 'risk at a glance' for politicians and decision-makers. It should, however, be emphasized that the ACS are conceived as a backdrop to emergency planning, not as a central government substitute for risk assessments carried out at more local levels by agencies.

Concerning the development and analysis of the scenarios, this can always be refined. DSB continuously examines ways of further improving how scenarios are made and compared, and how the results are presented.

References

Norwegian Directorate for Civil Protection (DSB) (2014), National Risk analysis 2014. Available at: https://www.dsb.no/rapporter-og-evalueringer/national-risk-analysis-2014/

Norwegian Directorate for Civil Protection (DSB) (2013), National Risk analysis 2013.

Directorate for Civil Protection and Emergency Planning (DSB) (2011), National Risk Picture, Process and method.

Chapter 18. POLAND

In Poland the National Risk Assessment (NRA) is part of the National Crisis Plan. The NRA is guided by two agencies, the Government Centre for Security (GCS) and the Internal Security Agency. The process provides for a top down bottom up system of risk identification allowing the public sector, ministries, central offices and provincial administrative areas (Voivods) to work together to identify risks and to provide a central government response to the most serious threats which are contained in the National Crisis Plan. This chapter discusses the methodology for hazard identification/analysis and vulnerability and impact analysis in some detail. The NRA takes an all hazards approach taking a broad perspective on potential threats from both internal and external sources. Poland takes an active role in keeping its NRA up to date with a legal obligation placed on each ministry to monitor, analyse and foresee threats in their area of responsibility. Awareness rising forms a large part of the government's strategy with widespread exposure within appropriate departments.

Key Words: All hazards approach; Brain storming and scenario development; Fragmentary reports; Monitor and analyse; Wide spectrum of experts:

Introduction

The biennial National Risk Assessment process in Poland is linked to the development of the "Report on Threats to National Security" and development of a "National Crisis Management Plan" (NCMP). The process entails the development of risk scenarios in 3 groups:

- natural disasters, major accidents and civil hazards (e.g., floods, epidemics)
- malicious acts (terrorism, organised crime, corruption etc.)
- defence and military issues (e.g., weapon of mass distraction proliferation).

Ministries, heads of central offices, and the 16 regional governors are charged with leading a process of risk scenario development covering risks for which they have responsibility, and to submit fragmentary reports" for each to the Government Centre for Security (GCS). The GCS, together with the national Internal Security Agency (ISA – which leads on terrorist threats), collates the national "Report on Threats to National Security" and associated development of a National Crisis Management Plan.

The first National Risk Assessment was conducted in 2011. By 2013 there were over 50 natural disaster and malicious act scenarios analysed and assessed. Based on the outcomes of the NRA, the Government Security Centre has proposed to include 17 of these risk scenarios in the NCMP. The 17 risk scenarios are presented in Table 18.1.

Table 18.1. Risk Scenarios

Natural Disasters, Major accidents and civil hazards	Malicious Acts
Floods	Social disorder
Human diseases (epidemics)	Terrorist attacks
Chemical contamination	Cyber attacks
Disruption of electricity supplies	
Disruption of fuel supplies	
Disruption of gas supplies	
Heavy snow and low temperature	
Storms	
Animal diseases (Epizootics)	
Plant diseases	
Construction disasters	
Landslides	
Droughts	
Nuclear/radiological accidents	

Source: Adapted from Government Centre for Security (2013)

Governance framework

The GCS is attached directly to the Prime Minister and is responsible for producing the Report on Threats to National Security (the Report), which serves as a basis for civil emergency planning. According to the "Act on Crisis Management" the conclusions of

the Report are part of the NCMP, and should be taken into account in plans prepared by other authorities. The NCMP is designed for events that require central government response and it provides a definition of the risks needing to be included in the Report.

Aims and objectives

The origins of the Poland's National Risk Assessment are to be found in 1997 reforms designed to clarify the responsibilities of local authorities and local responders for emergency risk management, and to establish a national co-ordination mechanism for response to national emergencies. The current legal bases are the "Act on Crisis Management" dated 26 April 2007, and "Regulation of the Council of Ministers dated 30 April 2010" concerning the Report on Threats to National Security. The aim of the Report is to provide the authorities with a common understanding of risks at the national level in order to determine appropriate preventive and preparedness actions aimed at reducing the likelihood of national-level risks and minimising their consequences. This breaks down in more detail as follows:

- identification of significant threats (and their risk map if appropriate)
- identification of strategic risk management objectives in relation to each threat
- identification of the capabilities and resources necessary to achieve strategic objectives
- programmes aimed at improvement of safety and security
- priorities in responding to specific risks.

The National risk assessment is qualitative rather than quantitative, and this affects the way in which it can aid decisions on investment in risk reduction and preparedness measures. The process provides a basis for public sector civil emergency planning by analysing the kinds of capabilities that are required, by indicating for each risk the priority between prevention and preparedness, and by promoting a consistent basis for planning between ministries, central offices and the provincial governors appointed by the central government *(Voivods)*.

The lack of a quantitative basis for the National risk assessment inhibits capacity planning (how much capability is needed or justified), financial planning, and creation of a fully-fledged risk management culture. In the next phase of development, GCS is considering further measures to improve the utility of the Report and associated analysis as part of a national risk reduction strategy; to create a risk management culture; and to enable emergency risk management among stakeholders across the public, private, NGO, community, and voluntary sectors.

Definitions of key terms

Terminology will be revised and updated in the forthcoming revision of the Polish NRA methodology. At present, risk is conventionally defined as a combination of consequences of a hazard (threat) and the associated likelihood of its occurrence. Other key elements of terminology under the 2010 Regulation of the Council of Ministers include a definition of the kinds of risks that should be taken into account in the National risk assessment process. These are defined as "threats that have a major influence on the functioning and development of the nation, threatening in particular the security, international position and economic and defensive potential of the nation" and so provide the basis for definition of the objects of value to the Republic of Poland and the impact

criteria for the National risk assessment process. The Report also outlines strategic objectives which are defined as actions intended either to minimise the likelihood of a potential threat or to mitigate its impacts.

Transparency and accountability

The Polish NRA is co-ordinated by the GCS, and involves all ministries, regional authorities (*Voivods*) and the main central offices in government. Assessment of the risk of terrorist acts is co-ordinated separately by the Internal Security Agency (ISA). In its co-ordinator capacity the GCS is responsible for the following tasks:

1) Preparation of the methodology and procedure for drawing up so-called "fragmentary reports" by ministries, heads of central offices, and voivodeships. The aim is to facilitate development of fragmentary reports and to ensure uniformity of the methodology used by all entities involved.
2) Organisation of relevant training and workshops. The aim is to present risk assessment the methodology and to raise awareness amongst crisis management experts. This preliminary phase requires the participation of expert, middle and high level decision-makers e.g., crisis management teams (high level advisory body). When a fragmentary report is prepared it needs to be approved by the relevant authority (ministry, head of central office, voivodeship).
3) Editing a draft of the “Report on Threats to National Security”.
4) Consulting on the document amongst all involved entities during the legislation process and preparing the relevant resolution of the Council of Ministers.

GCS’s role includes monitoring the use of the mandated NRA methodology by those agencies responsible for producing fragmentary reports, in order to ensure that the risks are assessed on a broadly consistent basis. GCS cannot direct the bodies responsible for carrying out the assessments (ministries, voivodeships, etc.) to make change, but it can make suggestions to correct bias or the inconsistent application of the approved guidelines.

The GSC prepares a draft of the "Report on Threats to National Security" on the basis of all fragmentary reports collected. This document goes to ministries and heads of central offices and “governors” for their approval. They can provide the Director of the GCS with remarks which either should be accepted or should be justified with a written explanation. When corrections and amendments are made a draft of the Report and a draft of respective "Resolution" go to the Council of Ministers. The Report is approved by the Council by Resolution. After approval the GCS sends the document to all involved entities. There is no independent validation of the assessments themselves. According to the "Efficient State Strategy 2020" approved by the Council of Ministries in 2013 the methodology should be revised and updated by the end of 2015. Moreover, it should be followed by relevant publications, dictionary, IT tool, trainings and user workshops.

Multi-level governance and multi-actor participation

The Government Centre for Security co-ordinates the involvement of many different stakeholders in the process of producing the National Risk Assessment. The widest possible spectrum of experts is supposed to be involved in the development of risk scenarios at the regional level and the GSC provides guidance in this respect. Scientific and research institutes subordinated to ministries or central offices should be involved in

risk assessment where appropriate – examples include the Institute of Meteorology and Water Management, and the Polish Geological Institute. Experts from the private sector should be similarly involved in the assessment of risks to critical infrastructure. All ministries, heads of central offices and regional authorities prepare "fragmentary" reports according to their competences. This is meant to enable the identification and analysis of threats from different perspectives as well as provide an opportunity to compare risk perception at national and regional level. Institutions charged with producing a fragmentary report are directed to determine what risk management functions in a given risk scenario might require support or involvement from a different institution. This prompts institutions to reflect on whether they are providing the leading, co-ordinating or supporting role during one of four phases of emergency management: prevention, preparedness, recovery or response. The GCS has a key role in identifying risks that may otherwise fall between the cracks between different elements of government – for example risks relating to money laundering which may engage more than one lead agency or department.

Risk analysis

The Polish NRA takes an all-hazards approach, including threats of intentionally harmful acts such as terrorism and cyber-attacks, and disruptive events such as riots and public disorder. Risk scenarios are evaluated for their likelihood and impact, key determinants of the risk value as indicated on a risk matrix.

Scope

The Report on Threats to National Security is an attempt at a comprehensive assessment of all those threats and hazards that fulfil the criteria established in the 2010 Regulation of the Council of Ministers[5]. This establishes a qualitative threshold that ensures that the Report addresses only those that are beyond the capacity of regional or local authorities to manage and so, for examples, it explicitly does not cover everyday events with high probability and low impacts (car accidents, common crimes, fires, etc.), nor those that are limited to local impacts. It aims to provide public authorities and the public with a (differentiated) understanding of risks at the national level, including risks that originate outside the borders of Poland, but which have a direct effect on the objects of value determined by the Government. Therefore, the risk scenarios are designed to include severe impact scenarios that are reasonably likely to occur.

Hazard identification and analysis

Risk identification is carried out in the process of developing the "Fragmentary Reports", which involves brain-storming and scenario development in various working groups. In the initial national risk assessment round starting in 2011 41 fragmentary reports] were sent to the Government Centre for Security for analysis, comments and aggregation. Thereafter, the process is that the Director of the GCS can express his remarks concerning the degree of detail, scope and form of a fragmentary report and ask

5. Threats that have a major influence on the functioning and development of the nation, threatening in particular the security, international position and economic and defensive potential of the nation.

for corrections. He can also ask to complete a fragmentary report with elements resulting from other fragmentary reports. Given that, in the experience of the Polish authorities, almost all risks serious enough to feature in the national report have multiple owners, the focus of the analysis focuses on clarifying the responsibilities – for leading and supporting risk management efforts – for each phase of the crisis management cycle (i.e. prevention, preparation, response and recovery) and incorporating these responsibilities into the National Crisis Management Plan.

A first step is to specify within which government administration unit a hazard/threat may occur. Government administration units include the following: construction, land management and housing, budget, public finance, economy, marine, water, financial institutions, computerisation, European integration, culture and protection of national heritage, physical culture and sport, communications, science, national defence, education and upbringing, work, agriculture, rural development, regional development, agricultural markets, fisheries, treasury, justice, higher education, transport, tourism, environment, family affairs, home affairs, religious denominations as well as national and ethnic minorities, social security, foreign affairs and health. In principle any or all of these can volunteer a candidate risk within their area of responsibility and these are illustrated by a scenario setting out the following elements:

- A general overview describing briefly the nature of the risk, possible locations, and possible causes (e.g., intentional or accidental).
- Possible impacts, based on a "most likely case" scenario on populations, the economy, property, infrastructure, and the environment.

The Polish consider that, given the seriousness of the risks, a "most likely case" scenario provides a better basis for comparing the risks and creating a generic contingency plan in the National Crisis Management Plan than either a "worst case" or "reasonable worst case" scenario.

Vulnerability and impact analysis

In analysing the impacts in these five areas, the Polish NRA process takes account of the following aspects. For each of these categories both direct and indirect effects are indicated:

Human impacts

- potential number of fatalities
- potential number of hospitalised (severely injured or ill)
- potential number of evacuated
- potential impact on everyday life including, where possible, indirect social effects (such as an increase in unemployment, permanent incapacity for work) as well as negative psychological effects.

Economic/property/infrastructure impacts

- Potential damage to property and infrastructure are estimated, where possible including potential cost.
- Both direct and indirect costs are taken into account (e.g., direct costs of restoration of a damaged building; indirect costs of business interruption resulting from damaged premises).

Critical Infrastructure impacts

The extent of the effect on the following systems:

- energy, fuel and energy resources supply systems
- communication systems
- tele-information network systems
- financial systems
- food supply systems
- water supply systems.
- health protection systems
- transportation systems
- rescue systems
- systems ensuring the continuity of public administration activities
- systems of production, storing and use of chemical and radioactive substances, including pipelines for dangerous substances.

Environmental impacts

Potential harm to fauna and flora as well as to air, soil and water should be described. It should be indicated whether the adverse impact of a scenario is reversible or irreversible (causes permanent or long - term degradation of the environment).

The potential impact on life and health is regarded as more important than any of the other criteria although, since the impact assessment is qualitative rather than quantitative, there is no formal weighting given to any of the criteria. In each case, the Polish NRA process assesses "residual risk", i.e., taking into account preventive or preparatory measures and capabilities to reduce the risk. The scales presented in Table 18.2 are used to assess the degree of harm done in each of the five impact categories.

Table 18.2. Impact categories

Scale	impact	Category	Description (Z - life and health, M - property, S - environment)
1	irrelevant	Z	There are no fatalities or injured people. No one or a small number of people have been displaced for a short period of time (up to 2 hours). No one or a small number of people need help (no financial or material help).
		M	Virtually no damage. None or very little impact on the local community. Little or no financial loss.
		S	Imperceptible effect on the natural environment.
2	small	Z	A small number of injured people but no fatalities. First aid required. Necessary displacement of people (less than 24 hours). Some people need help.
		M	There is some damage. There are some obstacles (no longer than 24 hours). Slight financial loss. No additional funds required.
		S	Little impact on the natural environment for short-term effect.
3	medium	Z	Medical help needed but no fatalities. Some people require hospitalisation. The extra space in hospitals and additional medical personnel needed. Evacuated people staying in the designated Areas with the possibility of a return within 24 hours.
		M	Determination of the damage sites, which require routine repair. Normal functioning of the community with minor inconveniences. Considerable financial losses.
		S	Some effects on the natural environment but short-term or small effects with long lasting effect.
4	large	Z	Badly injured, a lot of people hospitalised, a large number of people displaced (for more than 24 hours). Fatalities. The need for specific resources to help people and to remove the damage.
		M	Community partially functioning, some services are unavailable. Large financial losses. Help from the outside needed.
		S	Long-term effects on the environment.
5	disastrous	Z	A large number of seriously injured. A large number of hospitalised. General and long-term displacement of populations. A large number of fatalities. Enormous help to a considerable number of people required.
		M	Extensive damage. The community's inability to function without significant external assistance
		S	Large impact on the environment and/or permanent damage.

Source: Adapted from Government Centre for Security (2013).

Likelihood and plausibility analysis

Table 18.3 presents the qualitative scale used for assessing the likelihood or plausibility of events.

Table 18.3. Likelihood and plausibility events

Likelihood	Description
Very rare	May occur only in exceptional circumstances (once in five hundred years or even more rarely).
Rare	It is not expected to happen. It is not documented at all. It does not exist in human communications. The events have not occurred in similar organisations, facilities, communities. There is a minimal chance, reason, or other circumstances that the events could occur. They may happen once every hundred years.
Possible	It may happen within a certain time. Rarely random events that are documented or transmitted orally. Very few events. There is a chance, the reason, or the facilities causing the event to occur. It may happen once in twenty years.
Likely	It is likely that it will occur in most circumstances. The events are systematically recorded and communicated in the oral form. There is a considerable chance, reason, or a facility allowing it to occur. It may happen once every five years.
Very likely	It is expected to happen in most circumstances and/ or events are very well documented and/ or they operate among the population and are transmitted orally. May occur once a year or more often.

Source: Adapted from Government Centre for Security (2013).

This scale implies a non-linear progression from point 1 to point 5, which provides a measure of insurance against the uncertainties inherent in the assessment, and the Polish authorities does not use any other method to reflect these uncertainties. Nor do they have a precise timeframe for the assessment; rather, fragmentary reports are asked to consider the likelihood of the risk being realised in the foreseeable future Risk evaluation, monitoring and re-evaluation. The risk evaluation phase results in production of two risk matrices: one setting out a comparison of the risks of natural disasters, major accidents and civil hazards; and a second setting out in similar fashion the risk of deliberate and malicious acts.

Due to the dynamic nature of modern threats, Poland recognises the need to monitor and analyse constantly and systematically. Each ministry, central agency and regional authority is legally obliged to monitor, analyse and foresee threats in the area of their responsibility. Therefore, the risk assessment process in ministries, central agencies and provinces is carried out continuously in a two-year cycle, which is a very short amount of time to achieve approval by the Council of Ministers, at least once in two years as required by Article 5a of the Act on Crisis Management.

NRA Excursions

The NRA includes multi-risk assessments in the sense that the potential for a domino effect, with one kind of event triggering another, is highlighted in the assessment; but the effect is not analysed in detail. Cross-boundary risks (i.e., risks shared with one or more neighbouring states) are included; and risk maps are included in the Report (although the Polish authorities note that their definition of risk map does not correspond to the definition in the European Commission Guidelines).

Communicating the results of National Risk Assessment

Using the National Risk Assessment to raise awareness about risks

The way in which the Report is approved, first by the heads of the over 40 organisations contributing to it and then by the Council of Ministers, ensures that the outcome of the national risk assessment process is owned by the policy-makers who are responsible for implementing risk reduction strategies in their areas of responsibility.

The first of the two matrices, covering natural disasters, major accidents and civil hazards, is included in the National Crisis Management Plan, and is publicly available. The second, relating to threats of malicious acts (including steady-state risks such as organised crime, the misuse of dual use chemical products, espionage, and military threats) is not disseminated although it is not classified.

Main lessons learnt and policy outcomes

Lessons learnt

Real-life experience of crises or exercises, and new data, are incorporated in the Report through the two-year process of validating fragmentary reports.

Benefits

The Polish authorities believe that the main benefit of the NRA process so far has been to raise awareness of the risks within the public sector. The main strengths of the Polish system to this end are: the wide range of (nearly 50) participating organisations at the national and regional level of government; the sharing of different perspectives of risk by these organisations; the two-year review cycle which, although challenging in view of the need to package and present top-level risks to Ministers, has promoted a constant improvement in the analysis summarised in the Report in the two (nearly three) versions produced since the process started in 2011; and the establishment of a central co-ordinator close to the office of the Prime Minister with close working relationships with the ISA (for terrorist threat assessments) and the other government stakeholders.

Limits

Like many other countries adopting NRA, Poland is exploring different options for improving the outcome of the risk assessment process so as to aid development of a national risk reduction strategy. The options include:

- Reducing reliance solely on qualitative assessment of impacts and likelihood: this is linked to the objective of moving beyond analysing the kinds of capability required for emergency response to capacity planning (how much capability is needed or justified) and financial planning.
- Improving the data (historical, scientific, and technical) in order to introduce more quantitative assessment, perhaps on a selective basis; and improving the process of monitoring and verification of the risks of emergencies.
- Exploiting the risk assessment process and outcome to inform risk management policies and an overall risk reduction strategy.

Policy inputs and outcomes

The NRA is a basis for civil emergency planning. This year's review will examine how it could enhance national resilience and what changes would best enable it to do so.

References

Government Centre for Security (2013), Polish National Risk Assessment Report on Threats to National Security, Warsaw.

Further reading

National Development Strategy 2020

Chapter 19. PORTUGAL

Portugal's National Risk Assessment includes widespread representation from all sectors in society under the direction of the National Commission for Civil Protection where civil protection is based on territorial management organised at national, regional and municipal level. Uniquely Portugal's NRA excludes risks of an international dimension which was a deliberate policy choice. In addition, the NRA contributes to the National Platform for Disaster Risk Reduction in respect to implementation of the Sendai Framework in Portugal. This chapter discusses the methodology for hazard identification/analysis and vulnerability, and impact analysis in some detail. The process follows European good practice guidelines (Risk Assessment and Mapping Guidelines for Disaster Management) with a view prevailing that it is not necessary to try to re-invent the wheel. Communication of the NRA process is widespread through each government ministry and the public have access online where some areas are restricted.

Key Words: All hazards approach; Common event-based risk assessment; Risk mapping; Sendai Framework; Territorial management system; Widespread representation.

Introduction

Portugal decided in 2009 to update its national emergency plan, the previous plan from the 1990s being considered out of date. The starting point was to conduct a new National Risk Assessment of some 25 of the most common risks of accident or emergency facing the country. This first iteration was completed in 2011/2012 and adopted in 2013 by the Council of Ministers as part of an updated national emergency plan (NEP) developed in parallel with the NRA. In the spring of 2014, the NRA was made available to the public. The intention is that the NRA should be subject to further work within government and with the private and academic sectors so that a second iteration will be available to inform further evolution of the NEP. In Portugal, civil protection is based on a territorial management system organised at three levels (national, regional and municipal), so the NRA is being reflected also in risk assessment and associated emergency planning at the regional and municipal levels.

Portugal was one of the countries[1] contributing to the "non-paper" on National Risk Assessment prepared for the European Commission staff working paper of December 2010; the Portuguese NRA is similar in many respects to those of other EU Member States, but reflects Portugal's unique circumstances and the policy choice to exclude risks of intentional harm. A particular feature of plans for the development of the NRA is the widespread representation of all sectors of society on a consultative sub-Commission within the Portuguese National Platform for Disaster Risk Reduction, created in May 2010 under the auspices of the National Commission for Civil Protection.

Governance framework

Aims and objectives

Portugal's risk management system is regulated by law and based on a territorial management system organised at three co-ordinated levels (national, regional and municipal); the system is manifested in a number of ways including: through a set of land use planning instruments that explicitly considered risks and territorial vulnerabilities; a legal regime defining the National Ecological Reserve (REN), which distinguishes areas of natural hazards which must be taken into account in land use planning; and support for disaster reduction at the sectorial level, specifically to reduce the risk of forest fires, dam or reservoir breaches, floods, urban fires, radiological accidents and accidents under the Seveso regime; legislation defining the institutional and operational framework of civil protection at the municipal level, decentralising responsibilities and resources for disaster reduction.

Within this regime, the primary aim of the National Risk Assessment was to set the basis of understanding risks for the National Emergency Plan, by engendering a better knowledge of existing risks and vulnerable areas in order to define priorities in terms of prevention, preparedness and relief activities. Accordingly, the NRA addresses the full range of disaster risk reduction policies within the NEP, with the objectives of providing:

- Guidelines for regional and local risk analysis and risk mapping, in the form of guidance on risk identification, methods of analysing impact and likelihood, and risk evaluation using a matrix as the means of presenting risks.

- The basis for a risk reduction strategy at national level, including risk prevention, and reflecting Ministerial priorities.
- A basis of evaluating risk as part of the approvals process for projects.
- Evidence for investment in the resilience of critical national infrastructure, particularly in the energy and transport sectors.
- A basis for risk communication to stakeholders in the business and social communities, underpinning programmes of early warning, directly to the public or through radio or television broadcasters. Examples include: a project with TV networks to provide an infomercial about how to use the warning system; projects to establish sirens as a low cost tool to warn the population, and to use social media to interact with smart phones using applications to inform about rapid onset events; a memorandum of understanding with specific national radio and television to inform people in specific situations.
- Risk mapping (risk maps are in widespread use for land use planning; map are in PDF format and not interactive.
- Scenarios for national, regional or local emergency response exercises.

