

## JRC SCIENCE FOR POLICY REPORT

# Recommendations for National Risk Assessment for Disaster Risk Management in EU

*Where Science and Policy  
Meet*

*Version 1*

Karmen Poljanšek, Ainara Casajus Valles, Montserrat Marín Ferrer, Tomás Artes-Vivancos, Roberto Boca, Costanza Bonadonna, Alfredo Branco, Wesley Campanharo, Alfred De Jager, Daniele de Rigo, Francesco Dottori, Tracy Durrant Houston, Christine Estreguil, Davide Ferrari, Corine Frischknecht, Luca Galbusera, Blanca García Puerta, Georgios Giannopoulos, Serkan Girgin, Richard Gowland, Rosana Grecchi, Miguel Angel Hernandez Ceballos, Giorgia Iurlaro, Georgios Kambourakis, Vasileios Karlos, Elisabeth Krausmann, Martin Larcher, Anne Sophie Lequarre, Giorgio Liberta, Susan C. Loughlin, Pieralberto Maianti, Domenico Mangione, Alexandra Marques, Scira Menoni, Milagros Montero Prieto, Gustavo Naumann, Amos Necci, Duarte Oom, Hans Pfeiffer, Marine Robuchon, Peter Salamon, Marco Sangiorgi, Jesús San-Miguel-Ayanz, Maria Luísa Sousa, Marianthi Theocharidou, Georgios Theodoridis, Cristina Trueba Alonso, Georgios Tsionis, Juergen V.Vogt, Maureen Wood

2021



This publication is a Science for Policy report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

#### Contact information

Name: Karmen Poljanšek

Address: European Commission, Joint Research Centre (JRC), JRC.E.1, Via E. Fermi, 2749, 21027 Ispra (VA), Italy

Email: [karmen.poljansek@ec.europa.eu](mailto:karmen.poljansek@ec.europa.eu)

Tel.: +39 0332 783650

#### EU Science Hub

<https://ec.europa.eu/jrc>

JRC123585

EUR 30596 EN

PDF	ISBN 978-92-76-30256-8	ISSN 1831-9424	doi:10.2760/80545
Print	ISBN 978-92-76-30257-5	ISSN 1018-5593	doi:10.2760/43449

Luxembourg: Publications Office of the European Union, 2021

© European Union, 2021



The reuse policy of the European Commission is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Except otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated. For any use or reproduction of photos or other material that is not owned by the EU, permission must be sought directly from the copyright holders.

All content © European Union, 2021, unless otherwise specified

How to cite this report: Poljansek, K., Casajus Valles, A., Marin Ferrer, M., Artes Vivancos, T., Boca, R., Bonadonna, C., Branco, A., Campanharo, W., De Jager, A., De Rigo, D., Dottori, F., Durrant Houston, T., Estreguil, C., Ferrari, D., Frischknecht, C., Galbusera, L., Garcia Puerta, B., Giannopoulos, G., Girgin, S., Gowland, R., Grecchi, R., Hernandez Ceballos, M.A., Iurlaro, G., Kambourakis, G., Karlos, V., Krausmann, E., Larcher, M., Lequarre, A.S., Liberta`, G., Loughlin, S.C., Maianti, P., Mangione, D., Marques, A., Menoni, S., Montero Prieto, M., Naumann, G., Jacome Felix Oom, D., Pfeiffer, H., Robuchon, M., Necci, A., Salamon, P., San-Miguel-Ayanz, J., Sangiorgi, M., Raposo De M. Do N. E. S. De Sotto Mayor, M.L., Theocharidou, M., Trueba Alonso, C., Theodoridis, G., Tsionis, G., Vogt, J. and Wood, M., Recommendations for National Risk Assessment for Disaster Risk Management in EU: Where Science and Policy Meet, Version 1, EUR 30596 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-30256-8, doi:10.2760/80545, JRC123585.