A particular focus since the creation of a National Platform for Disaster Risk Reduction in 2010 has been to use the risk assessment to target work to implement the Sendai Framework in Portugal. Given the breadth of the priorities for action following Sendai, the Portuguese Government has sought to integrate its response into the pre-existing regime under the National Civil Protection Commission. Creating a three year programme of action with a focus on engagement of stakeholders in all sectors of society, and on reinforcing a culture of compliance with building regulation and risk based investment in the resilience of infrastructure. In addition to improve short term preparedness and to work towards longer term climate change adaptation goals. The lead for climate change adaptation policy is formally with the Environment Agency, but these governance arrangements enable the Civil Protection Directorate to use the result of the NRA, informed by analysis of the effects of climate change, to improve the protection of people, property and other assets. This includes a programme on education of risk, teaching how to invest in prevention and mitigation and how to communicate to people about risks.

Risk assessment also informs planning for large scale events such as the potential 2017 visit of the Pope to Portugal. In these cases, the Portuguese government analyse the risk associated with large gathering of people, in addition to risks related to terrorism. Normally, such risks of intentional harm are excluded from emergency planning NRAs but the co-ordination of a single plan (all hazards approach) for all contingencies, and exercising of those plans, was in these cases aided by having a common, event-based, risk assessment.

Transparency and accountability

How is the task of co-ordinating the NRA organised?

There is a National Commission for Civil Protection (CNPC) at national political level with representatives of all ministries which ensures a cross the government approach. It is established by law, and one of its tasks is to commission NRA work, as part of the NEP. The CNPC also acts as the National Platform for Disaster Risk

Reduction[2] (PNRRC). The PNRRC features a consultative sub-commission, that includes the private sector (e.g.,, banks and insurers), universities and media, and can establish ad hoc groups to work over a limited period on specific subjects (for example flood resilience, resilience for schools and hospitals, building regulations, and recovery) and include specialist staff, such as medicals, architects, volunteers or civil engineers.

The CNPC provides balanced strategic guidance on political risk tolerance levels, providing a bridging mechanism between the Council of Ministers – at the highest political level – and the more technical work of the groups subordinate to the Commission.

The NRA is approved, along with the NEP of which it forms a part, by the Council of Ministers; there has so far been no independent validation of the NRA but the voluntary engagement of subject matter experts in the National Platform for Disaster Risk Reduction - including independent, non-partisan, inputs from academics - and the enthusiasm that this brings to the work of the Commission that oversees the National Risk Assessment, has so far rendered such validation unnecessary. Approximately 85% of the civil protection NRA is made public, in Portuguese only.

Multi-level governance and multi-actor participation

National level

The Portuguese National Authority for Civil Protection (ANPC) – effectively the Civil Protection Directorate of the Ministry of the Interior - co-ordinates civil protection and related risk assessment work at national level. Work on the NRA was originally a team effort primarily with the support of the national forest services (forest fires), environmental agencies (for risks of floods, and from chemical plants), health agencies (for heatwaves) and the National Institute for Sea and Atmosphere (which provides meteorological services and also expertise on geological risks (earthquakes) and tsunami) under the Ministry of the Sea. Close links with these organisations enabled the Civil Protection Directorate to trigger the process for gathering information and work together on the first full NRA. Other actors, from the private and other sectors were brought in subsequently as described above. The NRA process (as part of the National Emergency Plan) was followed very closely by the National Commission for Civil Protection (CNPC), which acted as an advisory board. CNPC includes representatives from all ministries, including the ones dealing more closely with specific risk analysis (e.g., Ministry of Environment).

Sub-national levels

The 18 regions of mainland Portugal all carry out risk assessment as part of civil protection work to improve emergency response, prevention and preparedness. Regional risk assessments were due to be concluded for each by 2015 to be adopted by the regional civil protection Commission and then publicly distributed. At municipal level, the mayors of about 300 municipalities have the responsibility to assess the risks of emergency arising in their area and an estimated 200 municipalities have carried out their risk assessment to date, based on guidelines issued by the Civil Protection Directorate. The CPD is planning to develop tools that would improve the ease and reliability of local risk assessment. Local risk assessments are publicly available as are the emergency plans made by local authorities which are based on them. The role of the government here is to ensure that local authorities are aware of guidance and resolutions from the National

Commission (which in any case involves the National Association of Municipalities) by publishing these in the official journal. CPD can then evaluate local emergency plans and local risk assessments for consistency with national guidelines.

Risk analysis

CPD, as the Portuguese National Authority for Civil Protection (ANPC), followed closely the process that led to the publication of the European Commission Guidelines, which were used as a template for the main steps to creating a NRA. The guidelines were adapted but the Portuguese government did not see the need to reinvent the wheel. The process outcome bore a strong resemblance to the NRA of other EU Member States whom Portugal had collaborated in producing the "non-paper" in 2009/10.

Terminology was used according to civil protection usual practice, taking into account definitions adopted in the EC Guidelines, with some adaptations to the national context. The NRA includes an explanation on the terminology adopted. The Portuguese Civil Protection Act[3] distinguishes between “major emergency” (*acidente grave*) and “catastrophe” (*catástrofe*), the latter being more severe than a “major emergency”.

Scope

The first NRA considered a set of 26 natural and man-made hazards. It did not include intentional acts; nor does it include pandemics although the possibility of adding the risk of infectious disease might be considered for future iterations. Intentional acts were excluded because the National Emergency Plan does not include them in its scope. There is a National Security Council with its own risk evaluation for security, which is not made available to the public, and responsibility for this work (and for "cyber-security") is under the responsibility of the Prime Minister. The National Civil Protection Authority is part of that process, ensuring that national response plans for intentional or malicious acts are consistent with those having similar effects but arising from natural or man-made hazards or accidents.

Hazard identification

The Portuguese ANPC is responsible for identifying hazards for the NRA, working with different organisations dealing with specific risks (e.g., Environment Agency, Forest Services, Meteorological Institute, etc.) and facilitating compromises in case of a multiple or shared "ownership" of risks. "Reasonable worst case scenario(s)” are defined based on historical experience to examine the risks, which describes basic information related the causes and expected consequences. As an example, risk scenarios for a seismic event was based on the most serious event in recorded history, which was the 1755 quake estimated to have registered 8.1 on the Richter Scale. This was one of 26 main kinds of risk identified for the NRA by ANPC and lead departments and agencies (see 1.3 above) which used a variety of methods to develop the scenarios for use at the national emergency planning level.

Consideration is given to cross-border events, using links with Spain to identify cross-boundary risks of flooding, radiological leaks from nuclear power stations, dam inundation or forest fires originating in the border areas or further afield.

Impact analysis

The methodology for assessing risk combines the likelihood of a hazard's occurrence with its consequences. Scoring for impact uses the familiar criteria of consequences for people (these are given a greater weight than other kinds of impact), disruption of material goods and services, and the environment; the scales are stepped, and quantitative analysis is used as far as possible.

Likelihood and plausibility analysis

In scoring for likelihood in the National Risk Assessment, the Portuguese NRA considers the historical pattern of recurrence of hazards, projecting these estimates 5 years ahead (which is the period of time legally assigned for updating the National Emergency Plan).

Risk evaluation, monitoring and re-evaluation

Risk evaluation in presented in the format of a risk matrix showing the relative positioning of risks taking into account likelihood and impact. A disaggregated presentation by type of impact is not included – however the related data is available to the public and a disaggregated matrix may be drafted, if needed. Regular reviews are undertaken by ANPC. On a formal basis, the NRA should be reviewed by the end of 2018 (back-to-back with the update of the National Emergency Plan). Multi-risks are not included but risk mapping is a feature of the current NRA.

Communicating the results of National Risk Assessment

Using the National Risk Assessment to raise awareness about risks

Communication to decision-makers is assured via the National Civil Protection Commission, which assures the dissemination of results to each ministry. Communication to the public is assured via ANPC's website, and this includes both the main results and the basic methodology. Some sensitive information was withheld from the public – for example sensitive information provided by the private sector.

Main lessons learnt and policy outcomes

Lessons learnt

The National Risk Assessment process ensures lessons are systematically learnt through the review of methods as well as of available data. Lessons to be considered in the next update may include adjustments in thresholds for some impact criteria or the inclusion of other hazards (e.g., extreme wind/winter storms, pandemics).

Benefits

What are the observed benefits of the NRA, and how are they measured?

The primary benefit identified by the ANPC is the creation of a common understanding of the risks that affect the country, and the inherent hierarchy. The NRA did identify the main risks as earthquake, fires, floods, tsunami and chemical (Seveso) category incidents. It was not possible to say how much added value there was from producing an NRA that on the whole enjoyed consensus across government (there remain differences of opinion on what risk is higher than the others; and there was some debate

amongst academics; but generally the ANPC received a lot of support). This common framework of the NRA did allow improved comparative analysis and clearer definition of priorities for risk prevention and mitigation, feeding into several national processes.

- DRR and Sendai - see end-note 1.
- Climate change adaptation.
- Provision of public information and raising risk awareness.
- The NRA and the local RA are used for local land use planning.

Limitations

Two main limitations were evident in the first NRA, both concerned with the maturity of the process and the data and therefore likely substantially to be reduced in the next iteration due probably in 2018.

- The government only had a very short time to conduct the risk assessment. It asked for an evaluation of the National Emergency Plan to be performed by 2011; but to do this required first assessing risks. The NRA was completed in 2012 and adopted in 2013 by the Council of Ministers at the same time as the National Emergency plan; an additional technical adoption by National Commission for Civil Protection with representatives from several ministries also took place. Time constraints meant there was room for improvement and the work was done primarily by government bodies. It took account of some academic expertise, but not NGOs or the private sector. This was too short a time frame, so not enough account could be taken of the knowledge of academics and universities.
- The NRA in Portugal does not deal with intentional acts- e.g., terrorism, only with natural and technological disasters. One of the challenges to overcome has been on topics that are perceived to be the domain of public health – e.g., pandemics, heat waves and cold waves are seen as health issues not a civil protection issue. While extreme temperatures were brought into the NRA, pandemics were not considered due to the lack of data.

Policy outcomes

There is ample evidence that the first Portuguese NRA has contributed towards building a culture of risk management at national, regional and local level within Portugal; and that this is helping to reinforce an already active programme of capability building since Portugal established its own National Platform for Disaster Risk Reduction in May 2010, by indicating what the priorities should be for investment of what are evidently scarce resources of money and materials. The government has developed a legal and administrative framework that enables good practice in risk assessment and integrated emergency planning to be cascaded throughout the country, embedding risk consciousness in the people and mobilising public sector, businesses and communities to look after their own safety – all in a climate of significant resource constraint.

Notes

1. The countries were: France, Germany, Netherlands, Portugal, Slovenia, Spain and the UK.

2. Portugal subscribed to the Hyogo Framework for Action (HFA) in 2005 and has taken, since then, concrete steps to integrate and streamline Disaster Risk Reduction (DDR) into national development strategies, recognising the importance of DRR for the promotion of sustainable economic growth and progress.

The need for increased coordination among the relevant stakeholders led Portugal to create an institutional basis for the already existing informal settings and arrangements to promote DRR. The establishment of the Portuguese National Platform for Disaster Risk Reduction, in May 2010, was a key issue towards better coordination of prevention, preparedness, and response activities.

The Portuguese National Platform for Disaster Risk Reduction Work Programme for the triennium 2015 – 2017 considers the following main objectives:

1. Reinforce the exchange of good practices and lessons learnt:

- Local level

- Flood risk and Land Use Planning

- Private sector resilience

- Climate Change Adaptation

2. Increase the number of municipalities in the UNISDR Making Cities Resilient Campaign

3. Assess seismic safety on schools

4. Implement expert teams on seismic post-damage assessment

The activities are developed under the umbrella of 6 Working Groups:

- WG1 - Safety of schools and health facilities
- WG2 - Seismic post-damage assessment
- WG3 - Resilient cities
- WG4 - WG Floods
- WG5 - Private sector
- WG6 - Climate change

In addition to these activities, the national level is supporting the local level in increasing disaster risk reduction measures by developing several activities:

- All municipalities have civil protection emergency plans that are being reviewed according to the specific legislation issued in 2008 and updated in 2015.

- Special emergency plans for specific risks have been developed, which include the municipalities that can be affected by these risks, e.g., earthquakes and tsunamis, floods and forest fires.

- Internal and external emergency plans for Seveso industries, according to legislation which transposes the Seveso Directive into the national legal framework. The Seveso industries external emergency plans refer to the municipalities where the industries are located.

- Operator security plans for critical infrastructures, according to legislation which

transposes into the national legal framework the Directive for the Protection of European Critical Infrastructures.

- Spatial planning considers risks affecting municipalities and regions in order to organise construction and land use, avoiding increased vulnerabilities in the territory (also under appropriate national legislation).

- Exercises at national and local level are regularly undertaken in order to test emergency plans. In addition, under the national Fire Safety Regulation, special attention is given to high risk buildings such as schools, health facilities, hotels and residences for elderly people, where an exercise takes place once a year with the involvement of local authorities and civil protection agents.

- Concerning information and knowledge supply and sharing, useful for the municipalities to develop their work, several instruments can be referred to such as: (i) the Emergency Planning Information System (http://planos.prociv.pt); (ii)Technical Guidebooks on risk analysis and emergency planning; (iii) risk maps delivered to the municipalities affected by each considered risk; (iv) results of scientific studies developed with the scientific community; (v) data on natural and technological accidents occurred (inventories).

- More than 300 civil protection clubs are active in schools all over the country for children between 6 and 10 years old.

- Nine cities in Portugal joined the Campaign "Making Cities Resilient".

3. The General Law for Civil Protection (Law 27/2006)

References

Commission Staff Working Paper (2010), Risk Assessment and Mapping Guidelines for Disaster Management.

Further reading

OECD, UNISDR EUR & EC (2014), Finland peer review report 2013 - Building resilience to disasters: implementation of the Hyogo Framework for Action (2005-2015). Available at: https://www.unisdr.org/we/inform/publications/38523

Chapter 20. SLOVAK REPUBLIC

In respect to Slovak Republic, the main purpose of the National Risk Assessment is to improve preparedness and resilience in the local municipalities and to fill the gaps in their capability and capacity to respond to emergencies. The NRA will also create a better understanding of the prevailing threats in their areas. The full standard risk assessment process is scheduled for completion in 2020. The plan includes a risk matrix and a comprehensive joined up national database. The Slovak Republic Government has a very open approach to both transparency and accountability. The lead is taken by the Crisis Management Department with a well-developed cross cutting approach to accountability. A detailed risk register is made widely available to all stakeholders to improve business continuity, community resilience and risk awareness. In addition this overall risk assessment process is reinforced by legislation. The target by 2020 is a well-developed risk matrix and the consolidation of the NRA process.

Key Words: Bottom Up approach; Consolidation of NRA process; Capability and Capacity; National Risk Register; Preparedness and Resilience.

Introduction

A national risk assessment for Slovak Republic was proposed in the 2015 National Strategy for Security Risk Management (NSSSRM) of the Slovak Republic, as the outcome of one of five strategic areas covering:

1. A single regulatory and legal framework for effective risk management.
2. Risk management of security threats and sustainable development designed to build risk reduction. Measures into programmes and plans for the sustainable development of the Republic.
3. Implementation of national risk assessment in the Republic.
4. Improving preparedness and response at all levels (national, regional and local levels) of government.
5. Better use of science, research, learning, education and training.

Planned activities for strategy area 3 (risk assessment) are scheduled for completion during the years 2016 – 2020. This is being designed as a "bottom-up" system, and there is at present no National Risk Matrix, but a large amount of data has been collated to populate such a matrix once agreement is reached on a standard risk assessment methodology. This data is primarily of use for the first of the two main priorities for the Slovak Republic: the mapping of risk to help protect people and property throughout the country from the main current, recurring, risks of flash flooding, river flooding, landslides and other natural hazards. The government expect in the next three to four years to have developed from this and other baseline data a National Risk Assessment and matrix illustrating higher-level strategic risks to key assets in the country, in particular critical national infrastructure, reflecting early onset signs of climate changes and assisting cross-boundary cooperation in strategic risk management with neighbouring countries.

The legislative underpinning for the National Strategy has been in development since the 2002 Constitutional Act (no 227/2002) on state security in time of war or other states of emergency, which established a National Security Council, and Act No 387/2002 which provides crisis management machinery at the state level including a crisis staff and clarification of the responsibilities of lead government departments; these Acts, and subsequent legislation including on the role of local government, protection of critical infrastructure, flood protection, are now being reviewed for any shortcomings in the provision for constitutional bodies (ministries and other central government authorities, local state administration and self-governing authorities, municipalities) to assume and carry out their responsibilities.

Governance framework

Aims and objectives

From the National Strategy for Security Risk Management (NSSRM), it is clear that the main purpose of a National Risk Assessment will be to fill gaps in the capability and capacity of local municipalities to respond to emergencies by increasing understanding of the vulnerability of populations in their area of responsibility to the most common hazards, and to understand also their most common impacts. A National Risk Register

will raise popular awareness, to ensure that the main risks are fully identified and so to improve preparedness and resilience. The strategy points out that the risk of emergencies is regularly analysed at national and regional level. As a result, a consolidation of an all hazards approach is now planned which will be addressed in an action plan for the period 2016/2020. This includes the development of a risk matrix and the potential for a comprehensive joined up national data base where the risks can be identified in their entirety and the following gaps can be addressed.

1. A comprehensive database of emergencies and damage caused.
2. Improvements in the level of awareness and knowledge of threats and their impacts that are insufficient for effective risk management.
3. Improvements and standardisation of the risk assessment processes which can be understood in the various different sectors.
4. Putting in place an information system for sourcing, collection and distribution of data required for effective risk assessment.
5. Improvements in adopting the knowledge base for risk assessment, by citizens, volunteers and communities, to enable them to carry out preventive preparatory and protective measures.

In the longer term, the intention is that national risk assessment, and a risk management culture embedded at all levels, will aid the sustainable development of society in the face of strategic risks arising from and because of climate change and other major societal trends.

Transparency and accountability

The overall responsibility for co-ordinating work on a NRA rests with the Crisis Management Department within the Ministry of the Interior, which has the lead for most of the actions under Strategy Area 3 of the NSSRM. Some actions (for example relating to cyber security, building regulations, financial instruments) are allocated to other Ministries within an integrated risk system that recognises the cross-cutting nature of risk management.

All departments with lead responsibilities designated (by Act 575/2001) are required (by Act 387/2002) to make available information about hazards or threats in their area of responsibility, to analyse these risks and take measures to mitigate them.

Subsequent Acts prescribe the responsibilities of regional and local government, the emergency services, owners/operators of national infrastructure assets, and others to manage the risks in their areas. Similarly, the NSSRM sets out the lead responsibilities for all actions in the plan to overhaul the national crisis and risk management system.

The government of the Slovak Republic believes that one of the advantages of a detailed risk register comes from making the information widely available in order to improve business and community resilience, and this is reinforced by legislation (Act no 42/1994): information is made available on publicly available, seismological and meteorological websites, for example.

Multi-level governance and multi-actor participation

Following various Acts since 2002, the recognised crisis management institutions in Slovak Republic include the following:

- Government of Slovak republic
- The Security Council
- Ministries and other central state bodies
- The National Bank of Slovak Republic
- District Offices
- Security Council of District Office
- Municipalities.

Security Council is advisory body at national level and district level. It is steady body. Head of Security Council of Slovak republic is Prime minister. Head of Security Council at district level is head of district office.

Crises staff is executive body of crisis management institutions at all level. Head of central crisis staff is Minister of Interior. Head of crises staff at district level is head of district office.

Responsibility for bringing together all the parties needed to contribute to emergency response including the emergency services that (under Act 129/2002) are required to act in an increasingly integrated fashion.

Risk analysis

The NSSRM specifies that risk management will be based on an understanding of the frequency, size and impact of threats; and on the social and structural vulnerability of the population to the threat. The vulnerability assessment is thought to be a major challenge.

Scope

The NRA will be an all-hazards risk assessment including natural and man-made hazards. The outline risk identification template currently in development indicates that the risks listed at Table 20.1 are within scope.

Table 20.1. Risks within the scope of the Slovak Republic's NRA

Risk area	Scope
Disease	Human disease
	Plant disease
	Animal disease
Geophysical	Landslide
	Avalanche
	Volcano
	Earthquake
Hydrological	Flood
	Drought / water scarcity

Table 20.1. Risks within the scope of the Slovak Republic's NRA *(continued)*

Risk area	Scope
Meteorological	Windstorm
	Extreme temperatures
	Storm and flash flood
	Long term inversion
	Snow calamities
	Others (icing, fog, hail)
	Damage to territory by natural events
Man-made	Technogenic
	Biological agents – deliberate
	Biological agents – accident
Traffic accidents	Road
	Cableways
	Air
	shipping
	rail
Industrial accidents	Mine fire
	Dangerous chemical agents leak
	Radiological incident
	Water buildings disaster
Sociogenic	Migration
	Conflicts – economic, ethnic, religious, ideological, inter-state
	Public order threat
	Explosive devices
	Terrorism - CBRN
	Terrorism - other
Banking and finance	Monetary, currency & finance
	Economic "violation"
Infrastructure disruption	Transport & logistics
	Postal services
	Energy
	ICT
	Agriculture & food
	Health service/ healthcare
	Water & waste-water
	environment

Hazard identification

At the current stage of development, each of these types of risk is categorised according to the level at which planning needs to take place (i.e., which of the following planning levels apply: national, regional/county, district, and local); more than one planning level may apply to some risks – for example the risk of plant disease applies to all levels, but mass landslides are reserved to the national planning level. Collation of data to support risk assessment is delegated to a lead department; for many risks the district level of government is looked to provide historical data on the frequency of hazards and on the level of exposure which is measured primarily by the number of people who live in areas exposed to a particular hazard. It is not yet clear whether the approach to an NRA/Risk Matrix – when this happens – will be based on a probabilistic approach or on one based on scenarios - the most common method of risk identification at a national level.

Impact and likelihood analysis

At this stage, the data being collected focuses on the numbers of people exposed to each hazard in each location, the extent of the geographical area (in km2) threatened, the three most important consequential hazards (e.g., power outages as a secondary consequence of flooding), and whether there is any potential overlap with neighbouring districts or municipalities. It is not yet clear how this information will be brought together and brigaded under the impact and likelihood headings in a conventional NRA.

The data being gathered by lead departments includes a view from District Offices of the number of times that a hazardous event will occur in a given location over a given period. This is a current or historical figure. Yet, the analysis for each risk type also contains a broad indication of whether, at the national level, officials believe that the trend is for the risk to increase, decrease or remain broadly at its existing level. In most cases, the risk seemed to be steady or increasing.

Risk evaluation, monitoring and re-evaluation

This aspect was not assessed for Slovak Republic.

NRA Excursions

Risk mapping is widely used.

Communicating the results of National Risk Assessment

The Government of the Slovak Republic believes that one of the advantages of a detailed risk register comes from making the information widely available in order to improve business and community resilience, and this is reinforced by legislation (Act no 42/1994):information is made available on publicly available, seismological and meteorological websites. It is also considered necessary to publish this in an easily understood format for public consumption.

Main lessons learnt and policy outcomes

Lessons learnt and benefits

At this stage, the Government of the Slovak Republic has decided as an act of faith that improving popular understanding of risk will benefit national resilience, and that the

best approach to a NRA is to build understanding from the bottom up – the preferred approach of emergency risk management experts. This entails gathering data in a quite detailed way in local areas most affected by commonly recognised hazards, and then – at a later stage – extrapolating from this very detailed data base to inform an NRA. This is thought by policy-makers and practitioners to be the best way of fulfilling their primary obligation to protect people. It can also aid the identification of planning priorities for local, regional and national level planners; it can help in identifying priorities in both operational and financial/budgetary terms, and so save money; and it can also contribute to work already well advanced to develop international cooperation, especially in the area of early warning (e.g., the RAS BICHAT early warning system, based on the European standard ECURIE system, for warning of Chemical or Biological Hazards).

Looking ahead, the authorities in Slovak Republic have said that the next steps should be the consolidation of the national risk assessment process to include development of a National Risk Matrix before 2020 and the consolidation of the (formidable amounts of) data being collated onto one accessible database instead of the number of systems that currently exist, preferably built on a mapping database structure.

Limitations and challenges

The bottom-up approach presents challenges acknowledged in the NSSRM of clearly separating out the risk factors that contribute to the impact assessment, and to the likelihood assessment. The latter is a function of the nature of the hazard, how often and how severely it occurs, and what national assets (mainly people and buildings) are exposed to it; this can be hard to calculate at a national level from the mass of local data that has been collected without using the scenario method of identifying the risk at different levels of intensity: worst case; expected case; reasonable worst case etc. Calculations of impact need to take into account both the primary and secondary impacts (which the Slovak government does) and to assign a value to that based on approximate impact criteria and weightings that reflect their value to the nation. The approach of identifying trends that are thought to portend a change in risk levels in the future will need to distinguish between those that make a hazard more likely, and those that make it more potentially harmful.

Reference

Presentation from the Ministry of Interior of the Slovak Republic (2014), Risk Assessment in the Slovak Republic.

Chapter 21. SPAIN

The development of the National Risk Assessment (NRA) in Spain was built around the revision of the National Security Strategy of 2013 and in accordance with legislative requirements namely the 2015 National Security Act. Governance arrangements in Spain, similar to many other countries, have taken the form of an all of government/all of society approach to risk in the context of the taking a global view of new and emerging threats, as well as existing well known threats with an integrated and co-ordinated plan of effective mitigation. The overall objective of a national risk assessment for Spain as set out in this chapter is to provide evidence-based advice to the Prime Minister and his/her office , to provide evidence based advice on the overall risk profile and to provide input to Spain's National Security Strategy in accordance with legislation. At the time of writing, the NRA had not been brought to government due to transition arrangements.

Key Words: Collaboration; Integrated and co-ordinated action; Public and private collaboration; Strategic risk assessment; Operational risk analysis.

Introduction

At the time that the OECD interviews took place; officials in the Office of the Prime Minister were preparing proposals for an incoming Government on the development of a National Risk Assessment that would support eventual revision of Spain's 2013 National Security Strategy in accordance with the provisions of the 2015 National Security Act. Accordingly, the features of a Spanish NRA that are discussed below are provisional upon the agreement of the new Government which came into office in October 2016.

Governance framework

The 2013 National Security Strategy, a revision of the 2011 NSS, was designed to provide strategic level direction for the continued evolution of Spain's approach to the significant and continuing changes in the global security environment in recent times the early C21st. Spain, like many fellow OECD Countries, have adapted its national security system to include novel features: a comprehensive (and global) vision of national security, recognising new threats as well as traditional ones; engagement of citizens and collaboration between public and private sectors and all the Public Authorities in their areas of responsibility; a reformed institutional National Security System that is at the service of everyone and favours integrated and co-ordinated action in all fields of security.

Aims and objectives

The clear aim of a National Risk Assessment will be to provide relevant and evidence-based advice to the Prime Minister on the overall risk profile of the nation, to inform development of a successor to the 2013 NSS which will review the current risks and priorities in accordance with the 2015 National Security Act. The current priorities are set out in Table 21.1.

Table 21.1. 2013 National Security Strategy: Priority Areas of Action

Area of Action	Objective
National defence	To address armed conflicts that may arise as a consequence both of defending exclusively national interests or values – and require individual intervention – and of defending shared interests and values in accordance with Spain's membership of international organisations such as the UN, NATO and the EU, in which case intervention would be with other Allies or partners, pursuant to their founding treaties
Combatting terrorism	To neutralise the threat of terrorism & reduce society's vulnerability to its attacks, addressing the processes of radicalisation which can precede or underpin it
Cyber security	To guarantee secure use of information networks & systems by strengthening our cyber-attack prevention, detection & response capabilities
Combatting organised crime	To prevent organised criminal groups from settling, to bring to justice those that already operate within Spain's borders & to impede the consolidation of their criminal forms of action.
Economic and financial security	To promote sustainable economic development, mitigate market imbalances, combat criminal activities, enhance Spain's international economic presence & guarantee the resilience of essential economic & financial services
Energy security	To diversify energy sources, guarantee the security of transportation & supply & promote energy sustainability
Non-proliferation of weapons of mass destruction	To prevent proliferation, impede terrorists or criminals from gaining access to dangerous substances & protect the population
Management of migration flows	To prevent, control & manage migratory flows across Spain's borders, which also constitute outer limits of the EU
Counter-intelligence	To adopt counter-intelligence measures in defending Spain's strategic, political & economic interests in order to prevent, detect & neutralise concealed aggressions from other States
Protection from emergencies and disasters	To establish a national protection system for citizens that guarantees a suitable response to different types of emergencies & disasters stemming from natural causes or from human action, whether accidental or deliberate
Maritime security	To promote a security policy in maritime space in order to preserve freedom of navigation & protect maritime traffic & critical maritime infrastructure; to protect human life at sea; to prevent & respond to criminal activities & acts of terrorism carried out in this environment; to protect & preserve the coastline, marine resources, the marine environment & underwater archaeological heritage; & to prevent & respond to disasters or accidents in the marine environment.
Protection of critical infrastructure	To strengthen the infrastructures which provide essential services to society

Source: The Presidency of the government (2012).

Although there are risk assessments in these areas of subordinate strategy, these are conducted at an operational rather than strategic level, using methodologies that are particular to each area, and the recommendation of officials in the Prime Minister's Office is likely to be that revision of the NSS would benefit from collating risks in each of these subordinate strategy areas using a methodology that is broadly consistent across

the board; and that this would assist in decisions at a strategic level about the balance of investment needing to be made in security and resilience.

Transparency and accountability

The new National Security System introduced under the 2013 NSS and 2015 NS Act is based on the following principles:

- leadership – provided by the Prime Minister
- integrated and co-ordinated functioning – of all the Public Authorities with responsibilities in national security matters
- optimisation – to ensure effective use of available resources
- modernisation of structures and processes related to national security among Public Authorities
- involvement of civil society and fostering of a security culture
- public-private collaboration
- handling (sharing) of information and knowledge
- necessary transparency.

The Prime Minister has the role of directing, leading and giving impetus to National Security Policy. In performing these functions, the Prime Minister relies mainly on the National Security Council (NSC) whose members include the Deputy Prime Minister and Ministers for Defence, the Interior, Industry, Energy and Tourism, Foreign Affairs, Treasury/Public Administration, Development, the Economy/Competitiveness, the Chief of Defence Staff, State Secretaries and the Director of the Prime Minister's Office. In any event, the rest of the ministerial departments as well as other authorities, senior public officials, private-sector actors and experts may also be convened to attend when the Council needs to discuss issues related to their areas of responsibility or knowledge. Specialised Committees (set up by the NSC) support the Council in each of the 12 strategic areas of action in the 2013 NSS. National Crisis Management instruments were also set up under the 2015 Act including a National Situation Centre whose director has the responsibility for making recommendations on a National Risk Assessment if and when commissioned to do so.

Multi-level governance and multi-actor participation

As noted above, regional and sub-regional authorities are engaged in the NSC and its specialised sub-committees as the subject-matter requires. This is done in accordance with the principle of integrated and co-ordinated functioning of all public authorities with responsibilities for national security matters. These authorities also have their own regional security structures and systems within the principle of subsidiarity.

Risk analysis

The likely form that Spain's NRA will take is a strategic risk assessment covering both domestic risks and the possibility of Spain being affected by global risks. In that sense it would resemble more the Dutch NRA, which includes external risks to sovereignty as well as internal risks posed by natural hazards, man-made accidents, and malicious actors, and the UK National Security Risk Assessment, which includes broader geopolitical risks and threats to the economy.

Scope

The purpose of Spain's NRA being to review the risks covered by the 12 priority areas of action, the scope of the assessment covers in principal all 12 areas and any other risks that might emerge which entail a similar potential for damage to the security of the nation, the health and welfare of the population, the health of the economy, and for disruption to the essential services provided by critical national infrastructure. Each priority area of action defines the political objective and several strategic lines of action for each of them. These lines of action provide a framework for the specific actions required to preserve National Security.

Hazard identification

The NRA is likely to be comprehensive from the outset, being based on scenarios that illustrate the range of risks present within each of the 12 strategic areas in the 2013 NSS, plus any others that emerge through consultation with the principal stakeholders in Government and among other Public Authorities. Since there is already operational risk analysis in many of the government departments with lead responsibilities for the current national risk portfolio, it is unlikely that Spain will need to adopt the approach of building up its NRA from an initially small selection, as other nations have done. The kinds of scenario – i.e.: whether they are best case, worst case, or somewhere in between – has not been decided but the indications are that the government will lean towards worst case scenarios.

Impact and likelihood analysis

The criteria for judging impact have not been decided but are likely to include consequences for: safety and security of the populace; maintenance of essential services; and continuity of government. Current criteria in use – i.e., for emergency planning against the event of natural hazards which are designed to assist in land use planning - are more suited for a strategy of prevention and security than for emergency response planning, so there may need to be some adaptation so ensure that all elements of the risk (nature of the hazard or threat; exposure; vulnerability; and impact) are addressed in the assessment.

The likelihood of damage being sustained at the level portrayed in the scenario will be estimated probably on a five-point scale, with the highest point of the scale representing a judgement that a risk will be as likely as not to materialise in a 5 year forward-looking period. The nature of the risks, known return periods, the extent of exposure and vulnerability of the population, will be taken into account in considering where on the scale the risk should sit. Consideration will also need to be given to a method of estimating the plausibility of malicious threats by terrorists, criminals and hostile states, which are prominent categories of risk in the 12 strategic lines of action: the method in use by other nations, which takes into account the assessed capability and motivation of perpetrators of malicious acts, and the vulnerability of their intended victims, may suit the Spanish approach also.

In both impact and likelihood assessments, a stepped (or logarithmic) approach is likely to be taken, reflecting the degree of uncertainty in the estimates, so that each level on the scale is an order of magnitude different from its predecessor.

Risk evaluation, monitoring and re-evaluation

This aspect was not assessed for Slovak Republic.

NRA Excursions

Risk mapping is widely used in Spain, and is likely to form a basis for assessing the relative significance of the risk of certain common hazards (for example flooding) in the National Risk Assessment. The 2013 National Security Strategy recognises that there are risk drivers, and risk multiplier effects, that can generate new risks or threats, or amplify or make worse the effects and likelihood of existing risks. These include social factors (poverty, inequality), ideological extremism, demographic imbalance, climate change, and widespread misuse of new technology. The long term effects of climate change in particular will be a factor to be taken account of in the NRA.

Communicating the results of National Risk Assessment

No decision has been taken on whether to publish some kind of public Risk Register. The 2013 NSS is, however, a public document and it is likely therefore that there will be a risk communication element - excluding sensitive elements – to the successor document to ensure transparency and the involvement of civil society and businesses which are two of the principles on which the NSS is being built.

Furthermore, an Annual National Security Report is approved by the National Security Council each year since 2013, which is then submitted to and debated in Parliament. This Report presents the evolution of the National Security System, as well as a review of the state of its twelve component areas according to the development of the existing challenges in this field over the course of the year, and as a consequence of actions carried out.

Main lessons learnt and policy outcomes

Lessons learnt and benefits

There is no NRA at present and therefore no lessons identified. Benefits expected are:

- The ability to test the risk judgements underpinning the (currently 12) strategic lines of action and, possibly, to provide a weighting to each area in terms of the potential for harm to objects of value to the Spanish state and its people.
- The ability to identify new threats and hazards, particularly the new global risks arising from the interaction between traditional hazards and new vulnerabilities that are likely to be endemic to complex industrial and societal networks, and black swans.
- The ability to resolve differences and secure consensus on the priorities for action in the NSS, and to facilitate wise decisions on investments in security and resilience.
- To provide an initial basis on which the effects on Spain's national risk profile of other future trends and megatrends – particularly the effects of climate change on the natural environment - can be tested.
- To underpin a national exercise programme (current practice is to hold a Tier 1/Category 1 national exercise every two years), besides the participation on

strategic political level exercises organised by the international organisations Spain belong to, especially EU and NATO.

Limitations and challenges

It is too early to say what the challenges will be, although the effort to reconcile 12/13 different risk analysis methodologies will be considerable.

Reference

The Presidency of the Government (2012), The National Security Strategy Sharing a Common Project. Available at: http://www.lamoncloa.gob.es/documents/estrategiaseguridad_baja_julio.pdf

Chapter 22. SWEDEN

This chapter outlines the current NRA process for identifying risks in Sweden which is now called the National Risk and Capability Analysis. The purpose being to foster more informed analysis of the major risks that Sweden as a whole, is likely to face. The Swedish Civil Contingency Agency (MSB) is the lead agency in developing the NRA process which began in 2012 and continued up to 2016 with a number of iterations culminating in the 2016 version. This version contains a bottom up approach to risk and vulnerability assessment with a top down co-ordinated approach to risk assessment. This chapter discusses the methodology for hazard identification/analysis and vulnerability, and impact analysis in some detail. The results of the NRA process is widely available therefore there is widespread awareness of the risk profile by Swedish Society.

Key Words: Bottom up /top down approach; Scenario Analysis; Stakeholder involvement; Work in progress.

Introduction

This report was produced following interviews with the Swedish Civil Contingencies Agency (MSB) in late 2013 and describes progress with scenario analysis at the national level at that time. Since then, the Swedish government has continued to work with scenario analysis, producing a third a fourth and a fifth National Risk Assessment in March 2014, 2015 and 2016. The focus of this work has changed, from scoring risk and identifying the most serious for the Swedish people. In addition to assessing vulnerabilities and capabilities as an essential first step towards identifying risk management measures both for the emergency preparedness system and for the population as a whole. The resulting product – entitled the National Risk and Capability Analysis – is used to analyse capabilities both for prevention and for response. The MSB has complemented this approach with a programme of exercises, and evaluations of real life events, with the same objective. In 2015, Sweden began collaboration with Canada on risk and capability assessments with a view to developing systematic methods of capability assessment.

These developments suggest that Sweden has focussed on the main purpose of risk assessment, which is to provide information that can be used to develop risk management capabilities. A more detailed report on Swedish work on National Risk Assessments up to 2015 has been included because it demonstrates how one nation has gone about using risk assessment as a tool to aid in the governance of critical risks.

Swedish National Risk Assessment –2012-2015:

The Swedish Civil Contingencies Agency (MSB) published the first National Risk Assessment in 2012. Its methodology was largely inspired by the "Commission Staff Working Paper on Risk Assessment and Mapping Guidelines for Disaster Management"(European Commission, 2010), and the final report identifies specific points of divergence. The purpose of the NRA is to foster more informed analysis of the various major risks that Sweden's society as a whole is facing, as well as increase capacity to prevent, manage and recover from serious incidents and events. In future this may facilitate co-ordination, prioritisation and the building of consensus in a country's system of emergency preparedness. In the 2012 NRA, an insufficient number of risk scenarios have been assessed, however, to enable the prioritisation of specific measures.

The NRA process built on the results of a preliminary risk identification phase that was published in 2011. Several rounds of consultations with experts resulted in pairing down the number of particularly serious or national events to 27 in 2012. Of these, MSB developed eleven risk scenarios, and completed assessments of the likelihood, impact and uncertainty for seven of them. From 2012 to 2015, fourteen scenarios have been analysed. Impacts are assessed by the harm that would occur to human life and health, the economy and environment, or political and social functions. The results of the assessments are plotted in a risk matrix (Figure 22.1).

The risk matrix provides an overview of the assessments of the various events' likelihood, impact and uncertainty. In accordance with these, among the risk scenarios analysed, the highest risks were found to be associated with a fuel shortage leading to disruption in the food supply, failure of a large dam on a river and a prolonged heat wave. The most likely national risk events to occur are a school shooting or a prolonged heat

wave. The risk scenarios that would have the greatest impacts are a major fire on a cruise ship, disruption in the food supply due to fuel shortages and the failure of a large dam on a river. The assessments of a prolonged heat wave and extensive disruption to the Global Navigation Satellite System were found to have the highest degree of uncertainty.

MSB has sought to involve as many emergency management stakeholders as possible in the NRA process, and in its communications with them it openly accounts for the difficulties and choices involved in issues related to methodology. The risk identification and scenario analysis phases are carried out jointly with a large number of experts and key figures from different agencies, sectors and levels of the Swedish civil contingencies system. These workshops have helped the participants make valuable contacts and foster a deeper understanding of the complexity of events, as well as of inter-dependencies and vulnerabilities in the response to emergencies. Nevertheless, MSB considers that the process and methodology developed and tested in 2012 require improvement and additional development.

This report accounts for the status of the NRA in 2013. Since then new NRA-reports have been published every year, which include revised scales for assessments of likelihood and impacts as well as identification of key capabilities in dealing with the scenarios in order to form a strategic basis to further develop civil contingency. MSB has developed a method for incorporating assessments of capabilities related to the scenarios and has published English versions of all post 2013 NRA-reports.

Governance framework

The Swedish Civil Contingencies Agency (MSB) is mandated by Cabinet to act as lead co-ordinator for the NRA process. MSB published the Swedish National Risk Assessment 2012, which sets out an agreed methodology, identifies in principle 27 national risks, develops 11 risk scenarios and analyses seven based on assessments for impact, likelihood and uncertainty. Sweden has in effect complemented a previously Government mandated "bottom-up" approach to risk and vulnerability assessments conducted at local levels with a top-down, co-ordinated approach to risk assessment.

Aims and objectives

The National risk assessment was carried out for three identified purposes:

- To create a common understanding of the serious risks facing Sweden.
- To improve the design of measures related to national emergency preparedness planning for a safer society.
- As a complement to analysis of emergency management capability which have not yet been developed.

The Swedish National Risk Assessment 2012 is meant to support the development of civil protection and emergency preparedness at local and regional levels These include private organisations that perform vital societal functions as well as Sweden's capacity to cope with large-scale accidents and crises in collaboration with other countries. The report emphasises the importance of complementing the capacity to cope with more frequently occurring incidents with the ability to prevent and manage unusual events which have more extensive impacts, regardless of the accuracy of the assessments on which the work is based.

Definitions of key terms

The MSB methodology to produce Sweden's NRA defines several key terms:

"Risk" is the weighing together of the likelihood that an incident will occur and the (negative) impacts that this could conceivably have.

"Risk level" refers to a combined assessment of the likelihood of an event and its impacts, as well as the uncertainty in previous assessments. The level cannot be derived solely from an event's position in the risk matrix (where the y and x axes represent impact and likelihood respectively). When two events are of equal value in terms of combined likelihood and impact, but differ with respect to uncertainty, the event with the highest uncertainty is deemed to be the greater risk.

"Uncertainty" refers to the type of knowledge that exists about a particular event and how reliable this knowledge is as a basis for assessing likelihood, and impacts should the event actually occur.

A **"general event"** refers to a hypothetical event (that historically may have occurred) for which context-forming variables such as place, time (season, day of week, time of day), weather etc., have not been specified. It is only the type of event that is being referred to, e.g., a shipping accident.

A **"scenario"** refers to a hypothetical event for which variables such as place, time, weather etc., and their values have been specified.

Transparency and accountability

The NRA process incorporates several practices in support of transparency. MSB issued regulations in 2010 to increase the comparability and transparency of the risk and vulnerability analyses conducted at sub-national levels (MSB, 2010, p.6 and MSB, 2010, p.7) (DSB, 2012, p.13). In addition, the analysis of most risk scenarios includes expert workshops, which have proven valuable when supporting data are scarce or inadequate, and to provide a forum for discussion between experts of different disciplines. During the workshops, experts often identified new issues relevant to the risk assessment, which reinforced the need to validate findings with research.

To control for bias in the use of expert opinion the assessments are followed with in-depth interviews and after the expert workshops their analysis is checked by a desk research literature review. The final result of each analysis is then sent out to civil protection stakeholders for a quality review. The summary report of the NRA is also sent out for a quality review prior to publication by MSB. The quality of the assessments, i.e., the uncertainty assessments, provides an indication of the issues that need to be investigated more closely with other parties.

The risk analysis conducted in the workshops is based on an agreed, clear and open process/methodology, with active participation from government officials at local and national level. The NRA contains as far as possible open information; none of the analyses has been classified at this point.

Multi-level governance and multi-actor participation

The NRA process involves a range of stakeholders from different levels of government. MSB contacted 56 governmental agencies, 16 municipalities, 3 county councils and 14 other organisations to contribute throughout the process. MSB involves these experts, for example, in the assessment of risk scenarios, and to conduct a quality review of parameters to make sure it is realistic, i.e., a reasonable worst case scenario.

Risk analysis

The work process and methodology for the NRA is conducted in six steps:

1. specify what should be protected, i.e., to define the national protection values.
2. risk identification: identification of adverse events.
3. selection of events (risks) for analysis.
4. scenario development of the selected adverse events.
5. analysis of the scenarios: impact, likelihood and uncertainty assessments.
6. synthesis and evaluation of the risks.

Scope

For an event to qualify for consideration in the NRA it must meet the criteria for both a crisis in society and a national event. To be considered a national event, the incident does not need to have extensive impacts in geographical terms. An event that affects only a few municipalities may still be considered a national event due to there being significant numbers of deceased or injured and significant direct costs.[1]

Incidents and events that occur and impact Sweden outside the country's boundaries (such as the 2004 tsunami) are not included in the NRA. However, causes in the analysed scenarios may entirely or partially originate outside Sweden's national borders, e.g. fuel shortage, which leads to disruptions in the food supply (MSB, 2013, p.16).

The National risk assessment methodology revolves around analysis of risk scenarios. Not all events can be analysed thoroughly, thus the process identifies events that could have serious impacts for Swedish society at the national level. By analysing the longer list of general events in light of national protection values, a shorter list was selected for development into risk scenarios (Table 22.1).

Table 22.1. Five national protection values

National protection value	Description
Society's functionality	Covers the functionality and continuity of that which strongly impacts the daily lives of individuals, companies and other organisations (natural and legal persons). It includes the expertise of staff in maintaining the functionality of society.
Human life and health	Covers Swedish citizens, those who live in Sweden, or are there temporarily, and Swedes residing abroad. This includes the physical and psychological health of those affected directly or indirectly (e.g., loved ones) by an event. It also covers people included in the EU's solidarity clause and those included in Sweden's international disaster relief.
Economic values and the environment	Encompasses economic assets, in the form of private and public property, and the value of production of goods and services. It includes environment described as land, water and natural environment, biodiversity, valuable natural and cultural environments (environments in nature created and affected by people), and other cultural heritage in the form of personal property.
Democracy, rule of law and human rights and freedoms	Covers people's faith in democracy and the rule of law, as well as their confidence in society's institutions and political decision-making processes, leadership ability at different levels and lack of corruption and rights abuses.
National sovereignty	Covers control over the nation's territory. This protection value applies primarily when the cause of the event is antagonistic.

Source: Adapted from MSB (2013).

Hazard identification and analysis

The next step in Sweden's NRA process is "Risk identification", which singles out events that may in some way threaten or cause negative impacts to national protection values.[2] The events identified are combinations of a threat to a protection value and the path of contact. At this stage of the process the events are not referred to as risks, but as "general events"; they are depicted without context or an assessment of their likelihood, impact or uncertainty (MSB, 2013, p.28). Between 2010 and 2011, MSB developed and catalogued more than 200 different "general events" from risk and vulnerability analyses that had already been conducted by public agencies. This provided the material to hold a workshop with some 50 representatives from key governmental agencies and county administrative boards. The workshop reviewed the event catalogue to analyse how the national protection values referred to above could be threatened, with a view to identify a potential national event or crisis. The event catalogue was further reduced to those which workshop participants proposed would be interesting to analyse in greater depth. It was not possible to conduct a deeper analysis of all 40 events in the remaining event catalogue. In 2012 the NRA included 27 catastrophic events meeting the criteria for a national event or a crisis in Sweden. Each of these 27 events would threaten at least one protection value, as presented in Table 22.2.

Table 22.2. Indicators for the national protection values

Society's functionality	1.1 Disruptions to everyday life
Human life and health	2.1 Number of fatalities 2.2 Number of severely injured/ill 2.3 Lack of fulfilment of basic needs 2.4 Number of people who need to be evacuated
Economic values and the environment	3.1 Total economic impacts 3.2 Impacts for nature and environment
Democracy, rule of law and human rights and freedoms	4.1 Social unrest resulting in negative behavioural changes 4.2 Lack of confidence in public institutions 4.3 Serious impact on national political decisions 4.4 Lack of control over public institutions 4.5 Impact on Sweden's reputation internationally
National sovereignty	5.1 Lack of control over territory

Source: Adapted from MSB (2013).