**Contents**

Contents ..... i

Abstract ..... 8

Acknowledgement ..... 9

Executive summary ..... 13

1 Introduction..... 16

    1.1 From Version 0 to Version 1..... 18

        1.1.1 The purpose, content and outcome of Version 0 ..... 18

        1.1.2 The purpose and objectives of Version 1..... 19

    1.2 The structure of the Report..... 19

2 Towards a better understanding of disaster risks in the EU: an evolution of reporting process ..... 21

    2.1 The beginnings of an overall European approach to the prevention of disasters ..... 21

    2.2 First steps of the reporting process and lessons learned ..... 22

    2.3 Reporting process today..... 24

3 National Risk Assessment..... 27

    3.1 The purpose and objectives of national risk assessment process..... 27

    3.2 Governance of National Risk Assessment Process ..... 27

    3.3 ISO 31010 format of National Risk Assessment Process ..... 28

        3.3.1 Context of National Risk Assessment ..... 29

        3.3.2 Risk Identification ..... 30

            3.3.2.1 Scenario Building ..... 32

        3.3.3 Risk Analysis..... 32

        3.3.4 Risk Evaluation..... 34

        3.3.5 Risk Treatments ..... 35

    3.4 Key Messages ..... 36

4 Risk Management Capability Assessment ..... 37

    4.1 The purpose and objectives of Risk Management Capability Assessment ..... 37

    4.2 A link between capability assessment and capability development ..... 38

    4.3 Implementation of integrated DRM..... 39

        4.3.1 Knowing the process ..... 39

        4.3.2 Identifying the capabilities..... 43

    4.4 Risk Management Assessment methodology ..... 44

    4.5 Key messages..... 47

5 Linking the NRA and RMCA ..... 49

6 Climate Change and Disaster Risk Management ..... 52

    6.1 EU Strategy on adaptation to climate change ..... 52

    6.2 Synergies among the two processes; CCA and DRR strategies..... 54

7 Introduction to contributions ..... 58

8	Main findings from contributions and conclusions.....	61
8.1	Main findings from contributions.....	61
8.2	Overall conclusion.....	62
9	References.....	65
10	Floods.....	70
10.1	Context .....	70
10.1.1	Legal framework of flood risk assessment in the European Union .....	70
10.2	Risk identification .....	71
10.2.1	Hazard .....	72
10.2.2	Exposure.....	74
10.2.3	Vulnerability .....	75
10.2.4	Coping capacity.....	76
10.3	Risk analysis.....	76
10.4	Risk evaluation.....	77
10.5	Gaps and challenges .....	78
10.6	References.....	79
11	Droughts .....	81
11.1	Context of drought risk assessment.....	81
11.2	Risk Identification .....	81
11.3	Drought risk analysis and characterization .....	82
11.3.1	Hazard characterization .....	83
11.3.2	Exposure identification.....	83
11.3.3	Vulnerability identification .....	83
11.4	Risk identification in the context of climate change .....	85
11.5	Risk Treatment.....	86
11.5.1	Organizational issues .....	87
11.5.2	Short Term Actions, during and immediately after the emergency.....	87
11.5.3	Long-term actions, National Strategy.....	88
11.5.4	Quantification of the actions.....	88
11.6	Gaps and challenges .....	90
11.7	References.....	91
12	Wildfires.....	93
12.1	Context of Risk Assessment. Introduction.....	93
12.2	Risk identification .....	93
12.2.1	Wildfire Danger.....	94
12.2.2	Wildfire ignitions .....	95
12.2.3	Fire behavior .....	95
12.2.4	Fuel moisture .....	95
12.2.5	Fuel Types .....	97



12.2.6	Slope .....	98
12.2.7	Vulnerability .....	99
12.2.8	People.....	99
12.2.9	Ecological value .....	100
12.2.10	Socioeconomic value .....	101
12.3	Risk analysis.....	102
12.4	Wildfire risk and climate change .....	102
12.5	Gaps and challenges/Conclusions .....	103
12.6	References.....	103
13	Biodiversity loss .....	106
13.1	Context of Risk Assessment/Introduction.....	106
13.2	Risk identification .....	108
13.2.1	Past trends in biodiversity and NCPs .....	108
13.2.2	Risk drivers, exposure and capacities .....	111
13.3	Risk analysis.....	113
13.4	Risk Evaluation.....	116
13.5	Risk treatment .....	116
13.5.1	Policy responses to biodiversity loss .....	116
13.5.2	Socio-economic responses to biodiversity loss .....	117
13.6	Gaps and Challenges/Conclusion .....	117
13.7	References.....	118
14	Earthquakes .....	120
14.1	Context of National Risk Assessment .....	120
14.2	Risk identification .....	120
14.2.1	Potential impact of earthquakes and its cause .....	120
14.2.2	Seismic hazard .....	121
14.2.3	Exposure and vulnerability.....	123
14.2.4	Scenario-building process.....	124
14.3	Risk analysis.....	124
14.3.1	Damage assessment.....	124
14.3.2	Damage-to-loss models.....	125
14.3.3	Estimation of casualties.....	125
14.3.4	Estimation of shelter needs .....	125
14.3.5	Probabilistic seismic risk analysis .....	125
14.3.6	Tools for seismic risk analysis .....	125
14.3.7	Recent research .....	126
14.3.8	Examples of seismic risk assessment studies .....	127
14.4	Risk evaluation.....	128
14.5	Risk treatment .....	129