From these 27 events 11 risk scenarios were developed:

- extensive disruption to GNSS
- school shooting
- disruption to the drinking water supply due to diesel discharge in Stockholm's sewer water
- fuel shortage leading to disruption in the food supply
- prolonged heat wave
- major fire on a cruise ship

- failure of a large dam on a river
- pandemic caused by influenza virus A/H5N1 (avian influenza virus)
- nuclear disaster with radioactive discharge
- terrorist attack in Stockholm
- spread of social unrest and riots in Sweden

Vulnerability and impact analysis3

Each risk scenario is assessed in terms of its human, economic/ environmental and political/ social impacts with the help of a guide to impact assessments. The human and economic/ environmental impact assessments are guided by quantitative thresholds, whereas the political/ social impacts are assessed along qualitative scales (Table 22.3). These impact category scores are converted to an overall qualitative assessment ranging from minimal impact to very significant impact.

The risk scenarios assessed in the 2012 NRA with the most significant impacts are a major fire on a cruise ship, a fuel shortage leading to disruption in the food supply and failure of a large dam on a river. These three risk scenarios are considered to lead to very significant impacts, but for different reasons. The scenarios "Fuel shortage leading to disruption in the food supply"; "Failure of a large dam on a river" result in very significant impacts for the economy/environment; while a "major fire on a cruise ship" results in very significant impacts for both economy/environment and the human category. The dam failure scenario may also lead to very significant human impacts, but the assessment is uncertain and dependent, to a great extent, on how the incident is managed and on the location of the dam (DSB, 2012, p.25).

Table 22.3. Scales for Impact Assessment

Scale in the risk matrix	Scales for each impact category		
	Quantitative scale, Human impact	Quantitative scale, Economic/Environmental impact	Qualitative scale Political/ Social impact
Very significant	≥ 50 dead and/or >100 severely injured	>SEK 1 billion	Very serious
Significant	10–49 dead and/or 50–100 severely injured	SEK 500 million–SEK 1 billion	Serious
Average	2–9 dead and/or 10–49 severely injured	SEK 100–499 million	Serious
Minor	1 dead and/or 1-9 severely injured	SEK 20–99 million	Minor
Minimal	No deaths or serious injuries, a number of minor injuries	<SEK 20 million	Minimal

Source: Adapted from MSB (2013).

Likelihood and plausibility analysis[4]

A likelihood assessment is conducted for each risk scenario in which the probability of its occurrence on an annual basis is estimated and converted into a qualitative score

ranging from very low to very high likelihood (Table 22.4). The assessment mainly concerns the primary cause of the event and the direct impacts that are described in the scenario, not knock-on or secondary effects. Each scenario is designed to be of the worst probable type, which means that, unlike worst case scenarios, they may result in significant or very significant impacts and be considered realistic on the basis of expert knowledge in the field to which the scenario pertains (DSB, 2012, p.20).

The results of the 2012 NRA considered two risk scenarios to have high likelihood: a prolonged heat wave and a school shooting. Whereas the heat wave scenario draws upon climate data, the likelihood assessment of a school shooting is based on past threats and an actual occurrence, but it also considered the available means and motivation. Such acts do not require more than minimal resources; the weapons of the type used in school shootings in other countries are relatively easy to acquire in Sweden, and offenders today can inspire and copy each other via the internet (DSB, 2012, p.25).

The risk scenarios for an extensive disruption to GNSS and disruption to the drinking water supply due to diesel in Stockholm's raw water were assessed to have very low likelihood. For both systems, several protective barriers are in place and would have to fail in order for either event to occur. The likelihood assessment for these two events resulted in a score of very low for this reason, which illustrates how the NRA methodology in Sweden incorporates vulnerability analysis also into likelihood assessment.

Table 22.4. Likelihood scales

Qualitative scale (risk matrix)	Quantitative scale for likelihood assessment		
	Lower span	Magnitude	Upper span
Very high	≥0,2 on an annualised basis (≥ once per 5 years)	1 on an annualised basis (once per year)	1 (once per year)
High	High ≥0,02 on an annualised basis (≥once in 50 years)	0,1 on an annualised basis (<once per 5 year)	<0,2 on an annualised basis (<once per 5 year)
Medium	≥0,002 on an annualised basis (≥once in 500 years)	0,0001 on an annualised basis (once in 1 000 year)	<0,02 on an annualised basis (<once in 50 year)
Low	≥0,0002 on an annualised basis (≥once in 5000 year)	0,0001 on an annualised basis (once in 1 000 year)	<0,002 on an annualised basis (<once in 500 year)
Very low	≥0	0,0001 on an annualised basis (once in 10 000 year)	<0,0002 on an annualised basis (<once in 5 000 year)

Source: Adapted from MSB (2013).

Time horizon

The NRA methodology in Sweden focuses on the conditions that society faces at the present and events that could occur during the next 5-years; this is the time horizon that is referred to in the EU-guidelines. The ambition of MSB is to expand the time horizon over

the next few years to include risk scenarios that could occur as far in the future as 20-30 years from the present.

Uncertainty

Since the events described in the risk scenarios are often such that the availability of relevant statistics and experiences is limited, the methodology describes how the assessment is conducted and what it is based on. This is expressed in an uncertainty assessment presented in Table 22.5.

Table 22.5. Uncertainty scale in the National Risk Assessment

Figure in the risk matrix	Designation, uncertainty	Explanation, justification for the assessment
●	High	There are very few statistics and little data on which to base an assessment and the margin for error is significant.
○	Medium	Some statistics and data are available. Experts consider the assessment to be the most reasonable, but there is a margin for error.
○	Low	The assessment is supported by solid experience, statistics and other data. The assessment is possibly inaccurate, but it is not likely.

Source: Adapted from MSB (2013).

Updating the National Risk Assessment

The development of the NRA process/methodology is reviewed on an on-going basis. MSB evaluates the steps in the process based on the experiences from the previous year. Risk analysis that result in high uncertainty are continuously re-evaluate; currently there are 2 risks under re-evaluation. For each new NRA-cycle MSB begins the analysis with a brief review, if circumstances have changed or if some major event occurred that could affect the risk assessment results.

Communicating the results of National Risk Assessment

Using the National Risk Assessment to raise awareness about risks

The NRA report is published on-line for anyone to read in Swedish and English. When it was first released in March 2013 the results attracted great media attention, and MSB was heavily occupied with interviews. Media interest continues to be high at the time of writing, with MSB participating in one media interview every two weeks about the results of the NRA.

Tools for interpreting risk analysis

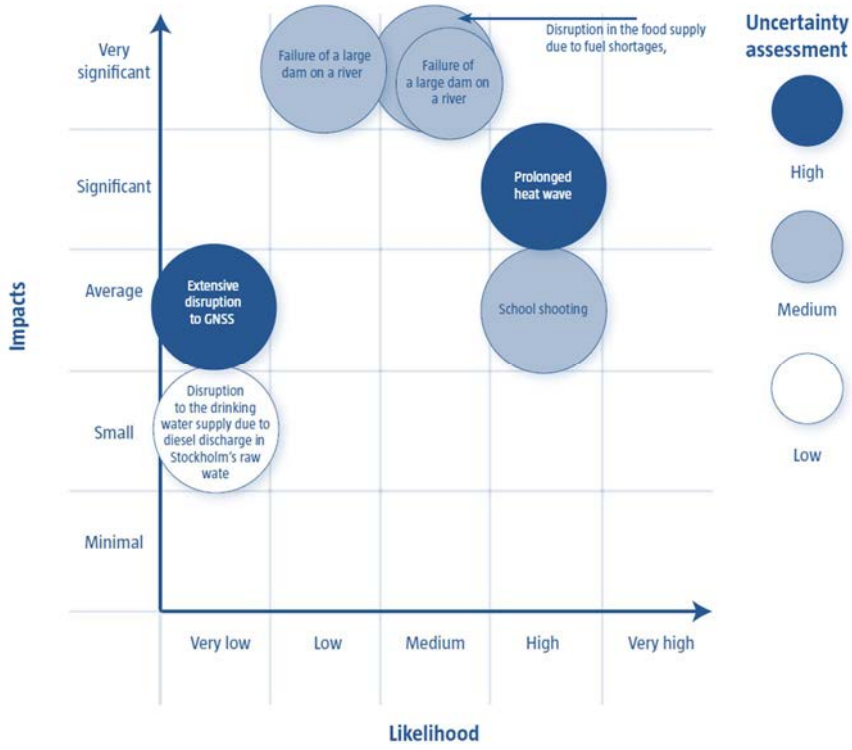
Sweden compiles the results of analysed scenarios in a risk matrix, which provides an overview of the assessments of the various events' likelihood, impact and uncertainty. The 5x5 matrix visually compares the results of the 7 risk scenarios (Figure 22.1) along 2 axes for impact and likelihood, divided into 5 columns and 5 rows. For each scenario

these two components are assigned a score from minimal to very high, and these scores determine where a risk scenario is plotted on the matrix.

The scenarios are also given a score for uncertainty, which reflects the reliability of the supporting data on which the underlying assessments are built, i.e., it is an estimate of the level of confidence in the accuracy of the likelihood and impact assessments. For each risk scenario the uncertainty has been assigned one of three levels of uncertainty, illustrated with black (high), grey (medium) and white (low).

In the risk matrix, the impact score presents the category where the most significant impacts are realised. It is sufficient for the impacts for one category (human, economic/ environmental or political/ social) to be considered very significant for the scenario's overall impacts to also be assessed as very significant. There is no ranking between the impact categories; all the categories carry equal weight.

Figure 22.1. Sweden's risk matrix[5]



Source: MSB (2013)

Main lessons learnt and policy outcomes

Lessons learnt

Sweden considers its NRA to be a work in progress. In particular the assessment does not yet fully correspond to the European Commission's guidelines. Moreover, to evaluate the risks and to propose mitigation measures, additional methods and analyses are needed. Among the revisions and improvements needed are the method for selecting events, as well as the development and analyses of scenarios. The current risk matrix needs to be refined in its scale to illustrate better the differences between the three events that were judged to pose the greatest combined risks in 2012. Sweden finds that some of

its protection values are very broad in scope and require further definition and the development of indicators to help measure the impact of a risk scenario, for example that affects democracy, rule of law and human rights and freedoms.

The National Risk Assessment 2012 identified too many serious general events to conduct thorough scenario analysis, so 15 events were merged into 7 new events, including a number of complex scenarios. One of the NRA objectives is to develop knowledge for each event through scenario analysis, and merging events is not an optimal substitute to developing and analysing scenarios for each of the events. If an event that was previously independent becomes either the cause or the effect of other events, the composite event then constitutes a limiting factor in the analysis (MSB, 2013, p.32). Among such composite events was a scenario in which a chemical spill following a ship collision results in contamination of the drinking water supply in Stockholm. Prior to analysis, this scenario was assessed to be of the type "worst probable". This was later revealed to be inaccurate given the Stockholm region's advanced water treatment technology. An analysis at the stage of scenario development may apparently be flawed and in need of revision after a more detailed analysis has been carried out (MSB, 2013, p.33). MSB recognises that to prevent similar situations in future work, it is vital to ensure that scenario drafts are reviewed by experts with the relevant expertise.

For six of the seven risk scenarios, the analysis was based largely on a workshop with experts and other key individuals. Great stock is placed upon the expertise provided at the expert workshops. The experience of conducting them has revealed lessons for the future. Each workshop requires thorough preparatory and supplementary work. A wide range of participation is key but demanding. It is crucial to involve experts and stakeholders affected by the scenarios early in the process and to keep them informed all the way to the final report. This requires a lot of planning and co-ordination work on top of the analytical tasks.

MSB cannot guarantee the participation of all relevant parties, which is why some stakeholders' views must be obtained in other ways. Variables, variable values and other assumptions behind a scenario need to be factually substantiated prior to a workshop. During the workshop, additional issues of relevance to the assessments of impacts, likelihood and uncertainty are usually identified. If these issues cannot be resolved on this occasion, they then need to be investigated further. In the scenario analyses of 2012, MSB did not have the time to further research the issues raised in the workshops to the extent desired. It is necessary to take this lesson into account when determining the number of future workshops, and to allocate more time for the supplementary research (MSB, 2013, p.33).

Benefits

The National Risk Assessment 2012 included methodologically coherent scenario analyses in which experts and stakeholders representing different sectors, levels and disciplines of the civil contingencies system were engaged. In the Swedish context, such an integrated, comprehensive approach is a novelty (MSB, 2013, p.33).

Participants found the workshops to analyse the impacts of risk scenarios to be instructive, in part because they gained insight into other emergency management stakeholders' perceptions and a deeper understanding of the complexity of crises. The NRA process creates an important arena for discussions about serious national events. The stakeholders learn more about their own roles, but more particularly about the roles

of different participants in the emergency management system. The analyses are also important to clarify mandates and to find gaps in public responsibilities and resources. Furthermore, they appreciated the coming together of agencies and professional groups at various levels and the opportunity to develop new networks. Some participants also felt that the scenario they analysed could be used as the basis for exercises within their own organisation and that the working method was an inspiration for their own risk and vulnerability analyses. Several governmental agency representatives suggested that the national risk assessment could contribute to greater consensus across subject and sector boundaries, as well as increased motivation in emergency management work and the organisations' own risk and vulnerability analyses (MSB, 2013, p.34).

MSB conducts a survey of the experience of participants in each expert workshop, and the results indicate that the experts and other civil contingencies actors greatly appreciate the process. When stakeholders apply for crisis preparedness funding from MSB they now sometimes refer to the results of the analyses conducted in the NRA workshops. MSB can also see that its scenarios are being used by stakeholders in their own work with risk and vulnerability analyses.

Limits

MSB intends to create a coherent process and uniform methodology for national risk and capability assessments. The goal is for the risk and vulnerability analyses of civil contingencies organisations to be designed so that they contribute more to risk and capability assessments at the national level, and that the national assessment, in turn, constitutes support for the risk and vulnerability analyses.

The current system needs to be revised both in terms of content and design. For example, a basic methodology is required for capability assessments, including a clearly defined concept of capability with specified empirical indicators. The national risk assessment needs to incorporate a more long-term perspective, as well as more types of complex events. It is also necessary to develop the methodology for societal cost-benefit analysis, to improve the assessment of impacts and facilitate the composition of a proposal that indicates the measures that should be taken (MSB, 2013, p.10).

Policy inputs and outcomes

An annual report on the NRA is submitted to the Cabinet through the Ministry of Defence. No policy recommendations were made in 2012. MSB is mandated to identify capability needs and to build capacities for different contingencies, and the results of the NRA will eventually feed directly into this process, however only seven scenarios have been analysed so far, which means that the risk matrix for 2012 is not yet suitable for decision-making or prioritisation. The comparative rankings between different risk scenarios do not yet provide a strong enough basis to prioritise efforts to build-up of civil contingencies capabilities or otherwise prioritise actions to mitigate significant national risks.

It is too early for policy decisions to be based on the outcomes of the NRA, or to consider that it has reduced vulnerability to major risks. The results of several years of risk and vulnerability analyses and capacity building efforts (e.g., procedures for early warning and co-ordination for a common operational understanding, coherent risk/crisis communication) have been tested in several large events. MSB finds the difference in organisational performance under duress between 2004 and 2013 to be striking.

Notes

1. For more details on the parameters of a national event and a crisis see MSB, 2013, p.16.

2. Strictly speaking this step goes well beyond "hazard identification", but for the purpose of facilitating subsequent comparison with different country chapters this section will describe the risk identification step.

3. In Sweden's NRA process an impact assessment for each scenario follows the risk identification phase. There is no separate step for vulnerability analysis- it is implicitly built-in to the impact assessment. To facilitate comparisons with different country chapters, the mechanics of the impact assessment are described here separately to maintain consistency with the other chapters of this report.

4. In Sweden's NRA process the likelihood assessment for each scenario follows the risk identification phase. To facilitate comparisons with different country chapters, the mechanics of the likelihood assessment are described here separately to maintain consistency with the other chapters of this report.

5. A note on the matrix methodology: "The likelihood assessments for each event in the matrix indicate the likelihood of an event similar to the one analysed in the risk scenario occurring in Sweden within one year. The reason given for this is that, from a national emergency preparedness perspective, it is often more relevant to assess the likelihood of a serious event occurring in the country as a whole within a given timeframe, than assessing the likelihood of a serious event occurring at a particular location in the country. The impact assessments, however, indicate the impacts of the very scenario that has been analysed." Taken from National Risk Assessment 2012, p.22.

References

The Swedish Civil Contingencies Agency (MSB) (2016), "A summary of risk areas and scenario analyses 2012–2015", https://www.msb.se/en/Products/Publications/Publications-from-the-MSB/A-summary-of-risk-areas-and-scenario-analyses-20122015/.

The Swedish Civil Contingencies Agency (MSB) (2013), Swedish National Risk Assessment 2012, https://www.msb.se/en/Products/Publications/Publications-from-the-MSB/Swedish-national-risk-assessment-2012/

Further reading

European Commission (2010), Commission Staff working paper, "Risk Assessment and Mapping Guidelines for Disaster Management. Available at: https://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf

Chapter 23. SWITZERLAND

The national risk Assessment process in Switzerland is used to prioritise the treatment of hazards, to help prepare emergency plans and capabilities and for training purposes. The requirement to develop a comprehensive approach to disaster risk management came from senior government level where the responsibility for its development was mandated to the Federal Office for Civil Protection (FOCP). There is significant transparency and accountability in the process with arrangement to consult all stakeholders and the publication of the process. There has also been an additional independent review and reporting mechanism put in place by the FOCP and this report has been sent to government. This chapter discusses the methodology for hazard identification/analysis and vulnerability and impact analysis in some detail. There is widespread acceptance and buy in to the NRA process in Switzerland and this is largely due to the widespread consultation with all stakeholders, public private sectors and the public.

Key Words: Bottom up/top down approach; Detailed methodology; Independent review; Integrated and co-ordinated action; Multi sectoral participation; Scenario Analysis; Stakeholder involvement; Widespread consultation.

Introduction

Switzerland produced its first national disaster Risk Report in 2012 (FOCP, 2013), encompassing analysis carried out during 2011 and 2012 of 12 key risks. A second was published in July 2015, based on assessments of these and a further 21 hazards carried out in 2013 and 2014. The context for this was a perceived need for information and evidence on which to prioritise hazards for treatment, to prepare emergency plans and capabilities, and to educate, train and exercise all kinds of responders. The Swiss constitution requires that the responsibilities for disaster risk management are widely distributed among the Cantons, and Federal agencies. The publication of the Risk Reports marks a significant development in the promotion of a culture of collaborative risk management using increasingly consistent methods at all levels.

Governance framework

The system for analysing hazards and risks in Switzerland combines top-down and bottom-up approaches reflecting the responsibilities of the federal authorities and the Cantons for disaster risk assessment and management:

- The Cantons are responsible for conducting risk assessments and drafting preparedness plans in their geographical area of responsibility. These responsibilities extend to establishing mutual aid arrangements with neighbouring Cantons.
- Based on the federal legislation, excluding armed conflict, five hazards are automatically the responsibility of the federal administration to manage: increased radioactivity, satellite re-entry, barrage incidents, pandemic and animal disease. In considering of what other kinds of risk should be in the national-level risk assessment, the main considerations is whether there is a need for co-ordination between different agencies, beyond the level of cooperation expected between neighbouring Cantons; whether there are links with other kinds of risk (i.e., whether these are cascading multi-risks), and whether there is a need for co-ordination arrangements to be implemented speedily.

In 2008, the Federal Council of Switzerland (i.e., the cabinet of the seven federal departments) gave a mandate to the FOCP to promote a co-ordinated and consistent approach to disaster risk management at all levels. The basis for this was Article 8 (on research and development) of the Federal Law on Protection of the Population and Civil Protection, and the quadrennial mandates for 2008-2011 and 2012-2015. The governance structure for this originally included a working group on the federal level, a risk forum with cantonal representatives and area specialists from the academia and the economy; and a steering committee with one representative from each federal department. But further discussions resulted in a more flexible structure, creating collaborative working groups for the specific hazards analysed with changing representation from the FOCP itself, the responsible federal agencies, the Cantons, first-responders and others including representatives from the business sector, owners/operators of critical infrastructure, and the academic community.

Aims and Objectives

- The national hazard and risk analysis system has the following aims (FOCP, 2013): to develop a method to analysing the risk of disaster and emergency scenarios that all responsible authorities can use,
- to elaborate standardised scenarios and other uniformly structured foundations for disaster management,
- to establish efficient and continuous analytical processes for disasters and emergencies.

This means that the Swiss hazard and risk analysis process has ambitions to fulfil most of the objectives of NRA processes set out in the OECD framework and principles for the governance of critical risks including as a tool to aid capability analysis and planning at Cantonal (i.e., sub-state) level and even at the community level; to monitor risks, at all levels; to communicate risks to stakeholders both in the public and the private sector, NGO (community and voluntary sectors) and the public at large; to gain consensus, to the extent possible and necessary, among these stakeholders, and so to create a risk management culture.

There are ambitions to expand the use of risk assessment, to provide a more systematic approach to planning, both of generic capabilities and for some specific contingencies. Challenges to these ambitions have been identified and are being systematically addressed in the section "Main Lessons Learnt and Policy Outcomes".

Definition of key terms

The FOCP provides a glossary of terms both for the national level and as part of the voluntary guidance for Cantonal risk assessment. The National Disaster Risk Assessment (NDRA) process was officially launched by a mandate of the Federal Council (i.e., the Swiss federal cabinet) in December 2008. ISO 31000 is used to describe terms and processes. A distinction is drawn between disasters (or Katastrophen) and emergencies, the first being defined as a major incident that exceed regional capacities (e.g., major earthquake) and the latter a major development that exceed regional capacities (e.g., pandemic flu).

Transparency and accountability

The Swiss disaster risk analysis process incorporates significant transparency and accountability measures, through a process that is highly participatory, and through the publication of the assessment, of the detailed methodology, and of the names of the organisations of those involved in the process.

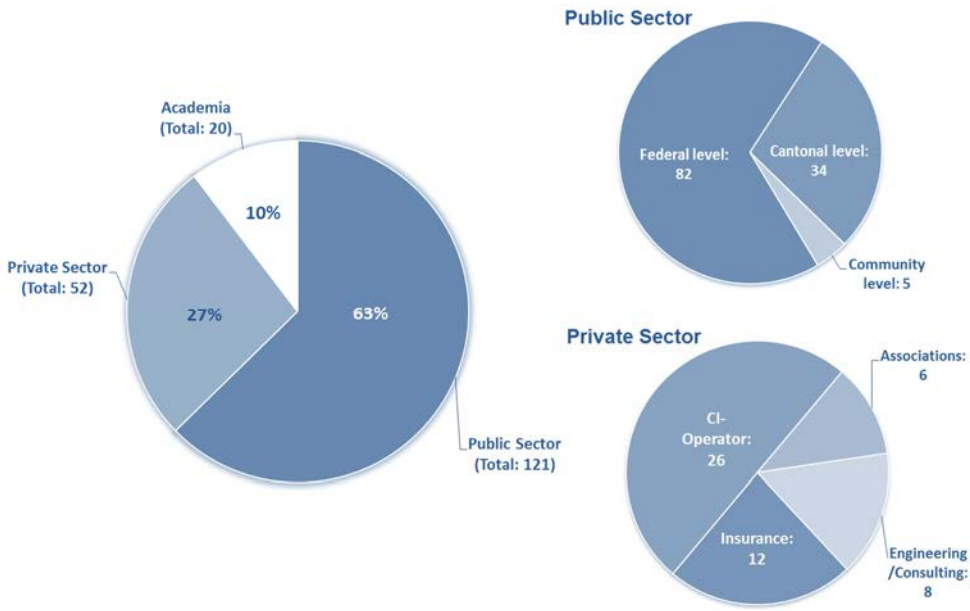
The lead organisation for national risk assessment in Switzerland is the FOCP, whose role is to collate information on the hazards, develop hazard scenarios, to develop guidelines on the methodology) and to moderate the process of the actual analysis. The methodology was validated in the Forum (later the Working Group) set up under the original governance arrangements, following a series of two-day workshops to test-run the methodology.

On the cantonal level, KATAPLAN[1] is applied on a voluntary basis. Even though the Cantons have no legal obligation to use the guideline, they have done so in increasing numbers since its promulgation.

Arrangements ensure the involvement of all relevant organisations with responsibilities for disaster management, and participation by interested parties and

experts from the public, private and academic sectors. Overall, these arrangements brought together over 190 participants in the national disaster risk assessment process, of whom nearly two-thirds were public sector (in proportions roughly 2:1 Federal: Cantonal), one quarter private sector, and 10% academic sector.

Figure 23.1. Stakeholders with responsibilities for disaster risk management



Source: Presentation on "Update on National Disaster Risk Assessment (NDRA) in Switzerland: at the OECD High Level Risk Forum, Paris, December 10, 2014, slide 9.

The form of collaboration which took place was the creation (under the Working Group) of workshops with attendance determined according to subject matter so that, for example, the workshop on the risk of animal disease outbreaks (a subject where the main competences are on the federal level) had representation from: the FOCP, Federal Office for Food Safety and Veterinary, a Cantonal Veterinary Service; Associations including the Swiss Meat Association and Swiss Farmers Union; private sector representation from the country's largest dairy and cheese producer and a major food retailer; and academic representation from the University of Zurich. Participants in the workshops of 2011 and 2012 were named in the Risk Report 2012 together with the organisations which they represented, so increasing transparency of the process.

This widespread participation in itself promotes a lack of bias in the assessment; but the FOCP has introduced additional controls by referring the risk analysis for a second and independent opinion to the Paul Scherrer Institute. The resulting Risk Report 2015 has been sent to the Government with a note of information. However, no formal agreement was sought to keep the analysis as independent as possible (no consultation process with the federal and cantonal agencies).

Multi-level governance and multi-actor participation

The above-described broad arrangements for participation ensure that the NDRA process is able to inform local/Cantonal disaster risk assessment.

Risk analysis

The Risk Report 2012 presented 12 types of hazards. The 2015 Report, published in July 2015, includes a total of 33 hazards, reflecting work on a further 21 hazard types carried out during 2013 and 2014. Subsequent Reports may show additional hazards, but the FOCP does not expect the addition of an equally high number as in the last two years.

Scope

The NDRA covers all kinds of hazards including natural hazards, technical failures, and man-made incidents, including malicious/intentional actions such as terrorism. The scope of the risks is outlined in Table 23.1.

Table 23.1. Hazards selected for the national risk assessment in 2011-2014

Natural hazards	Technical hazards	Societal hazards
Earthquake*	Power outage*	Attack with dirty bomb*
Inland flooding*	Road accident with dangerous goods*	Attack with Sarin*
Windstorm*	Accident in a chemical plant*	Pandemic*
Drought*	Rail accident with dangerous goods	Animal disease*
Severe weather	Airplane crash	Mass influx of refugees*
Forest fire	Biological plant accident	Biological attack
Meteor strike	Barrage incident	Cyber attack
Cold wave	Nuclear power plant incident	Conventional attack
Heavy snowfall	Information and communication technology outage	Violent disturbances
Heat wave	Gas distribution failure	Power supply shortage
Solar storm	Waterway incident	Oil supply shortage
Spread of invasive species		

Source: FOCP (2013) Note: *Indicates the 12 risks assessed in Risk Report 2012.

Hazard Identification

The FOCP is responsible for the initial identification of hazards that may possibly qualify for inclusion in the NDRA process. For this purpose, the FOCP has developed a hazard catalogue containing some 120 possible hazards. Down-selection to the short list of (currently) 33 hazards for detailed analysis in the risk analysis process was carried out in the Working Group. Hazards on the short list were those that require a significant level of co-ordination between different responders or agencies, beyond the level of cooperation expected between neighbouring Cantons; where there are links with other kinds of hazards (i.e., whether these are cascading multi-hazards), and in particular where there is a need for co-ordination arrangements to be implemented speedily.

Analysis of the short-listed hazards is based on a comparison of scenarios. These scenarios illustrate three levels of impact of the hazard (significant; major; extreme) of which the middle level (major) is used for the basis of comparing the risks in terms of likelihood and damage. The other two levels are elaborated as vignettes, which illustrate

the range of impacts that each hazard may cause and associated likelihood. Although the FOCP stress that all scenarios are plausible, the three levels may be seen as corresponding to the "expected case", "reasonable worst case", and "worst case". This approach demonstrates to planners the potential variability of outcomes of these risks, which may provide useful data for calculating risk tolerance.

Impact Analysis

Switzerland's risk analysis process defines risk as a product of damage caused and the associated likelihood of harm arising from an event. Analysis of impact (and likelihood) was carried out by workshops with multi-disciplinary and multi-sector participation (as outlined above). There are twelve criteria for judging impact (or damage), reflecting objects of value to Switzerland in four main areas according to the Swiss federal constitution (Table 23.2).

Table 23.2. Criteria for judging impact

Area of damage	Sub-category of damage	Indicator
Population	Life and health	B1 – casualty (ie numbers of dead)
		B2 – numbers of people injured or sick
	Help in emergency	B3 – numbers of people in need of support
Environment	Ecosystem	U1 – damaged area
Economy	Wealth	W1 – damage to property and assets
	Economic productivity	W2 – reduction of economic productivity
Society	Provision of vital goods and services	G1 – disruption of provision
	Law and order	G2 – limitations of law and order
	Image of and trust in institutions	G3 – reduction of good image (abroad)
		G4 - reduction of trust (domestic)
	Territorial integrity	G5 – loss of territorial control
	Cultural goods	G6 – damage or loss of cultural goods

Source: FOCP (2013)

Scales for each of these impact criteria are stepped i.e., logarithmic, each of 8 points on the scale representing a three-fold increase on the previous point. In the hazard files which are compiled for each hazard to inform disaster risk management planning, no weighting is given to the main impact criteria or, within the main four areas, to the sub-categories of damage. But, for the purposes of the overall presentation and comparison of risks in the Risk Report, impacts are translated into monetary terms, on a logarithmic five-point scale in which the entry level is 0.1 Billion Swiss Francs and the scale increases by a factor of ten at each point up to a maximum of 1,000 Billion Swiss Francs.

Likelihood and Plausibility Analysis

Estimation of the likelihood of hazards is on the eight-point scale shown in table 23.3.

Table 23.3. Likelihood estimation of hazards

Class	Description in words	Per 10 years	Once in x years	Frequency (1/year)
L-8	Happens on average a few times in a lifetime, in Switzerland	>30%	<30	>3x10-2
L-7	Happens on average once in a lifetime, in Switzerland	10-30%	30-100	3x10-2 – 10-2
L-6	Has already happened in Switzerland, possibly several generations ago	3-10%	100-300	10-2 – 3x10-3
L-5	Has not happened so far in Switzerland, but is known from other comparable countries	1-3%	300-1000	3x10-3 – 10-3
L-4	Has not happened so far in Switzerland, but there are several known cases worldwide	0.3 – 1%	1000 – 3000	10-3 – 3x10-4
L-3	Has not happened so far in Switzerland, and there are few known cases worldwide	0.1 – 0.3%	3000 – 10,000	3x10-4 – 10-4
L-2	Only single case are known worldwide but they are also conceivable in Switzerland	0.03 – 0.1%	10,000 – 30,000	10-4 – 3x10-5
L-1	Very unlikely anywhere in the world; even more so in Switzerland but not completely inconceivable	<0.03%	> 30,000	< 3x10-5

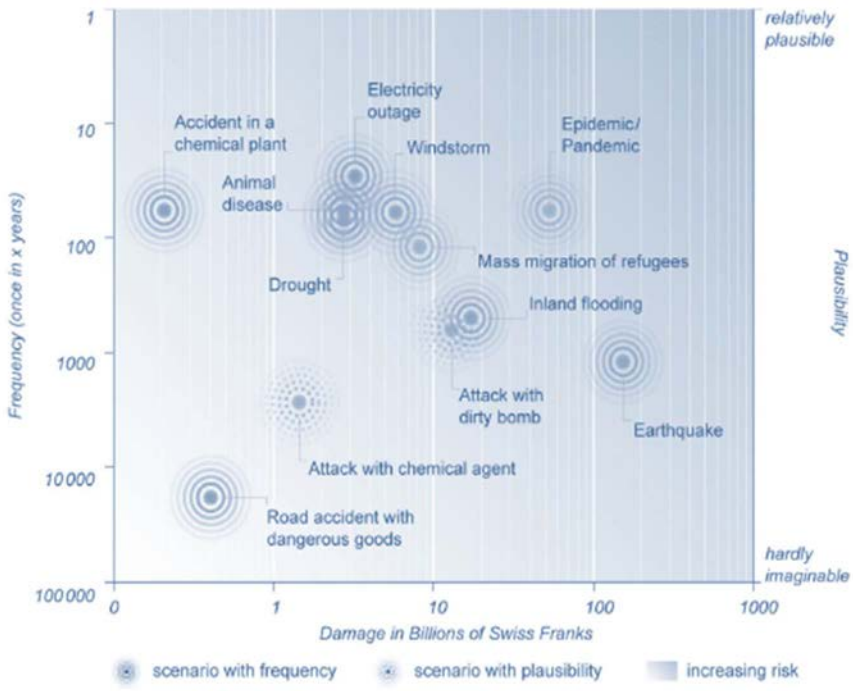
Source: FOCP (2013).

The method of estimating the plausibility of threats is more qualitative, reflecting judgements of whether the threat is "relatively plausible" (the highest mark P - 8 of 8) or "hardly imaginable" (point P-1 of 8).

Risk evaluation, monitoring and re-evaluation

For each hazard investigated, a hazard file is compiled. This defines and gives historic examples of the hazard, lists factors that influence the likelihood and impact of the hazard, outlines scenarios (at three levels: significant; major; extreme), identifies dependencies, and references in legislation or scientific literature. These hazard files are intended in these ways to provide the groundwork for planning emergency preparedness measures including emergency plans and operational concepts, resource planning, training and exercises.

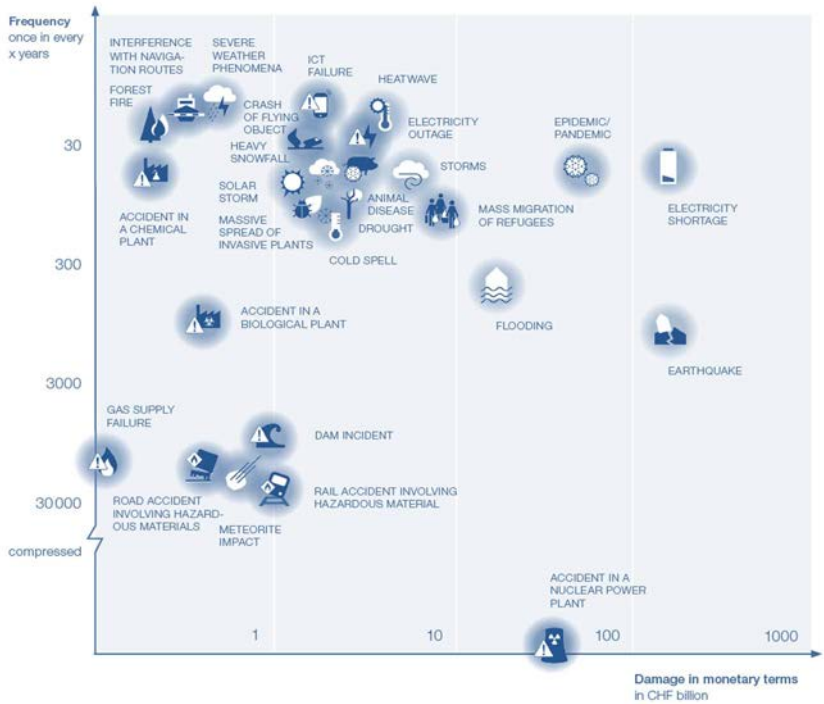
Figure 23.2. Risk matrix of Switzerland (2012)



Source: FOCP (2013).

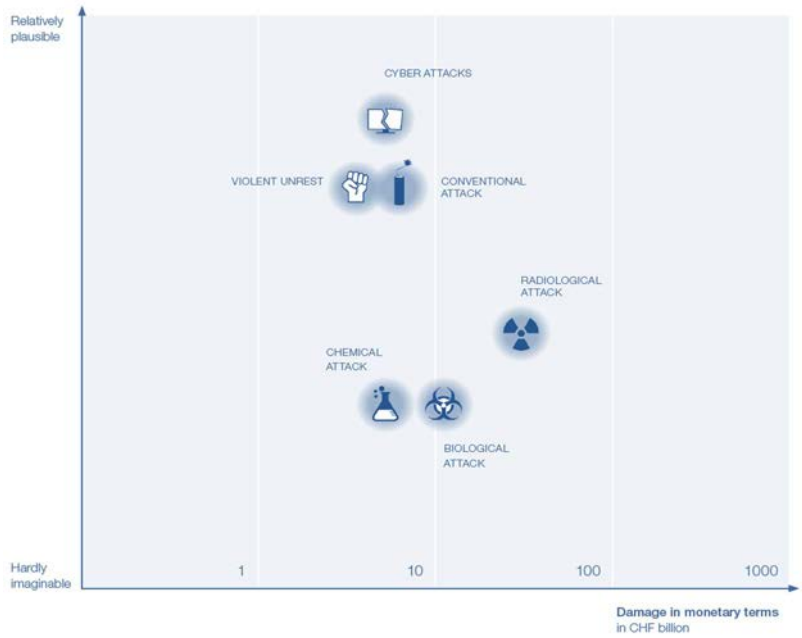
For the Risk Report itself, hazards are plotted on a matrix showing, on the horizontal axis, aggregated damage under the four headings expressed in Billions of Swiss Francs and, on the vertical axis, likelihood or plausibility scores according to the eight-point scale shown above (Figure 23.2). The 2012 Report included all 12 risks on one such diagram. The Risk Report 2015 shows malicious/intentional actions (using a plausibility instead of frequency scale separately from unintentional hazards (mostly natural and technical/accidental) (Figure 23.3 and 23.4). The Swiss Risk Report does not include separate presentation of risks by types of impact, but the data collected would allow them to do so.

Figure 23.3. Risks matrix of Switzerland : frequency and damages



Source: FOCP (2015).

Figure 23.4. Risk matrix of Switzerland : malicious/intentional actions



Source: FOCP (2015).

As regards re-evaluation, the intention of the FOCP is to continue to analyse hazards at the national level including one or two hazards (e.g., hailstorm) not yet included in the

short-list for promulgation in 2015.The intention here is to integrate methodological improvements in the risk analysis process including for example the more sophisticated assessment of cascading effects, and to conduct further research into risks that are less well understood, for example the impact of solar storms on satellite and other communication operations.

Communicating the results of National Risk Assessment

Using the National Risk Profile to raise awareness about risks

The Swiss Government publishes the Risk Report, (including the identities of the main contributors and the organisations to which they belong), hazard files and hazard catalogues on its web-site[2]. The Report makes clear that its main audiences are organisations tasked with disaster and emergency management, that are cantonal command staffs and the Federal NBCN Crisis Management Board (an interdepartmental board of directors responsible for nuclear, biological and chemical incidents as well as natural hazards), as well as the critical infrastructure programme (CIP) and the Security Network Switzerland (Sicherheitsverbund Schweiz, SVS). But the level of detail published, which matches or exceeds that provides in the risk registers of most other countries, enables organisations and communities throughout the country to view for themselves in outline the risk analysis on which the public sector's emergency planning is based.

Tools for interpreting risk analysis

The risk matrices show the relative likelihood and impact of the risks.

Main lessons learnt and policy outcomes

Lessons learnt process

In its conclusions, the 2015 Risk Report analysed the lessons learnt from this assessment process to create a systematic and standardised nationwide risk analysis in civil protection; to include the result in the national disaster and crisis management as well as in the preparedness and capability planning; and the fostering a risk dialogue.

Benefits

The main benefits so far of the Swiss approach have been that:

- The adoption (and road-testing) of an agreed methodology for assessing likelihood/plausibility and impact have made dialogue on the risks between experts from the different sectors much easier, and have facilitated the formulation of a minimum consensus on the risks.
- The approach of engaging with all sectors (public, private, academic, community) has improved stakeholder engagement and acceptance.
- Consensus on the methodology to be employed has also facilitated the task of selecting additional hazards from the catalogue, without overpopulating the Risk Report.
- There has been real results in terms of operationalising the risk analysis at Cantonal level, with two thirds of Cantons having both completed their analysis

using the KATAPLAN method and implemented changes to their emergency and disaster management planning.

Limitations

The 2012 Risk Report set out some relatively minor limitations, most of which have been overcome with the passage of time:

- the difficulty of measuring and therefore taking into account in the assessment some non-material impact criteria (in particular, the curtailment of basic rights – an impact deriving from the Swiss Federal Constitution)
- the need for minor clarifications in other damage indicators (e.g., damage to ecosystems) to provide for a more precise and improved method of assessing these impacts
- the need for the expert risk analysts to be engaged at an earlier stage in the development of risk scenarios.

Policy Outcomes

The main issues requiring further policy work are:

- the need for more systematic exploitation of the risk analysis to inform capability and capacity planning, both for generic capabilities (i.e., capabilities not linked to specific hazards but to mitigating common kinds of impact) and for some capabilities linked to some specific hazards; the intention in the Risk Report, to develop planning assumptions to this end is still being discussed.
- the integration of the risk assessment process and results into the national security policy covering approaches to the protection of the civil population.

Notes

1. A guideline on methodology and analytical tools for risk assessment. For more information refer to: FOCP (2008) Leitfaden KATAPLAN – Kantonale Gefährdungsanalyse und Notfallvorsorge, Federal Office for Civil Protection (FOCP), Berne.

2. Available at: www.risk-ch.ch.

References

Federal Office for Civil Protection (FOCP) (2013), Disasters and Emergencies Switzerland Risk Report 2012, Berne.

Federal Office for Civil Protection (FOCP) (2015), Disasters and Emergencies Switzerland Risk Report 2015, Berne.

Further readings

ISO 31000:2009, Risk management – Principles and guidelines

ISO Guide 73:2009, Risk management – Vocabulary.

Chapter 24. UNITED KINGDOM

The United Kingdom National Risk Assessment has been in place (in its present form) since 2005 and has been guided by legislation, the Civil Contingencies Act of 2004. The process is co-ordinated by the UK Cabinet Office and looks forward in a time scale of (a 5 year period) drawing of expertise from a wide range of departments, agencies, academia and external experts. It has an all of government approach using evidence to determine the range of risk that the UK should be prepared for. The NRA is designed to function as a top down process and guides the identification of risk for the whole of the UK, guiding regional entities in the identification of their own risks as mandated by the Civil Contingencies Act 2004. In respect to transparency and accountability, the NRA is published in an abridged form but there is widespread consultation and input internally within government circles and subject matter experts.

Key Words: All of government approach; Evidence based; Reasonable worst case scenario; Subject matter experts; Wide-spread consultation.

Introduction

The National Risk Assessment (NRA) and National Resilience Planning Assumptions (NRPAs) have underpinned emergency response planning for terrorist and other civil emergencies in the United Kingdom since 2005, after emergency planning legislation (the Civil Contingencies Act 2004) was passed requiring identified local Emergency Responders to assess the risks of emergency arising in their area of responsibility and plan accordingly. A National Risk Assessment has been conducted every year since then.

The Cabinet Office Civil Contingencies Secretariat (CCS) co-ordinates the annual National Risk Assessment (NRA) to monitor the most significant risks of emergencies that could arise including natural events, major accidents and malicious attacks. The National Risk Assessment considers risks that may impact the United Kingdom over the next five years. It is a confidential assessment, drawing on expertise from a wide range of departments and agencies of government and external experts. The NRA is a cross-government assessment that provides an evidence base for determining those risks that require specific planning and it is a source of data on the scale of consequences of emergencies for which the country should prepare, which are further analysed in the National Resilience Planning Assumptions (NRPA).

In 2011, the very high priority risks in the NRA were: pandemic influenza; catastrophic terrorist attacks; coastal flooding; and a severe volcanic activity abroad emitting mainly sulphur dioxide, which would have significant impacts for aviation, public health and the environment. New risks are added as they are identified including, in 2011, the risk of severe space weather, which could have impacts on power distribution, satellites and telecommunications. CCS is aware of international differences in opinion on the severity of the consequences of such an event, which are not fully understood, but believed to stem from differential vulnerabilities; the risk was included in the NRA initially on a precautionary basis pending expert scientific advice on the reasonable worst case scenario and the full range of potential impacts on, primarily, business continuity.

The NRA assesses and prioritises risks to allow a proportionate allocation of resources by assessing their relative likelihood/plausibility and impact. To ensure risks are compared on a consistent basis and the NRA presents a proportionate yet robust perspective of civil emergency risks, a reasonable worst case scenario is identified for each generic risk. This scenario is selected by subject-matter experts to represent a challenging yet plausible manifestation of the wider group of risks it represents.

For non-malicious hazards (i.e., natural hazards and accidents) the likelihood is assessed using a combination of the best available data (e.g., analysis of trends) and expert judgements. For malicious threats (e.g., terrorism) the Joint Terrorism Assessment Centre (JTAC) and the Government's Centre for the Protection of National Infrastructure make a qualitative assessment of plausibility based on judgements on intent, capability and vulnerability. The impact for both threats and hazards is assessed against a number of dimensions, using pre-defined criteria. For both likelihood/plausibility and impact each risk is scored on a scale of 1-5, and these scores are used to plot risks on a two axis matrix. The positioning of risks on this matrix is used to categorize priority given to planning for each risk.

Governance framework

The Cabinet Office Civil Contingencies Secretariat (CCS) leads the co-ordination of the National Risk Assessment, in accordance with the CCS's strategic role in co-ordinating emergency preparedness at a Government level.

The UK Government attempts for each known risk to designate a risk owner – a government department or agency which is responsible for co-ordinating relevant evidence to inform the assessment of these risks. Decisions on which department or agency owns the risks were initially taken on the basis of the allocation of lead government department responsibilities as part of the published central government arrangements for responding for an emergency. Where the lead government department is not clear – as is the case for the many truly cross-cutting risks - it is the responsibility of the Cabinet Office (CCS) to make recommendations. The Civil Contingencies Secretariat has also shown capacity to ensure an integrated approach to cross-cutting risks and help to identify risks that may not fit the remit of one specific department and therefore go undetected and unassessed.

Aims and objectives

The United Kingdom's National Risk Assessment (NRA) was initially devised to support the implementation of the Civil Contingencies Act, as a tool to improve national resilience to the risks of emergencies; as such it had four main objectives:

- to develop a common understanding of the risks of emergency among those responsible for managing them
- to enable civil emergency contingency planning for the highest risks
- to enable wider resilience planning
- to provide the basis of guidance to local emergency planning, to assist them in their duties under the Act.

These objectives primarily focussed on preparation for the consequences (e.g., mass fatalities, casualties, disruption to transport) of the risks in the NRA. CCS sets benchmarks of capability required to ensure that the United Kingdom is prepared to respond to the majority of the risks it faces. Generic planning for the common consequences of risks helps ensure a degree of insurance for unanticipated events and that a proportionate approach is taken.

Since 2008, when the UK published its first National Security Strategy, the NRA has increasingly been used as a reference work for wider security planning, to inform priorities for prevention, and protective security. In 2010, the NRA formed a basis for the first UK National Security Risk Assessment which aimed for the first time to analyse the broader, global, risks to national security in a timeframe that looked forward twenty years; and provided an evidence base for the identification of national resilience as a primary aim of national security.

Definitions of key terms

The only clearly defined term from the available documentation is Civil emergency, which is defined in the 2004 Act as (a) an event or situation which threatens serious damage to human welfare in a place in the United Kingdom, or (b) an event or situation which threatens serious damage to the environment of a place in the United Kingdom, or

(c) war, or terrorism, which threatens serious damage to the security of the United Kingdom.[6] Serious damage to human welfare is defined as "loss of human life, human illness or injury; homelessness; damage to property; disruption of a supply of money, food, water, energy or fuel; disruption of a system of communication; disruption of facilities for transport; or disruption of services relating to health"; and this definition helps to define the impact criteria for the NRA.