14.6 Gaps and challenges .....	130
14.7 References.....	131
15 Volcano eruptions.....	135
15.1 Context of Risk Assessment .....	135
15.2 Risk identification .....	136
15.2.1 Volcanic hazards .....	136
15.2.2 Vulnerability aspects .....	137
15.3 Risk analysis.....	138
15.4 Risk evaluation.....	140
15.5 Risk treatment .....	141
15.6 Gaps and challenges/conclusions .....	142
15.7 Acknowledgements .....	143
15.8 References.....	143
16 Biological disasters .....	149
16.1 Introduction.....	149
16.2 Human epidemics .....	149
16.2.1 Risk identification and the policy context .....	149
16.2.1.1 International Public Health policies .....	149
16.2.1.2 EU policies controlling human communicable diseases.....	150
16.2.2 Risk analysis and risk evaluation.....	150
16.2.3 Risk Assessment methodology for human diseases.....	151
16.2.4 Risk Treatment.....	154
16.3 Animal diseases .....	155
16.3.1 Risk identification and the policy context .....	155
16.3.1.1 International Animal Health policies .....	155
16.3.1.2 EU policies controlling animal diseases.....	156
16.3.2 Risk analysis and risk evaluation.....	156
16.3.3 Risk treatment .....	157
16.4 High-security level biological laboratories .....	158
16.4.1 Risk identification and the policy context .....	158
16.4.1.1 International conventions and agreements on biosecurity.....	158
16.4.1.2 EU policies on biosafety and biosecurity .....	158
16.4.2 Risk analysis and risk evaluation.....	158
16.5 References.....	159
17 Natch accidents.....	161
17.1 Risk Assessment Context.....	161
17.2 Risk Identification .....	163
17.3 Risk analysis.....	164
17.4 Risk evaluation.....	167

17.5 Good Practices .....	168
17.6 Gaps and Challenges .....	169
17.7 References .....	169
18 Chemical Accidents .....	172
18.1 Overview .....	172
18.2 Prevention and mitigation of chemical releases.....	172
18.3 Principles of effective risk assessment and management.....	174
18.4 Performing a risk assessment .....	174
18.5 Selecting accident scenarios for the risk assessment.....	175
18.5.1 Hazard identification (what can go wrong) .....	176
18.5.2 Selecting the accident scenarios (How likely is it that it will happen and if it does happen, what are the consequences?) .....	176
18.6 Evaluating the consequence analysis .....	178
18.6.1 Evaluating impacts and severity .....	178
18.6.2 Human health effect evaluation.....	179
18.6.3 Consequence and risk assessment modelling tools .....	181
18.7 Presenting the risk assessment outcome for decision-making .....	181
18.8 Making decisions based on the risk assessment .....	183
18.9 References .....	184
19 Nuclear accidents .....	185
19.1 Context .....	185
19.2 Risk identification .....	185
19.3 Risk Analysis.....	186
19.4 Risk Evaluation.....	188
19.5 Risk Treatment.....	189
19.6 Gaps and challenges .....	192
19.7 References .....	193
20 Terrorist attacks.....	196
20.1 Introduction.....	196
20.2 Lessons learned from prior terrorist attacks .....	197
20.3 Risk assessment.....	199
20.3.1 Threat identification.....	200
20.3.1.1 Threat identification on national level.....	200
20.3.1.2 Threat identification on local level .....	202
20.3.2 Risk analysis.....	202
20.3.2.1 Exposed asset identification.....	202
20.3.2.2 Vulnerability identification .....	203
20.3.2.3 Likelihood and consequences assessment.....	204
20.3.3 Risk evaluation.....	206