Transparency and accountability

Initially, the National Risk Assessment was a confidential assessment conducted within government and subject to approval by the National Security Council and its predecessors. In order to incorporate transparency and accountability into the NRA process, all central government departments participate in a cross-government group chaired by the Civil Contingencies Secretariat (CCS) when proposing new risks or changes to previously assessed risks. This allows for open discussion in a cross-government forum, and for challenges to be made either at official or senior Government levels. The Government Office of Science participates in this group and acts as independent arbiter in assessing whether scientific and technical evidence has been given due consideration in the assessment both of likelihood and impact. The NRA itself sets out the process in which the evidence base was collected for both likelihood and impact and provides to that extent an audit trail.

The National risk assessment informs priority decisions and therefore some departments may have the tendency to exaggerate or underplay risks for reasons of policy preference. Although it is difficult to ensure no bias enters the process, the role of the Government Office of Sciences as an independent arbiter helps since it does not fund planning nor take an active role in the analysis and its independent in the process is quite strong. CCS also owns very few of the risks and can play a moderating role.

In 2008, the UK Government disclosed the existence of the NRA and published a National Risk Register which set out in unclassified and summary form the results of the National Risk Assessment for that year. This was designed to explain the basis of the assessment and the Government's judgement of the most likely and most serious types of emergency, to promote business continuity planning and community resilience measures, and to draw attention to the existence of Community Risk Registers. Parliamentarians have twice held hearings on the conduct of the NRA: once by the House of Commons Science and Technology Committee, on the use that the Government makes of scientific expertise in planning for and managing emergencies; the second in 2014 by the House of Lords Science and Technology Committee.

Multi-level governance and multi-actor participation

Due to the UK's administrative structure and particular regional considerations, the NRA is designed to describe the risks to the UK as a whole. To this end, the risk scenarios are intended to apply to the entirety of the UK and inform contingency planning within central government, meaning at the national level of planning. However, the NRA also

6. As defined by the Civil Contingencies Act 2004.

acts as guidance for local level emergency responders who are required to assess and plan for the risks of emergencies in their areas of responsibility. The governments of Scotland, Wales and Northern Ireland may also take the NRA into account in conducting their own assessment of risks in their areas of responsibility. In effect, the NRA highlights the process and risks the national government takes into account and helps local and regional governments understand which issues and risks they should consider. Alongside the NRA, the CCS produces guidance for the local level (and the devolved administrations) around how they can interpret the NRA at their level, taking into account both the risks spanning the entirety of the UK and particular risks to certain areas, as well how the evidence on the hazards threats map out across the country. The CCS thus provides assistance in the regional or local risk assessments; it does not actually carry out those assessments as such.

Local emergency response planners are required to produce a specific risk assessment that reflects the unique characteristics of its territorial area. HM government provides guidance to emergency responders through their Local Resilience Forums (LRFs) on the likelihood and expected consequences of emergencies based on national assessments, along with guidance on how to interpret these locally. Emergency responders also have a responsibility to maintain public Community Risk Registers, which are approved and published by Local Resilience Forums.

The CCS consults regularly with the academic sector and has drawn on outside expertise for analysis of some risk scenarios, including from private sector companies. It also uses select private sector representatives for some particular risks and more recently has drawn on scientific data for risk assessment from the natural hazards partnership, which is a number of government agencies led by the Government's Office of Science. The CCS also receives disagreements from stakeholders as an accepted part of the process. For example, the work carried out on volcanic eruptions received some stakeholder disagreement on the probability of the scenario and the impact.

In its work to improve the resilience of national infrastructure, the CCS has engaged increasingly with private sector owners and operators and, in some cases, with sector regulators. The need to build a strong relationship with private sector stakeholders before beginning to identify risks and gain information on key vulnerabilities has been a learning process and there has been slow improvement over time.

Risk analysis

Scope

The National Risk Assessment is intended to capture the range of emergencies that would be of national concern and hold potential to overwhelm local resources. That is, the NRA is intended to capture the range of emergencies that might have a major impact on all, or significant parts of, the national territory. The risks cover 3 broad categories: natural events, major accidents and malicious attacks.

The NRA identifies generic risks rather than every combination of events. Risk descriptions have to strike a balance between being sufficiently generic to enable adequate coverage of a range of possibilities but specific enough to be meaningful for planning purposes. For instance, the category terrorism is too broad for an assessment of threat, vulnerability and impact to be useful for planning. Equally a terrorist act involving a particular type of explosive at a particular site is so specific that an

assessment at this level of detail would not be useful. The scope of the assessment is intended to focus on risks that subject-matter experts collectively consider to be:

- emergencies within the meaning of the Civil Contingencies
- that are relatively likely to occur in the next 5 years
- and would present a challenge to Government during response and recovery - this could be because it would overwhelm resources and/or because it would require cross-government co-ordination).

The NRA is designed also to identify and assess risks that have unique or uniquely damaging consequences, which would require extraordinary measures of preparedness to be considered over and above the range of generic capabilities for the more common types of emergency or impact. Examples of unique risks include those of extreme space weather, and of uniquely damaging risks include the potential impacts of a volcanic effusion that is rich in sulphur dioxide.

Hazard identification and analysis

To begin the process of developing an NRA, lead government departments and agencies are called upon to identify risks within their area of responsibility. They are invited to illustrate the risk by means of a "reasonable worst case scenario", defined as challenging yet plausible manifestation of the risk which represents one scenario of many for that risk. A reasonable worst case scenario describes not necessarily the worst possible nor the most optimistic scenario within the bounds of the plausibility threshold (the NRA only considers risks of events that have at least a 1 in 20 000 chance of occurring in the next 5 years). In terms of detail, the CCS encourages government departments to draft their reasonable worst case scenario at the level of detail that inform central government contingency planning in terms of response and recovery in a civil emergency.

The reasonable worst case scenarios are reviewed by cross-government groups as a quality assurance measure. If they are accepted, the CCS-led Risk Assessment Group encourages government departments to do a more detailed risk assessment which serves as an evidence base for the national risk assessment, including a probabilistic analysis of the full range of risk scenarios they are assessing. Where data and evidence are not immediately available to enable the scenario to be described in a way that facilitates assessment, the Group may refer the risk to external experts for advice on developing a deterministic scenario.

Vulnerability and impact analysis

Once there is a provisional list of reasonable worst case scenarios, an assessment of the impact of these risks is carried out via cross-government workshops, including pre-defined scoring scales setting out how to score the impacts. The impact criteria are based primarily on the definition of emergency in UK legislation, but include additionally: impact criteria relating to the expected impact on the UK economy, measured in terms of the effects on GDP; and criteria relating to the broader psychological impacts on the population (i.e., beyond those expected to be felt directly by the victims of an emergency) (Table 24.1). The latter criteria were added following the 2005 London bombings, reflecting a need to encompass such impacts in the assessment.

Table 24.1. Assessment of the impacts

Main Criteria	Sub-criteria	Weighting
Human Impact	Deaths Illness/injury including psychological injury	20% 20%
Economic Impact	Net annualised economic cost • Demand-side consequences • Supply-side consequences	20%
Disruption of: Essential services Social services Environment	Transport Food/Water Fuel Gas Electricity Cash/finance Communications Education Health Evacuation Shelter Environment	20%
Psychological	Anxiety Outrage	20%

Source: United Kingdom Civil Contingencies Secretariat

Many of these impacts have owners in much the same way as do the risks themselves – for example, the health impacts are owned for the purposes of the assessment by the Health Department. For some, the expertise lies within the lead government department for the risk – for example, most UK Government Department will have an economic adviser who can be consulted on the economic impact assessment. At this point of the assessment leads are not asked to provide a precise cost estimate, but to give a rough order of magnitude according to a logarithmic scale agreed by the Risk Group at the outset. In some cases, greater precision may be required when proceeding to the contingency planning or investment appraisal stage and the need for this may be identified during the risk assessment stage.

Likelihood and plausibility analysis

To determine the likelihood of a risk scenario there are two slightly different approaches. In the case of a naturally occurring event (a hazard) or an accident, the risk owners draw on historical evidence, available forecasts of predictable events, and expert advice to provide an opinion about its likelihood along an order of magnitude. Factors assessed include the inherent potential of the hazard, the exposure of key assets (population, infrastructure etc.) and the vulnerability of the same.

In the case of a threat, the CCS works with government subject matter experts, and asks them to provide an assessment on the intent and capability of the range of threat actors for a particular risk scenario, as well as the vulnerability of the targets (population, infrastructure etc.) to the risk. These judgements are combined to provide the equivalent

of the hazard plus exposure plus vulnerability judgements to provide an estimate of the relative likelihood of a successful attack. These plausibility scores are reviewed every year and are done in relative terms, which means the result is not an absolute number or probability, but a ranking of the risks relative to one another in terms of being more or less likely.

Uncertainties

In all risks there is always a range of uncertainty as well as a range of opinions on what a realistic risk scenario should look like. In part, the variety of opinion in the scenario development phase is a benefit of collective discussions in the risk assessment group, which facilitates debate about what the reasonable worst case scenario is. This is why the national risk assessment considers the risk scenarios to represent orders of magnitude rather than precise measures. The CCS does not expect eventual events to reflect the scenarios with precision, but rather that its impacts fall within an order of magnitude. This approach effectively implies that CCS accepts a margin of uncertainty in the development of the estimates.

Time horizon

The choice of a 5 year time horizon was based on two aspects. First, the risk assessment should be forward looking, not backward looking. Otherwise, there is a risk in some cases of simply looking back at what happened in the past and calculating probability from these events. Whereas the UK is trying to look forward and assess what reasonable order of magnitude of likelihood of events that could be occurring in the future, and also potential new risks. Second, the risk assessment should be used for capabilities based planning, but it is time consuming to build capabilities, so the risks should not be those that are the most immediate. A separate horizon scanning process is put in place for these.

The longer the time horizon, the greater the uncertainty and there is therefore a balance between selecting risk scenarios that are close enough to come up with reasonable assessments, but far enough away to have time to plan for the events which come out of the assessments.

Risk monitoring and re-evaluation

The UK Government has conducted a National risk assessment each year since 2005. A recent review concluded that the interval should in future be two years rather than one. The risk review process takes roughly 9 months. At the beginning of the process, the CCS approaches all government departments that own a risk and asks them to provide information on whether their risks have changed. The CCS asks them for evidence, in the form of amendment to the reasonable worst case scenario, of changes in the likelihood or impact of a risk that they own. They are also asked whether they wish to propose a more fundamental change to the scenario suggesting a changed risk.

In more recent years, the CCS has consulted the **national hazards partnership** – a group of external experts – to review the risks and provide recommendations on how any risks need to change. The purpose of this is to get an independent view of the current stock of risks in the NRA, and to identify new risks that may otherwise be neglected either because they fall outside the area of responsibility of any single department (e.g., space weather) or because events have increased their significance in ways that existing

risk owners are unaware (e.g., the new wildfire risk which is an example of the interaction of known risks with new vulnerabilities).

The results of this systematic review of existing risks, and the search for new or significantly altered risks have been the identification of one or two new risks every year, and substantial amendment of about 5 or 6 risks.

Communicating the results of National Risk Assessment

Using the National Risk Assessment to raise awareness about risks

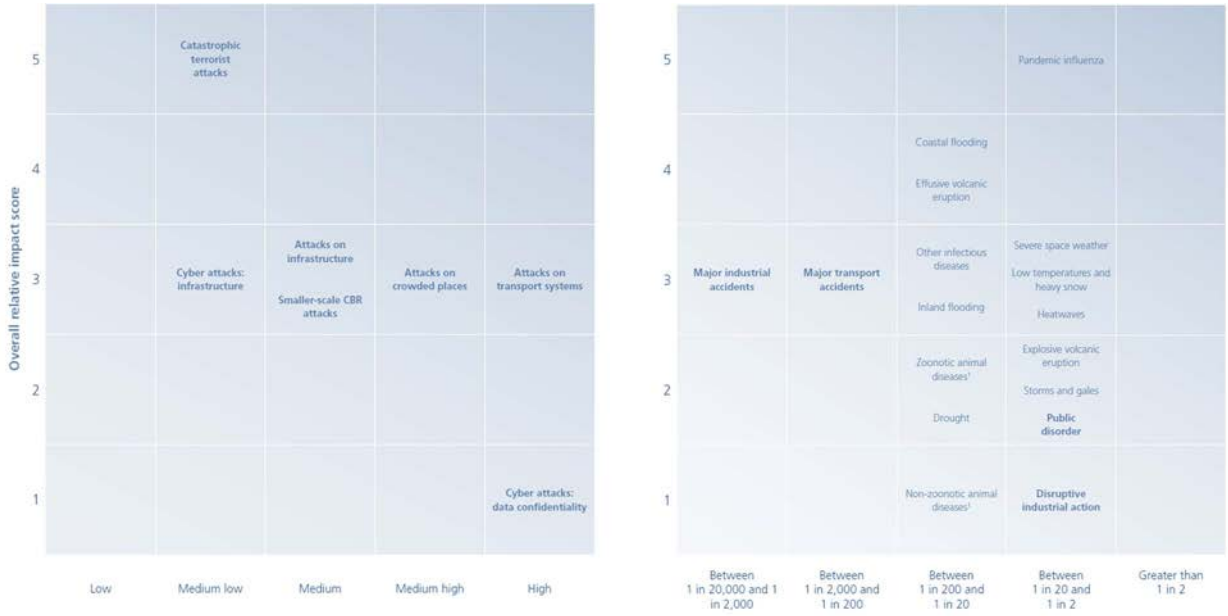
The outcome of the National Risk Assessment process is used to raise awareness or risk at the highest level of policy within Government, through the submission of the full assessment to the National Security Council, chaired by the Prime Minister, and by the use of the NRA – in particular the matrix – to brief new Ministers on the responsibilities they and their Departments are expected to manage. The NSC approves both the National Risk Assessment and the National Resilience Planning Assumptions that derive from the NRA, and so its members affirm their departmental responsibilities for risk management and, in some case, responsibilities for managing the impacts that they own. At the local level, as noted above, the NRA and associated guidance is designed to aid construction of risk registers by Local Resilience Forums.

Tools for interpreting risk analysis

The NRA forms the basis for a range of risk communication products. Since 2008, the Government has periodically published a summarised version of the NRA entitled the National Risk Register (NRR) which is intended to promote greater awareness of the commonly recurring risks of emergency and so promote community, business and organisational resilience. The unclassified NRR aims to raise public and community awareness, including the voluntary sector and small, medium enterprise. It provides information on government preparedness and encourages community resilience and business continuity. The origin of the policy to publish this abridged form of the NRA is linked to the overall civil contingency strategy to not just protect citizens, but to make them more resilient. This implies the need to inform people about the risks that they are knowingly or unknowingly accepting. If government does not explain what the risks are, then the people and businesses would make uninformed decisions, and possibly more expensive ones about their own security and resilience.

The availability of information pertaining to risks has steadily increased to help those who want to improve their ability to respond to emergencies. Restricted guidance for statutory resilience planners has been issued since 2005 to provide guidance on how to locally interpret the NRA. Since 2011, the NRA has been circulated to the chairs of Local Resilience Forums (usually the Chief Constable of Police in the area concerned) and a restricted version of the NRPAs is distributed to all statutory resilience planners. The CCS provides support to local emergency responders to identify, quantify and assess the risks in their own areas. The local levels of government are provided with a significant amount of information to generate local planning assumptions coherent with the national planning assumptions. CCS has also identified 9 infrastructure sectors with whom it shares its risk assessments. These are useful to inform Business Continuity Planning Assumptions (BCPA) and thereby raise awareness of planning considerations for the business sector, which are key to encourage supplementary resilience planning.

Figure 24.1. Risk of terrorist and other malicious attack (left)
Risk of natural hazards and major accidents (right)



Source: Cabinet Office (2012).

Main lessons learnt and policy outcomes

Lessons learnt

The National Risk Assessment in the context of the United Kingdom was never conceived to be a crystal ball, and this view has been confirmed by the experience of several renditions. It should be noted that the NRA has survived as a tool for civil contingencies planning in part because of its track record for accuracy in identifying hazardous events that subsequently happen. Nonetheless, the CCS avoids speculating on, or attempting to predict, future shocks in an inherently unpredictable risk landscape. It is fundamental to couch each risk scenario in terms of likelihood or plausibility to convey that these events will not necessarily happen. Uncertainty about this runs in both directions; the risk scenarios might not materialise, but there have also been cases where major civil contingencies occurred and for which no risk scenario had been retained for inclusion in the final NRA. This was the case, for example, when many air passengers were stranded both in the United Kingdom and abroad as a result of a volcanic ash cloud over Northern Europe.

One lesson learnt from the volcanic ash cloud event of 2011 was that if an NRA process looks to the government departments as its main source to identify risks, the risks that do not have any obvious owner, for example, volcanic ash clouds or space weather might fall between the cracks. Moreover, events that have happened may not be directly described in the risk scenarios, yet their common consequences are captured within a range of scenarios. A good example is rioting in London, of which the common consequences were covered by a range of scenarios. The event was not exactly as described, but it did mean that there was some preparation in place for that particular type of event.

Secondly, the NRA has allowed the UK to develop a strategy for managing risk, building off a generality of risks approach, focusing on the general risks, on the consequences and it also enables the UK to identify the 5 or 6 risks for which to have special programs such as flu pandemics, major flooding, catastrophic terrorism and volcanic effusions. For those for which the UK had identified early on, such as pandemic, the government was able to use the risk assessment to justify major programs of investment.

Benefits

The immediate benefits in planning terms are that the NRA has helped the UK to adopt a better strategy for managing risks, providing an objective and systematic evidence base for government-level emergency planning, prioritising investment in resources so as to be proportionate to the risks, and providing accessible guidance to local emergency planning for their emergency planning work. The wider benefits that CCS has identified are that systematic national risk assessment enables governments to:

- Build consensus on the risks of emergencies, breaking down departmental stove-pipes and facilitating cross-cutting collaboration between Departments and agencies.
- Avoid the need for speculation on, or attempting to predict, future shocks in an inherently unpredictable risk landscape.
- Prioritise risks according to the likelihood of them materialising and the potential impact when they do.
- Identify the highest risks requiring special programmes of mitigation by the government.
- adopt strategies for managing the risks, including identifying the potential and priority for preventive action.
- Communicate information on the risks more widely, and so support a strategy of building resilience from the bottom up.
- Provide a basis for both nearer term horizon-scanning for imminent emergencies, and a longer-term strategic assessments of risk trends.

Limits

Challenges for national risk assessment in the UK have included:

- Identification of risk owners in circumstances where the risk is ubiquitous or ambiguous - for example, the risks in cyber-space which may have many origins and many outcomes.
- Striking the balance between science and policy judgment. The UK approach puts policy makers to the fore – especially in allocating lead responsibility for the risks – but has accorded a strong role for Departmental Chief Scientific Advisers in supporting the policy judgements with scientific analysis. The UK has a Scientific Advisory Group for Emergencies which advises both planning and crisis management, and the Government's chief scientific adviser signs off the NRA as a valid planning document.
- The availability of data. The UK system avoids over-precise calculations of impact or likelihood where the evidence does not support this; and uses a logarithmic scale to counter the temptation to excessive precision.

Policy inputs and outcomes

The NRA informs decisions on which risks should be prioritised for risk mitigation work; what the best approach is to mitigating risks or their consequences (through prevention, or improved preparedness for consequence management, or a mixture of both); and what scale of impacts need to be planned for.

Before the NRA is delivered to and considered by decision-makers to finally make policy changes the risk assessment goes to the National Security Council for clearance and so do the national resilience planning assumptions. Every risk has a departmental risk owner, every planning assumption has a departmental owner and in accepting the risk assessment and the planning assumptions ministers are accepting in relation to risks and planning assumptions that they own.

Ministerial agreement to the NRA and the National Resilience Planning Assumptions triggers revisions to the national resilience capabilities programme – a portfolio of programmes (for example a community resilience programme, an infrastructure resilience programme, and a resilient telecommunications programme) designed to implement improvements in national resilience across most sectors.

In the longer term, risk assessment at a national level is also employed in constructing the UK's National Adaptation Plan for Climate Change, which is based on the 2012 Climate Change Risk Assessment, in the National Infrastructure Plan, and in providing strategic early warning of changes in the risks to UK's national security interests, currently set out in the 2010 National Security Risk Assessment.

References

Cabinet Office (2012), National Risk Register (NRR) of Civil Emergencies and Emergency planning.

Cabinet Office (2015), National Risk Register (NRR) of Civil Emergencies and Emergency planning.

Chapter 25. UNITED STATES

The Strategic National Risk Assessment (SNRA) in the United States has a wide scope and covers in general terms natural hazards, terrorism, the use of weapons of mass destruction and cyber-attacks. The driving force behind the SNRA is the Presidential Policy Directive 8 (2011) which gives responsibility to the Department of Homeland Security (DHS) to act as lead agency. Stakeholder involvement in this process is high with an ethos of openness when appropriate given national security consideration. It is considered that there is a balance to be struck in making the process as transparent as possible for those who need to know such as planners and regional entities and protecting and ensuring security. The SNRA is therefore not available to the public at this time. National preparedness is seen as a shared responsibility at all levels of government with the integration of risk analysis across state, regional and local levels.

Key Words: All of government approach; Collaborative thinking; Common understanding and awareness; National Risk profile; National preparedness goal; National security consideration; Identification of relevant risk factors.

Introduction

The Department of Homeland Security (DHS) and the Federal Emergency Agency (FEMA) led the development of the Strategic National Risk Assessment (SNRA) in 2011, which evaluates known threats and hazards that have the potential to significantly impact the homeland security of the United States. The broad purpose of the SNRA is to inform homeland security preparedness and resilience activities. The process was carried out under the authority of the DHS, with the participation of experts from across DHS and FEMA, as well as members of the Federal interagency community.

The results of the SNRA include a comparison of risks for potential incidents in terms of the likelihood (calculated as a frequency, i.e., number of events per year) and consequences of threats and hazards, as well as an analysis of the uncertainty associated with those incidents. The assessment finds that a wide range of threats and hazards pose a significant risk to the United States, affirming the need for an all-threats/hazards, capability-based approach to preparedness planning. Its scope includes analysis of natural hazards, including hurricanes, earthquakes, tornadoes, wildfires, and floods, infectious disease, technological and accidental hazards with the potential to cause extensive fatalities and severe economic impacts. It also considers risk drivers that increase the likelihood of occurrence that a risk may occur, such as accidents due to aging infrastructure. The assessment covers various facets of the risk of terrorism, including the use of weapons of mass destruction and conventional terrorist attacks, such as those by lone actors employing explosives and armed attacks. Cyber-attacks are also considered for their capacity to initiate other hazards, such as power grid failures or financial system failures, and to amplify different hazards.

The development of the SNRA is considered a first step in an on-going effort. Further analysis through regional and community level risk assessments is under consideration to help communities better understand their risks and form a foundation for their own security and resilience. In conjunction with federal, state, local, tribal, and territorial partners, the SNRA will be expanded and enhanced and will ultimately serve as a unifying national risk profile to facilitate preparedness efforts.

Governance framework

The overall policy context for the development of the Strategic National Risk Assessment is found in Presidential Policy Directive 8 (2011), issued by the United States President to strengthen the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the country. PPD-8 calls for the development of a “National Preparedness Goal” (NPG) that identifies the 30 core capabilities necessary for preparedness, ranging from mass care to search and rescue to infrastructure protection etc., and a “National Preparedness System” (NPS) to guide activities that enable the United States to achieve the goal and track progress.

The PPD-8 implementation plan directed the Secretary of Homeland Security to conduct a strategic national-level risk assessment to identify the relevant risk factors that guide where core capabilities are needed and develop a list of the capabilities and associated performance objectives for all hazards that will measure progress toward their

achievement. Consequently the Department of Homeland Security had the lead co-ordination role in the SNRA.

Aims and objectives

The SNRA is used to:

- Identify high risk factors that supported development of the core capabilities and capability targets in the National Preparedness Goal.
- Support the development of collaborative thinking about strategic needs across prevention, protection, mitigation, response, and recovery requirements.
- Promote the ability for all levels of Government to share common understanding and awareness of national threats and hazards and resulting risks so that they are ready to act and can do so independently but collaboratively (The Strategic National Risk Assessment in Support of PPD 8, 2011, p.1).

Definition of key terms

The Department of Homeland Security has produced a DHS Risk Lexicon to make available a common, unambiguous set of official terms and definitions to ease and improve the communication of risk-related issues for DHS and its partners.[1] It is intended to facilitate the clear exchange of structured and unstructured data that is essential to the exchange of ideas and information amongst risk practitioners by fostering consistency and uniformity in the usage of risk-related terminology for the Department.

The Department of Homeland Security (DHS) distinguishes between persistent risks and contingency or event based risk. Persistent risk are classified as activities that DHS carries out continuously and on a regular basis (365 days a year) such as boarder security as opposed to contingencies. However the Strategic National-Level Risk Assessment focuses on the contingency side and does not address high frequency/low consequences actives, such as immigration, facilitating trade and travel, as they are persistent in nature.

Transparency and accountability

While the outcomes of the Strategic National Risk Assessment have been outlined extensively to all stakeholders who participated at federal, state and local level, it must be said that the document in its present form is classified. To this end, there are efforts ongoing to produce a releasable or sanitised version. From the perspective of planners, the release of an unclassified and publicly available document is important.

The challenge lies in balancing the content of a document to be released with sufficient detail that it is useful for planners but without revealing such information about vulnerabilities that it would undermine security objectives. Notwithstanding its classified character, all sources and estimates used to conduct the risk analysis in the SNRA were documented to promote credibility, defensibility, and transparency within the community involved in the assessment.

Multi-level governance and multi-actor participation

PPD-8 envisages national preparedness as the shared responsibility of all levels of government, the private and non-profit sectors, and individual citizens. The SNRA is a multi-agency effort of the federal government, but its goal is to integrate of analysis across state, regional, and local levels. The Department of Homeland Security works with

experts in the federal government to find the best data sources for risk analysis. In terms of co-ordination and stakeholder input, FEMA's PPD 8 implementation team organised working groups with interagency members as a main mechanism for co-ordination and synchronisation. The team continues to be a standing body with working groups on prevention, protection, mitigation, response and recovery. DHS has leveraged those groups for co-ordination and also established additional SNRA working groups focusing on natural hazards, technological/accidental hazards and adversarial human-caused threats/hazards. These remain in place to date in a forum to ensure stakeholder input and opinion sharing across the whole-of-government. By enabling discussion through a standing body, the idea is to have a discussion over competing views or issues, with ultimately the work still being driven by the lead agency.

The body within DHS responsible for executing the SNRA at the time (the Office of Risk Management Analysis) viewed themselves for the most part as an independent group, searching for the best available knowledge. The office took a more scientific based analysis and approach by systematically and transparently documenting all sources and assumptions. To some extent experts were drawn from outside the ranks of government departments and agencies, and in particular for information about some of the natural hazards. These various sources provided the SNRA process with data and information, existing government models and assessments, historical records, structured analysis and judgments of experts from different disciplines.

DHS tried to find the best information regardless of the source in light of time constraints. Participation of subject matter experts from across federal government agencies was an important element of a successful effort. For this purpose, the working groups on assessment of pandemic influenza included experts from the Department of Health and Human Services, the Centres for Disease Control and Homeland Security's Internal Office of Health Affairs. Each organisation readily contributed data to build this assessment. In addition to leveraging the experts in other departments through the working groups themselves, different agencies were specifically mentioned by the directive to contribute to the assessment. For example, the Director of National Intelligence and Attorney General provided relevant and appropriate terrorism-related intelligence information to the Secretary of Homeland Security for the development of the SNRA.[2]

DHS also draws from internal federal agencies along with the weather service and academic work in which it looked at some of the consequence types. In addition, DHS reached out to academic centres of excellence[3], which provide subject matter expertise on areas such as psychological impacts and social displacement

Risk analysis

The results of the SNRA include a comparison of risks for potential incidents in terms of the likelihood (calculated as a frequency—i.e., number of events per year) and consequences of threats and hazards, as well as an analysis of the uncertainty associated with those incidents.

The SNRA relied on the best available quantitative estimates of frequency and consequence from existing Government assessments, peer-reviewed literature and expert judgment. Where sufficient quantitative information was not available such as data related to the frequency of high-consequence space weather, these events were assessed qualitatively. The estimates of the frequency and consequences for each of the events considered were compared where appropriate.

No effort was made to create a single risk judgment for any event type because it was deemed impractical to aggregate all consequence types into a single metric. Instead, the assessment treated consequence categories separately (i.e., economic consequences are reported separately from fatality consequences). This allowed stakeholders to apply their own expert judgments to the findings and decide how those findings should inform core capability targets in the National Preparedness Goal.

Information about the frequency and consequences of the events included in the SNRA is at varying stages of maturity, with additional work required in some areas to ensure that event data can be appropriately compared.

Scope

PPD-8 is meant to prepare for all-hazards, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters. The events are grouped into three categories: 1) natural hazards; 2) technological/accidental hazards; and 3) adversarial, human-caused threats/hazards.

Only events that have a distinct beginning and end and those with an explicit nexus to homeland security missions were included. Events that present risk to the national level, such as nuclear attacks or chemical releases, require additional specialised response activities. Some events, such as explosives attacks or earthquakes generally cause more localised consequences, while other events, such as human pandemics, may cause consequences that are dispersed throughout the country, thus creating different types of impacts for preparedness planners to consider. This approach to scoping the SNRA excluded: chronic societal concerns, such as immigration and border violations, and those that are generally not related to homeland security national preparedness, such as cancer or car accidents, and political, economic, environmental, and societal trends that may contribute to a changing risk environment, but are not explicitly homeland security national-level events (e.g.,, demographic shifts, economic trends).

Hazard identification

The SNRA participants identified 23 risk scenarios as those with the potential to pose the greatest risk to the security of the United States (Table 1). The SNRA's risk scenarios are very short descriptive vignettes. Floods occurring in the United States that results in direct economic losses greater than USD 100 million. This threshold was agreed upon within the working group structure and serves as an example of what would qualify the risk as nationally oriented risk rather than regional or local. In the assessment, DHS tries to understand the range of consequences (given the event is above the threshold), and how frequently such an event may occur.

Table 25.1 is not a complete list of the risks that exist and will be reconsidered in future iterations of the SNRA. Participants in the process identified a number of risk scenarios for possible inclusion in future versions of the SNRA. These included droughts, heat waves, winter storms, rain storms, and different types of technological/accidental or human-caused hazards that can also pose a risk to jurisdictions across the country and should be considered, as appropriate, in preparedness planning. Non-influenza diseases with pandemic potential and other animal diseases should also be considered.

Table 25.1. SNRA National-Level Events

Hazard Group	Hazard Type	National-level Event Description
Natural	Animal Disease Outbreak	An unintentional introduction of the foot-and-mouth disease virus into the domestic livestock population in a U.S. state
	Earthquake	An earthquake occurs within the U.S. resulting in direct economic losses greater than $100 Million
	Flood	A flood occurs within the U.S. resulting in direct economic losses greater than $100 Million
	Human Pandemic Outbreak	A severe outbreak of pandemic influenza with a 25% gross clinical attack rate spreads across the U.S. populace
	Hurricane	A tropical storm or hurricane impacts the U.S. resulting in direct economic losses of greater than $100 Million
	Space Weather	The sun emits bursts of electromagnetic radiation and energetic particles causing utility outages and damage to infrastructure
	Tsunami	A tsunami with a wave of approximately 50 feet impacts the Pacific Coast of the U.S.
	Volcanic Eruption	A volcano in the Pacific Northwest erupts impacting the surrounding areas with lava flows and ash and areas east with smoke and ash
	Wildfire	A wildfire occurs within the U.S. resulting in direct economic losses greater than $100 Million
Technological/ Accidental	Biological Food Contamination	Accidental conditions where introduction of a biological agent (e.g., Salmonella, E. coli, botulinum toxin) into the food supply results in 100 hospitalisations or greater and a multi-state response
	Chemical Substance Spill or Release	Accidental conditions where a release of a large volume of a chemical acutely toxic to human beings (a toxic inhalation hazard, or TIH) from a chemical plant, storage facility, or transportation mode results in either one or more offsite fatalities, or one or more fatalities (either on- or offsite) with offsite evacuations/shelter-in-place
	Dam Failure	Accidental conditions where dam failure and inundation results in one fatality or greater
	Radiological Substance Release	Accidental conditions where reactor core damage causes release of radiation
Adversarial/ Human-Caused	Aircraft as a Weapon	A hostile non-state actor(s) crashes a commercial or general aviation aircraft into a physical target within the U.S.
	Armed Assault	A hostile non-state actor(s) uses assault tactics to conduct strikes on vulnerable target(s) within the U.S. resulting in at least one fatality or injury
	Biological Terrorism Attack (non-food)	A hostile non-state actor(s) acquires, weaponised, and releases a biological agent against an outdoor, indoor, or water target, directed at a concentration of people within the U.S.
	Chemical/Biological Food Contamination Terrorism Attack	A hostile non-state actor(s) acquires, weaponized, and disperses a biological or chemical agent into food supplies within the U.S. supply chain
	Chemical Terrorism Attack (non-food)	A hostile non-state actor(s) acquires, weaponised, and releases a chemical agent against an outdoor, indoor, or water target, directed at a concentration of people using an aerosol, ingestion, or dermal route of exposure
	Cyber Attack against Data	A cyber-attack which seriously compromises the integrity or availability of data (the information contained in a computer system) or data processes resulting in economic losses of a Billion dollars or greater
	Cyber Attack against Physical Infrastructure	An incident in which a cyber-attack is used as a vector to achieve effects which are —beyond the computerll (i.e., kinetic or other effects) resulting in one fatality or greater or economic losses of $100 Million or greater
	Explosives Terrorism Attack	A hostile non-state actor(s) deploys a man-portable improvised explosive device (IED), Vehicle-borne IED, or Vessel IED in the U.S. against a concentration of people, and/or structures such as critical commercial or government facilities, transportation targets, or critical infrastructure sites, etc., resulting in at least one fatality or injury

Nuclear Terrorism Attack	A hostile non-state actor(s) acquires an improvised nuclear weapon through manufacture from fissile material, purchase, or theft and detonates it within a major U.S. population centre
Radiological Terrorism Attack	A hostile non-state actor(s) acquires radiological materials and disperses them through explosive or other means (e.g.,, a radiological dispersal device or RDD) or creates a radiation exposure device (RED)

Source: The Strategic National Risk Assessment in Support of PPD 8 (2011): A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation.

Impact analysis

The SNRA examined the consequences associated with six categories of harm: loss of life, injuries and illnesses, direct economic costs, social displacement, psychological distress, and environmental impact. This multi-criteria approach for qualifying consequences is designed to reflect the broad and often interdependent effects of incidents that require whole of community preparation and cooperation. For instance, community resilience relates to both mitigating human and economic consequences and addressing the psychological and social distress caused by the incident within the community. Similarly, other types of resilience involve withstanding environmental and infrastructure degradations to ensure that essential services continue to be delivered.

Most of the impacts were carried out using a quantitative methodology. Therefore, rather than specifying scoring for example from 1 to 5, DHS includes estimates using numbers, e.g., 1500 people, or which numbers the models or data sources would give as an output. As a result, the aim is to achieve a best estimate as well as a low and a high value situated on either side of the best estimate point to represent the inherent uncertainty.

For the purposes of the assessment, DHS identified thresholds of consequence necessary to create a national-level event. These thresholds were informed by subject matter expertise and available data. For some events, economic consequences were used as thresholds, while for others, fatalities or injuries/illnesses were deemed more appropriate as the threshold to determine a national-level incident. In no case, however, were economic and casualty thresholds treated as equivalent to one another (i.e., dollar values were not assigned to fatalities). Event descriptions in Table 1 that do not explicitly identify a threshold signify that no minimum consequence threshold was employed. This allows the assessment to include events for which the psychological impact of an event could cause it to become a national-level event even though it may result in a low number of casualties or a small economic loss.

Likelihood and plausibility analysis

The SNRA measures likelihood in terms of frequency (i.e., the number of events per year) e.g., a 1 in 10 or 100 year event for many events, however when the data is not available to support these methods DHS described the events more qualitatively in narrative form. The SNRA found many of the identified events have the potential to occur more than once every 10 years. Many of the models leveraged (for example models from DHS' Science and Technology Directorate) incorporate aspects such as intent, capability, feasibility but also a frequency initiation concept, which is how frequently a group may try to initiate an attack. Taking into account the group and government's capabilities DHS calculates the frequency with which the model expected would be successful.

Although historic events provide a useful perspective on homeland security risks, the changing nature of society and the risk landscape means that the United States must also

be prepared for new hazards and threats, or for events that result in greater consequences than have occurred in the past. Therefore, similar to the analysis for consequence, a best estimate for frequency is provided as well as low and high bounds to reflect uncertainty. Where substantial additional research is warranted, events are discussed qualitatively and are not compared with other events. Examples of sources of uncertainty include incomplete knowledge of adversaries' capabilities and intent, variability in possible event severity and location and lack of historical precedence.

Time horizon

The SNRA uses a 3/5 year time horizon to characterise the events that fall within its scope. DHS has different efforts ongoing to explore the current strategic environment which help shape the government's strategic planning for the future. Chief among these is the foresight analysis carried out under the 2010 FEMA Strategic Foresight initiative4, which emphasises the importance of understanding and addressing the drivers of future change. This initiative urges the emergency management community to establish a foresight capability to identify future issues and trends and other factors for the agenda in the next 20 years. There is an argument to expand the foresight analysis to analyse the interdependencies in these areas and go beyond the defined end points of risk scenarios and take an overall holistic view given the threats to critical systems that might be impacted over time.

Risk evaluation, monitoring and re-evaluation

PPD-8 states that the risk assessment is to be updated periodically; however, it does not provide specificity. From DHS's perspective it should be reviewed every two years in order to stay current with respect to the strategic environment and ensure the assessment of risks the pace of change in the surrounding environment. Changing events could drive DHS to conduct national level assessments more frequently, however in light of supporting budgeting processes, long range planning processes and strategic planning a two year is most feasible. Discussion between all partners may be necessary in this regard, however consensus is for the most part that the SNRA does need to be updated and a two-year period would be suitable.

Communicating the results of National Risk Assessment

Using the National Risk Profile to raise awareness about risks

The foundational work of the Strategic National Risk Assessment is largely classified. Future work on the SNRA might consider the production of a publicly available version to ensure openness in Government and the wider application of the underlying data. In such a case, the information regarding likelihood and consequences of the identified risks would be made available to the general public and business community, in some format, to encourage implementation of capabilities by the "whole-of-society", i.e., from the departments of the Federal Government to individual citizens.

Main lessons learnt and policy outcomes

Lessons learnt process

The goal was to tie the risk assessment explicitly to capability targets. In practice however, because the list of capabilities were being developed at the same time as the risk

assessment. This was not a realistic goal at that time and needed further analysis. Planning for this type of result will take place in the future.

One of the lessons learnt from any risk assessment process is that analysis of available information supports better decision making as long as key limitations and assumptions are noted. Participants designed the SNRA to capture the best information the Nation has about homeland security risks to support the development of the National Preparedness Goal, while recognising the limitations of conducting such analysis in a shortened time frame. Some assumptions have been made and therefore it is an iterative process and needs constant vigilance with the prevailing threat landscape.

Benefits

The strategic national risk assessment exercise is considered as very successful from the US Government stand point and also from a national level risk scoping point of view. The DHS can now start to expand upon SNRA and authorities are confident it will serve as a good launching pad for building future work. This is evidenced by the positive tone of the 2014 Quadrennial Homeland Security Review Report and the DHS's Strategic Plan for fiscal years 2014 to 2018 which pay glowing tributes to previous work carried out by practitioners in the Emergency Management Community.

Whilst the initiative to identify and quantify national risks has been completed, there is much work to be done. As the first initiative in bringing together the multiple agencies to assess risk, the SNRA is now helping to inform the future strategies. It also has the advantage of having brought together experts in this field at that time. However, similar to all processes they have a shelf life, not only in the data but also in skill set.

The SNRA is acknowledged to have changed the tone and thinking in the national risk mind-set and led FEMA and planners to think about risks and capabilities through the periscope of a detailed national risk assessment. This is beneficial for moving forward the foresight analysis in the risk characterisation for changes in the risk landscape.

Limitations

The Department of Homeland Security considered the initial version of the SNRA to be a step forward in the establishment of a new homeland security risk baseline, but acknowledges that it contains data limitations and assumptions requiring additional study, review, and revision. Additional research is required to further explore psychosocial factors that enable resilience in individuals, organisations, and communities and at the societal level. For national-level events where historic data was used as the basis of analysis, the risk from low-likelihood, high-consequence incidents may not be adequately captured. This is particularly true for technological/accidental hazards. Future iterations of the assessment are expected to reflect an enhanced methodology and improved data sets.

The scope and nature of the strategic national risk assessment does not comprise of a full view of the risks facing the United States, Those risks facing sub-national communities, many of which differ from region to region. Nor does the SNRA explicitly assess persistent, steady-state risks such as border violations, illegal immigration, drug trafficking, and intellectual property violations. While these remain important considerations for DHS and the homeland security enterprise, the emphasis of PPD-8 is on contingency events with defined beginning and endpoints (e.g., hurricanes, terrorist attacks).

The SNRA methodology does not explicitly model the dynamic nature of some of the included hazards. The evolving tactics of terrorists in response to changes in defensive posture are not included. Experts consulted about psychological consequences emphasised caution in the application of the SNRA's measure of psychological distress, and stressed the need for additional research. The Department of Homeland Security and its partner organisations leveraged previously funded social and behavioural research to better understand how to anticipate, prepare for, counteract, and mitigate the effects of terrorist acts, natural disasters, and technological accidents.

Policy Outcomes

The SNRA served as an integral part of the development of the National Preparedness Goal, assisting in identification of core capabilities and establishing a risk-informed foundation for the National Preparedness System. The core capabilities identified in the NPG are mapped to events assessed in the SNRA to identify any additional core capabilities that may need to be included. In addition, the SNRA can be used to inform discussions on priorities for capability investment decisions. Finally, the SNRA results could be used to drive other preparedness priorities at the national level.

In addition, conducting a Strategic National Risk Assessment supports the National Preparedness System by providing a consolidated list of national level events for threat and hazard identification and risk assessment processes at multiple jurisdiction levels. Finally, the results of the SNRA provide the basis for risk-informed priorities in the Quadrennial Homeland Security Review (QHSR),5 which lays out the vision, mission areas, goals and objectives for homeland security, and drives operational planning, as well as analysis of resource and capability options and trade-offs.

Notes

1. Available at: https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

2. Implementation plan for presidential policy directive 8: national preparedness, p.2

3. Centres of excellence include: University of Maryland, Study of Terrorism and Responses to Terrorism (START) http://www.start.umd.edu/start/; University of Southern California (USC) CREATE: http://create.usc.edu/

4. http://www.fema.gov/strategic-foresight-fema

5. https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf

Reference

Department of Homeland Security, (2011) The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk Based Approach towards a Secure and Resilient Nation"

ANNEX A

National Risk Assessments and the purposes to which they are put

COUNTRY	
Australia	*National Emergency Risk Assessment Guidelines* are designed to: 1) Improve understanding of risk and ensure that risk treatment measures provide a sound return on investment, 2) Standardise risk assessments and development of risk reduction proposals, Increase transparency so that processes can be understood, checked or modified in light of improved knowledge/ information, 3) Improve consistency to allow meaningful comparison between different geographical areas and/or hazard classes, NERAG's aim is to provide a risk assessment method that: 1) Can be used for assessing emergency-related risks at a range of scales, 2) Examines historical and/or modelled (synthetic/scenario) emergency events across a range of likelihood and consequence levels, 3) Identifies current risk levels under existing controls and can be used to assess effectiveness of proposed treatments (which may include new controls or control improvements), 4) Allows the use of various forms of evidence to inform the understanding and assessment of risks, including quantitative data, expert evidence and stakeholder consultation, 5) Allows risk evaluation at varying levels of confidence, 6) Provides outputs that allow for risks to be prioritised, and suggests either treatment planning, further investigation, or ongoing monitoring and review for each risk. NERAG is not intended to support or replace operational emergency-related risk assessment tools. That is, it is not intended that the NERAG method be used to assess risk to emergency personnel who are, for example, undertaking emergency response duties.
Austria	• Maintaining social peace and social cohesion in Austria and promoting a good and safe coexistence, • Ensuring the availability of vital resources, • Enhancing the resilience of the public and private sector when faced with natural or man-made disruptions and disasters, • Maintaining an efficient national economy and taking precautions for the eventuality of crisis- related economic disruptions, safeguarding the supply of vital goods to the population, and protecting critical infrastructure, • Maintaining a liveable environment as part of comprehensive environmental protection and minimising the negative effects of natural or technological disasters, • Combating international terrorism, organised crime and corruption, • Promoting a broad awareness of security amongst the population.
Canada	1) The All Hazards Risk Assessment (AHRA) is primarily used for the emergency management planning functions for departments that own specific risks 2) To produce a collective judgment of risk assessments currently being carried out by different federal government institutions and provides a whole-of-government picture to inform future actions and initiatives.
Denmark	Primarily a risk communication tool, which complements other guidance (on *crisis management in Denmark*, on *comprehensive preparedness planning*, and on *risk and vulnerability* analysis) in order to 'contribute to preparedness planning assumptions among organisations within different sectors, across sectors, and at the central level of the national planning system'.
Estonia	Three kinds of documents concerned with risk assessment, each with different objectives: *National summary of emergency risk assessments*, providing an overview of (currently 27) types of emergency requiring government intervention. Acts as a brief for Ministers, raising awareness of national risks, clarifying responsibilities, promoting a risk management culture and, to a limited extent, establishing government priorities, *Emergency risk assessments* by government institutions designated by statute, designed to contribute to 'ministry development plans' for those risks and to inform capability development; 2009 legislation implies that Ministers have to take account of risk assessments in drawing up departmental plans, *Vital service continuity risk overviews* designed to inform plans to ensure the continuous operation of 46 different kinds of essential service, and aid capability building by each of the providers.

Finland	A first *National Risk Assessment* in 2015 will harmonise risk assessment processes for the country as a whole, with the objective of: promoting consensus and a risk management culture; and developing risk management strategies and capabilities at national, regional and local levels, reflecting the evolution of the Country's risk profile: • Identifying and quantifying the (probably 6) 'top tier' national risks for which the government will develop risk management strategies at the national level, • Identifying and assessing 'tier 2' risks that will be for the regional level of government, • Promoting the development of local risk assessments covering 'tier 3' risks deemed to be for local management.
Germany	The Federal government in cooperation with the Lander compiles a nationwide risk analysis providing "a neutral and transparent basis of decision-making [relating to] risk management (e.g., prioritisation of measures for the minimisation of risks), emergency planning (e.g., preparation for incidents that cannot be avoided) and crisis management (e.g., provision of resources for response)". The aim of the risk analysis for civil protection is to create as comprehensive and comparative an overview as possible (a risk portfolio) of the likelihood of various risks and events occurring and the extent of damage they are expected to cause.
Hungary	The Government produces a *National Disaster Risk Assessment* specifically designed to be compatible with guidance issued by the European Commission (SEC (2010)1626 dated 21.112.2010), so satisfying the so-called ex-ante conditionality for access to EU funds for thematic operational programmes in 2014-2020. In Hungary's case, the government aims to develop an operational programme that promotes climate change adaptation and risk prevention, so the NRA will cover both a near-term (5 years) perspective and a much longer term (20-25 year) forward look taking into account the potential effects of climate change
Korea	• Building national consensus on priorities for risk management, in an inherently complex risk environment encompassing threats, natural hazards, and man-made accidents. • Support for the adoption risk management strategies. • Informing the objective quantification of risk analyses – both in terms of likelihood and consequence – to aid decisions on investment in capability and capacity. • Assisting in risk communication to citizens to mobilise self-help preparedness among business and social communities.
The Netherlands	• To provide a consistent evidence base for decisions to be made by the Government on the priorities for and approaches to the management of the main risks to national safety and security, and investment in the capabilities needed for response and recovery, • For each of the main risks assessed, a capability analysis is carried out and research conducted on whether the Netherlands has sufficient capacity available to stand up to the threat and on which areas capacity should be increased.
New Zealand	• Illustrate the spectrum of risks from those affecting individuals and communities, those affecting security of the State, to those that are clearly in the international domain, • Identify overlaps of responsibilities, • To provide a visual comparison of the approximate scale of the main components of significant risks – likelihood and consequence – in order to indicate for planning purposes the relative importance of the risks.
Norway	• Provide high level decision-makers and politicians an easily accessible comparative overview of disaster risks, • To frame planning in the ministries, sectors, municipalities, regional and local levels and private companies, • To inform capacity planning and the resources needed to cope with worst case scenarios that might occur in the future. The aims of the NRA vary according to different levels of government: o government leaders need an overall risk analysis, which does not go into detail nor serve as a basis for prioritisation of resources and overall management but rather provides a contextual basis for decision-making, o municipalities, counties and sectoral authorities can use the NRA to survey what national events might affect them and require preparedness measures, and as a basis for less serious scenarios that they can analyse themselves, • at the operational level of civil protection, the scenarios can be used as an input for exercises and emergency planning.
Poland	The *Report on Threats to National Security* has the objective of providing the authorities with a common understanding of risks at the national level in order to determine appropriate preventive and preparedness actions, to reduce the likelihood of national-level risks and minimising their consequences. This breaks down in more detail as follows: • Identification of significant threats (and their risk map if appropriate) • Identification of strategic risk management objectives in relation to each threat • Identification of the capabilities and resources necessary to achieve strategic objectives • Programmes to improve safety and security • Priorities in responding to specific risks

Portugal	• Guidelines for regional and local risk analysis and risk mapping, in the form of guidance on risk identification, methods of analysing impact and likelihood, and risk evaluation using a matrix as the means of presenting risks, • The basis for a risk reduction strategy at national level, including risk prevention, and reflecting Ministerial priorities, • A basis of evaluating risk as part of the approvals process for projects, • Evidence for investment in the resilience of critical national infrastructure, particularly in the energy and transport sectors, • A basis for risk communication to stakeholders in the business and social communities, underpinning programmes of early warning, directly to the public or through radio or television broadcasters. Examples include: a project with TV networks to provide an infomercial about how to use the warning system; projects to establish sirens as a low cost tool to warn the population, and to use social media to interact with smart phones using applications to inform about rapid onset events; a memorandum of understanding with specific national radio and television to inform people in specific situations, • Risk mapping (risk maps are in widespread use for land use planning; map are in PDF format and not interactive, • Scenarios for national, regional or local emergency response exercises.
Slovak Republic	• A comprehensive database of emergencies and damage caused, • Improvements in the level of awareness and knowledge of threats and their impacts that are insufficient for effective risk management, • Improvements and standardisation of the risk assessment processes understood in the various different sectors, • Putting in place an information system for sourcing, collection and distribution of data required for effective risk assessment, • Improvements in adopting the knowledge base for risk assessment, by citizens, volunteers and communities, to enable them to carry out preventive preparatory and protective measures.
Spain	The clear aim of a National Risk Assessment will be to provide relevant and evidence-based advice to the Prime Minister on the overall risk profile of the nation, to inform development of a successor to the 2013 NSS which will review the current risks and priorities in accordance with the 2015 National Security Act.
Sweden* (*Report based on 2013 survey; Sweden has subsequently developed National Risk and Capability Assessment)	The Swedish National Risk Assessment is an evolving project. The 2013 version identified 27 risks, for 11 of which risk scenarios were developed, of which 7 have been analysed for impact and likelihood; the 2014 version analysed [14] scenarios. Three purposes are identified: • To create a common understanding of the serious risks facing Sweden, • To improve the design of measures related to national emergency preparedness planning for a safer society, • As a complement to analyses of emergency management capability, which have not yet been developed. In addition, the NRA is meant to support the development of civil protection and emergency preparedness at local and regional levels, including for private sector organisations that perform vital societal functions.
Switzerland	The first *Disasters and emergencies Switzerland – Risk Report* was produced in 2012, setting out analysis of 12 key risks; a second has been produced in 2016, with a total of 33 risks assessed. A co-ordinated approach between the Cantons and Federal Agencies has the following aims: • To develop a method for analysing the risk of disaster and emergency scenarios that all responsible authorities can use, • To elaborate standardised scenarios and other uniformly structures foundations for disaster management, • To establish efficient and continuous analytical processes for disasters and emergencies.
United Kingdom	The *National Risk Assessment* is currently undergoing its twelfth iteration as part of a suite of risk assessment tools that include a short-term (6 month) *forward look* designed as an aid to crisis management, and a longer-term (5-20 year) National Security Risk Assessment, whose aim is to provide strategic early warning of changes to the risk environment. The purpose of the NRA has been under review but is considered to be: • To develop a common understanding of the risks of emergency among those responsible for managing them, • To enable civil emergency contingency planning for the highest risks, • To enable wider resilience planning, • To provide the basis of guidance to local emergency planning authorities, to assist them in their duties under emergency legislation (the Civil Contingencies Act 2004). A major review of the NRA in 2015 is being implemented in the 2016 NRA which will have the same fundamental purpose but introduce multi-risk scenarios an amended scoring system, and a two-year review cycle.
United States	• Identify high risk factors supporting development of core capabilities and capability targets in the National Preparedness Goal, • Support the development of collaborative thinking about strategic needs across prevention, protection, mitigation, response, and recovery requirements and, • Promote the ability for all levels of Government to share common understanding and awareness of National threats and hazards and resulting risks so that they are ready to act and can do so independently but collaboratively

ANNEX B

Transparency and Accountability and multi-level governance/multi-actor participation

COUNTRY	
Australia	The NERAG does not dictate the governance arrangements that will be appropriate to governments and other organisations using the guidelines, but the guiding principles for emergency risk management (ERM) make the clear the importance of: • Mainstreaming ERM activity so that it is effectively integrated into standard business practices of organisations, governments and communities. • Involving decision-makers and other stakeholders in a transparent way. • Basing decisions on ERM on the best available data and information from a variety of sources, ensuring that decision-makers are aware of the limitations of data and modelling, and of any divergence of opinion among experts.
Austria	The GERIAN project has been an open process, with the study of options for an Austrian NRA, conducted by the Austrian Institute for Technology (AIT), being published and the outcome – in terms of the process – being well enough known to those with an interest. Overall responsibility for co-ordinating this process lies with the Federal Ministry of the Interior, as the lead authority in Austria for co-ordination of civil protection and disaster management approaches.
Canada	The AHRA methodology is published publicly on Public Safety's website and results and methodology are reviewed by the Interdepartmental Risk Assessment Working Group (IRAWG). Results of the AHRA are presented to a committee of senior officials through a presentation and final report. Discussions and results are tracked in a risk scoring tool and through meeting minutes.
Denmark	The Danish Emergency Management Agency (DEMA), an authority under the Ministry of Defence, has a remit to improve preparedness for major emergencies in Denmark. DEMA cannot direct but assists competent state authorities with their preparedness plans, within the Danish national crisis management system. First produced in 2013, the National Risk Profile (NRP) is not supported by a specific legal framework but is a product of collaboration between DEMA as authors and the state authorities concerned, aided by feedback from international for a including the Nordic forum for risk assessment and the EC's expert group. Separately, DEMA co-ordinates guidance on risk and vulnerability analysis, compatible with ISO 3010, for voluntary use by public and private sector organisations throughout the country. DEMA consulted 60 organisations on the draft 2013 NRP, representing all levels of government and some key infrastructure providers, but no-one from the academic world.
Estonia	The 2009 Emergency Act sets out responsibilities for emergency preparedness at national, regional and local level; the Ministry of the Interior chairs the national Crisis Committee, which has a collective policy-making rather than executive role, and co-ordinates most crisis management and preparedness work including a summary of emergency risk assessments at national level. Separately, emergency risk assessments are carried out under the Act for 46 kinds of essential services (and involving 125 named vital service providers) under the supervision of the organising authority for each service, and within the overall co-ordination of the Ministry of the Interior. At this stage, participation by regional or local level government, by the academic sector, and by the private sector other than in 'vital service emergency risk assessments' is constrained.
Finland	For the first NRA, The Ministry of the Interior co-ordinates a Working Group of the national Security Committee with participation of all responsible departments of state including the Prime Minister's office and Ministries of foreign affairs, health and social affairs, agriculture and forestry, transport and communication, employment and the economy, environment, education and culture, and defence. The private sector is represented through the national emergency supply agency, and regional authorities through the Regional State Administrative Services, and the Centre for Economic Development, Transport and the Environment. Subject-matter experts can be consulted. Submission of first NRA to Ministers due autumn 2015, and publication of the outcome, including methodology, will enable stakeholders not directly consulted to feed back; creation of an independent challenge function ,ay follow following review of the first NRA. Development of regional and local risk assessments may follow, to cover 'tier 2' and 'tier 3' risks identified in the NRA 2015

Germany	In accordance with the Federal Civil Protection and Disaster Assistance Act, the Federal Government (with co-ordination by the BBK) in cooperation with the Lander compiles a nationwide risk analysis conducted through: a Steering Committee of representatives from federal ministries chaired by BBK; a Working Committee; and hazard-specific sub-groups of subject-matter experts led by specialised lead agencies. An annual report is made to the Federal Parliament on risk analysis for civil protection, and published online. BBK ensures that results of work on NRA scenarios are continuously communicated to Lander during the analysis phase to ensure transparency between national and federal governments. BBK guidance encourages engagement of scientists, economists and other SME through "Network Risk Analysis in Federal Agencies" and through the equivalent of this network approach at other administrative levels.
Hungary	The Ministry of the Interior (National Directorate General for Disaster Management - NDGM) takes lead responsibility for the NRA. NDGDM led an ah hoc Group on Disaster Risk Assessment including three thematic sub-groups (for natural disasters, man-made disasters, and intentional incidents) comprising SMEs from ministries, public authorities and research institutes. The outcome of the nRA was published on the government website. More than 20 institutions and authorities including the insurance industry, external consultants, multiple scientific research institutions and national ministries. Mayors and local disaster management committees are directed (Government Decree 10) to perform a disaster risk assessment.
Korea	The arrangements for development, implementation and maintenance of the risk assessment process are set out in exhaustive detail in the Guide. This includes the names and parent organisations of those involved in the method group for the National Safety and Security Steering Group, who compiled the Guide. This unusual degree of openness includes: identification of the organisations participating in the national risk assessment process, their roles, and the documents to which they are expected to refer in varying out their roles, and the extent to which and terms under which some kinds of information are withheld for reasons of cost, privacy, confidentiality and national security
Netherlands	The Ministry of Security and Justice has the co-ordinating responsibility for security and crisis management and thus for the NRA. The government works closely with the private sector, academia, scientific and public organisations, in a Network of Analysts for National Safety and Security. Detailed guidance sets out the arrangements for conducting NRA including the methodology, identification of those participating in the NRA process and their roles, and the extent to which some information is withheld for reasons of cost, privacy, confidentiality and national security. The process both feeds and is fed by risk assessment at the regional level. The concept of risk ownership operates at national level but also in the safety/security regions and in communities/cities. Safety/security regions are involved in the identification of risk at national level, and in the Network of Risk Analysts.
New Zealand	The DESC system provides a practical means of overseeing implementation based on the four main principles of national security. In particular, the principle of subsidiarity, and the need for active partnerships between multiple stakeholders at local level, is underpinned by a Co-ordinated Incident Management System (CIMS).
Norway	By Royal Decree, government ministries must assess the risk, vulnerabilities and robustness of critical social functions in their own sectors as a basis for continuity and emergency planning, based partly on a National Risk Analysis by the Directorate of Civil Protection (DSB) within the Ministry of Justice. DSB has consulted widely on risk assessment methodology, involving SMEs in risk identification, scenario building, and risk analysis. NRA methodology and outcome are distributed to ministries, agencies and local authorities to complement their own work on risk and vulnerability assessment, and to the public through the DSB website and in print. DSB offer briefings but these have so far largely been limited to public authorities
Poland	The Government Security Centre (GSC) collates risk assessments from responsible ministries in a National Report on Threats to National Security, which is linked to the development of a National Crisis Management Plan. The GSC involves all ministries, regional authorities as well as the main central offices in government, on the methodology to be used by responsible ministries, in training on the use of the methodology, and in editing the Report and on the terms of the submission to the Council of Ministers. There is no independent validation of the assessments, but GSC is in the process of consultation with a view to revising and updating the methodology by the end of 2015
Portugal	There is a National Commission for Civil Protection (CNPC) at national political level with representatives of all ministries which ensures a cross the government approach. It is established by law, and one of its tasks is to commission NRA work, as part of the NEP. The CNPC also acts as the National Platform for Disaster Risk Reduction (PNRRC). The PNRRC features a consultative sub-Commission, that includes the private sector (e.g., banks and insurers), universities and media, and can establish ad hoc groups to work over a limited period on specific subjects (for example flood resilience, resilience for schools and hospitals, building regulations, and recovery) and include specialist staff, such as medicals, architects, volunteers or civil engineers.

Slovak Republic	All departments with lead responsibilities designated (by Act 575/2001) are required (by Act 387/2002) to make available information about hazards or threats in their area of responsibility, to analyse these risks and take measures to mitigate them. Subsequent Acts prescribe the responsibilities of regional and local government, the emergency services, owners/operators of national infrastructure assets, and others to manage the risks in their areas. Similarly, the NSSRM sets out the lead responsibilities for all actions in the plan to overhaul the national crisis and risk management system.
Spain	The Prime Minister has the role of directing, leading and giving impetus to National Security Policy. In performing these functions the Prime Minister relies mainly on the National Security Council (NSC) whose members include the Deputy Prime Minister and Ministers for Defence, the Interior, Industry, Energy and Tourism, Foreign Affairs, Treasury/Public Administration, Development, the Economy/Competitiveness, the Chief of Defence Staff, State Secretaries and the Director of the Prime Minister's Office. In any event, the rest of the ministerial departments as well as other authorities, senior public officials, private-sector actors and experts may also be convened to attend when the Council needs to discuss issues related to their areas of responsibility or knowledge. Specialised Committees (set up by the NSC) support the Council in each of the 12 strategic areas of action in the 2013 NSS. National Crisis Management instruments were also set up under the 2015 Act including a National Situation Centre whose director has the responsibility for making recommendations on a National Risk Assessment if and when commissioned to do so.
Sweden	The Swedish Civil Contingencies Agency (MSB) is mandated by Cabinet to act as lead co-ordinator for the NRA, and published the first edition in 2012. MSB has: issued guidelines/regulation for risk and vulnerability analysis at sub-national level; convened expert workshops to analyse risk scenarios and resolve differences; followed up with interviews and desk research literature reviews to control for bias in the assessment; and subjected the summary report of the NRA to quality review prior to publication. The NRA process involves a wide range of stakeholders from different levels of government including 56 governmental agencies, 16 municipalities, 3 county councils and 14 other organisations.
Switzerland	The Federal Office for Civil Protection (FOCP) is the lead organisation for national risk assessment, collating information on the risks, developing risk scenarios and guidelines on methodology, and facilitating resolution of disputes. All organisations with responsibility for risk management are involved together with interested parties and experts from the public, private and academic sectors: over 190 participants of whim nearly two-thirds were public sector (in proportions roughly 2:1 Federal: Cantonal), one quarter private sector, including selected infrastructure service providers; and 10% academic sector. FOCP has introduced additional controls for bias by referring risk analysis for a second and independent option to the Paul Scherrer Institute. Risk Reports are sent to the Government for information but not agreement, and are available to Cantonal authorities to aid their own risk assessment work
United Kingdom	The Cabinet Office (Civil Contingencies Secretariat) is the lead organiser of work on national risk assessment, working through a Steering Group and working groups whose membership includes all lead government departments (ie those owning risks or generic impacts of emergencies) and a representative of the Government Chief Scientific Adviser whose role includes endorsing the methodology. Other experts are consulted as required.
United States	While the outcomes of the Strategic National Risk Assessment have been outlined extensively to all stakeholders who participated at federal, state and local level, it must be said that the document in its present form is classified. To this end, there are efforts ongoing to produce a 'releasable' or sanitised version. From the perspective of planners, the release of an unclassified and publicly available document is important.

ANNEX C

Methodological Features: Categories of Impact

COUNTRY	Main Criteria	Sub-criteria/indicators
Australia	1. People 2. Environment 3. Economy. 4. Public administration 5. Social setting 6. Infrastructure	• Physical health of people and the ability of the health system to manage • Ecosystem of the area including fauna and flora • Governing body as reported in the annual operating statement for the relevant jurisdiction, and industry sectors as defined by the Australian bureau of statistics • Governing body's ability to govern • Society and social fabric, including cultural heritage, and resilience of community • Infrastructure/lifelines/utilities and its ability to service the community
Austria	1. Human impacts 2. Economic damage 3. Environmental damage 4. Political/social concerns.	• 1. Deaths and injuries
Canada	1. People 2. Economy 3. Environment 4. Territorial Security 5. Canada's Reputation and Influence 6. Society and Psycho-Social	
Denmark	1. Harm to life, health & well-being 2. Harm to property & economy 3. Environmental harm 4. Impact on availability of critical societal functions	• dead • injured • ill/infected/contaminated • anxiety/insecurity/fear • material damage • financial losses • loss of intellectual property • loss/destruction of cultural heritage • land pollution • water pollution • harm to animals • harm to plant life • energy supply • ICT • Transport • Water • Food • Finance • Emergency service • Health/social services • Defence, intelligence, security services • Ability of government institutions to carry out their lawful functions
Estonia	1. Human health and life	• Fatalities • Numbers requiring immediate medical care • Extent to which number of injured exceeds regional care resources

	2. Asset damage	• Cost of damage to property • Harm to GDP
	3. Natural environment	• Change in the population of any species • Change in the ecosystem function • Need for human intervention to restore environment to original state
	4. Vital services	• Extent of disruption of vital service • Duration of disruption of vital service
Finland	1. Human impact	• Fatalities • Seriously injured • numbers evacuated
	2. Economic impact	• material damage • property damage • affected area (in kilometers^2) • duration of impact
	3. Environmental impact	• energy production & distribution • Information and communication technology systems • Financial services • Transport & logistics • Water supply
	4. Impact on critical infrastructure	• Building and maintenance of critical infrastructure • Waste management • Food supply • Health care system • industry • Production that supports military defence
	5. Impact on vital functions	• Government functions • International activity • Defence capability • Internal security • Functioning of the economy and infrastructure • Public income security and ability to function • Psychological resilience to crises
Germany	1. People	• Fatalities • Injured • People in need of public aid • Persons missing
	2. Environment	• Impairment of protected area • Impairment of water bodies • Impairment of forests • Impairment of agricultural land • Impairment of livestock
	3. Economy	• Impact on public administration • Impact on private economy • Impact on private households
	4. Non-material	• Impact on public order and safety • Political implications • Psychological implications • Damage to cultural assets
Hungary	1. Human	• Deaths • Injuries
	2. Nature/environment	• Long-term damage to nature & the environment

	3. Finance/economy 4. Stability of society 5. Ability to govern and control territory	• Material & financial losses • Social unrest • Disturbance to daily life • Weakened national ability to govern • Weakened control of territory
Korea	*Not applicable*	
The Netherlands	1. Territorial security 2. Physical security 3. Economic security 4. Ecological security 5. Social & political security	• Encroachment on Territory • Infringement of international position • Fatalities • Injuries • Physical suffering • Costs and impairment of the economy • Long-term impact on nature & the environment • Disruption of everyday life • Violation of the democratic system • Social psychological impact & social unrest
New Zealand	1. Physical 2. Social (including health) 3. Economic 4. Built/infrastructure environments	
Norway	1. Life & health 2. Nature & the environment 3. Economy 4. Societal stability 5. Capacity to govern & maintain territorial control	• Death • Injuries and illness • Long-term damage to nature & the environment • Financial & material losses • Social unrest • Impact on daily life • Weakened national capacity to govern • Weakened territorial control
Poland	1. Human impacts 2. Impacts on Economics, property & building infrastructure 3. Impacts on critical infrastructure	• Fatalities • Numbers hospitalised • Numbers evacuated • Impact on everyday life including indirect social effects (e.g., unemployment or permanent incapacity for work) and negative psychological effects • Damage to property and infrastructure • Direct & indirect costs to the economy • Energy • Information Technology & Communications • Financial systems • Food supply systems • Water supply systems • Health protection systems • Transport systems • Emergency services • Continuity of government • Facilities for production, storage, distribution & use of chemical & radioactive systems

	4. Environmental impacts	• Harm to fauna, flora, air, soil & water
Portugal	1. People (these are given a greater weight than other kinds of impact), 2. Disruption of material goods and services, 3. The environment	
Slovak Republic	Not applicable	
Spain	Not applicable	
Sweden	1. Functioning of society 2. Human life & health 3. Economic values & the environment 4. Democracy, rule of law & human rights & freedoms 5. National sovereignty	• Disruptions to everyday life • Fatalities • Severely injured/ill • Lack of fulfilment of basic needs • Numbers needing evacuation • Total economic impacts • Impacts on nature & the environment • Social unrest resulting in negative behavioural changes • Lack of confidence in public institutions • Serious impact on national political decisions • Lack of control over public institutions • Impact on Sweden's reputation internationally • Lack of control over territory
Switzerland	Population Environment Economy Society	• Fatalities • Injured/ill • People in need of support • Damaged ecosystem • Damage to property & assets • Reduction of economic productivity • Disruption of provision of vital goods and services • Constraints on enforcing law and order • Harm to reputation of governing institutions • Loss of territorial integrity Damage to cultural goods
United Kingdom	Human impact Economic impact Disruption of essential services, social services & the environment	• Deaths • Illness & injury • Net annualised economic cost including demand-side and supply-side consequences • Transport • Food/water • Fuel • Gas • Electricity • Cash/finance • Communications • Education • Health • Evacuation • Shelter • Environment

	Psychological	• Anxiety outrage
United States	*Not applicable*	

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

OECD PUBLISHING, 2, rue André-Pascal, 75775 PARIS CEDEX 16
(42 2017 54 1 P) ISBN 978-92-64-28752-5 – 2017

National Risk Assessments

A CROSS COUNTRY PERSPECTIVE

This report provides a synthetic view of national risk assessments (NRAs) in twenty OECD Member countries. NRA are used to support risk management decisions in a rapidly changing global risk landscape characterized by increasingly complex, interconnected societies and highly mobile people, information and goods. The report highlights good governance practices in establishing NRAs and how the results are used to inform public policy. It identifies challenges that OECD Member countries continue to confront in their efforts to implement NRA, and makes concrete recommendations where improvements could still be made.

Consult this publication on line at ***http://dx.doi.org/10.1787/9789264287532-en***.

This work is published on the OECD iLibrary, which gathers all OECD books, periodicals and statistical databases. Visit ***www.oecd-ilibrary.org*** for more information.

OECD*publishing*
www.oecd.org/publishing

THE LONDON BOOK FAIR WINNER
INTERNATIONAL EXCELLENCE Awards 2017
IN PARTNERSHIP WITH THE PUBLISHERS ASSOCIATION

ISBN 978-92-64-28752-5
42 2017 54 1 P

9 789264 287525

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

OECD PUBLISHING, 2, rue André-Pascal, 75775 PARIS CEDEX 16
(42 2017 54 1 P) ISBN 978-92-64-28752-5 – 2017

National Risk Assessments

A CROSS COUNTRY PERSPECTIVE

This report provides a synthetic view of national risk assessments (NRAs) in twenty OECD Member countries. NRA are used to support risk management decisions in a rapidly changing global risk landscape characterised by increasingly complex, interconnected societies and highly mobile people, information and goods. The report highlights good governance practices in establishing NRAs and how the results are used to inform public policy. It identifies challenges that OECD Member countries continue to confront in their efforts to implement NRA, and makes concrete recommendations where improvements could still be made.

Consult this publication on line at ***http://dx.doi.org/10.1787/9789264287532-en***.

This work is published on the OECD iLibrary, which gathers all OECD books, periodicals and statistical databases. Visit ***www.oecd-ilibrary.org*** for more information.

OECD*publishing*
www.oecd.org/publishing

THE LONDON BOOK FAIR WINNER
INTERNATIONAL EXCELLENCE Awards 2017
IN PARTNERSHIP WITH THE PUBLISHERS ASSOCIATION

ISBN 978-92-64-28752-5
42 2017 54 1 P

9 789264 287525