20.4 Key messages and challenges .....	207
20.5 References .....	208
21 Critical infrastructure disruptions .....	209
21.1 Introduction.....	209
21.2 Policy background.....	210
21.3 Risk assessment.....	213
21.3.1 Defining the scope.....	213
21.3.2 Risk Identification .....	214
21.3.3 Risk Analysis.....	214
21.3.4 Risk evaluation.....	216
Figure 57: .....	217
21.4 Frameworks, methodologies and tools .....	217
21.4.1 Frameworks .....	218
21.4.2 Methodologies .....	222
21.4.3 Tools .....	223
21.5 Risk treatment .....	227
21.6 Gaps and Challenges .....	228
22 Cybersecurity threats .....	230
22.1 Introduction.....	230
22.2 Context establishment .....	232
22.3 Risk identification .....	233
22.4 Risk Analysis.....	240
22.5 Risk evaluation.....	241
22.6 Risk treatment .....	242
22.7 Key thoughts and Challenges .....	244
22.8 EU and International cybersecurity and cyber risk policy landscape .....	248
22.8.1 EU landscape.....	249
22.8.2 International landscape.....	250
22.8.3 Others.....	252
22.9 References.....	252
23 Hybrid Threats .....	260
23.1 Introduction.....	260
23.2 The political landscape and the respective conceptual model .....	261
23.3 Examples of hybrid activity .....	262
23.4 Assessing vulnerabilities: what to look for?.....	263
23.5 Changing paradigm of risk management: vulnerabilities self-assessment methodology .....	264
23.6 Beyond vulnerabilities assessment: fostering resilience.....	266
23.7 Future Challenges in the domain of hybrid threats .....	267
23.8 References.....	267

List of boxes ..... 269  
List of figures ..... 270  
List of tables..... 273

## Abstract

**Union Civil Protection Mechanism Decision No 1313/2013/EU** requires EU Member States and UCPM participating states to report to the Commission on their disaster risk management activities to support formulating an EU risk management policy that would complement and enhance the national ones. The aim of this report is to support the use of the new “**Reporting Guidelines on Disaster Risk Management**, Art. 6(1)d of Decision No.1313/2013/EU,” (2019/C 428/07) by relevant national **authorities**.

This report is the second in the series of reports “Recommendations for National Risk Assessment for Disaster Risk Management”. The aim of this series of reports is to build-up a network of experts involved in the different aspects of the national risk assessment process.

The European Commission Joint Research Centre joins national, regional and global efforts to acquire better risk governance structure through evidences, science and knowledge management. Risk governance facilitates policy cycle for the implementation of integrated disaster risk management. Risk Assessment is positioned at the heart of the policy cycle and provides evidence for DRM planning and the implementation of prevention and preparedness measures.

This report explains the purpose and objective of each step of the reporting to give meaning and motivation to demanding risk governance processes. It collects the contributions of **fourteen expert teams** that prepared short step by step description of disaster risk assessment approaches specific for the chosen hazard/asset usable in the context of a national risk assessment exercise and addressed national risk assessment capability to be further developed in order to bring the evidence to next level. A special focus is dedicated to capability needed to tackle climate change. The risks covered are of natural, anthropogenic and socio-natural origin: floods, droughts, wildfires, biodiversity loss, earthquakes, volcano eruptions, biological disasters, Natech accidents, chemical accidents, nuclear accidents, terrorist attacks, critical infrastructure disruptions, cybersecurity and hybrid threats.

## **Acknowledgement**

### **Editors**

**Karmen Poljansek** – European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Ainara Casajus Valles** – European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Montserrat Marin Ferrer** – European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

### **Authors of Chapters 1-9**

**Karmen Poljansek** – European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Ainara Casajus Valles** – European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Montserrat Marin Ferrer** – European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

### **Authors of Chapters 10-23**

Chapter 10: FLOODS

**Francesco Dottori**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Peter Salamon**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

Chapter 11: DROUGHTS

**Alfred De Jager**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Gustavo Naumann**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Juergen V. Vogt**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

Chapter 12: WILDFIRES

**Duarte Oom**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Daniele de Rigo**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Jesús San-Miguel-Ayanz**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Tomás Artes-Vivancos**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Roberto Boca**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Alfredo Branco**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Wesley Campanharo**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Rosana Grecchi**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Tracy Durrant Houston**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Davide Ferrari**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Giorgio Liberta**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Pieralberto Maianti**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Hans Pfiesser**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

#### Chapter 13: BIODIVERSITY LOSS

**Marine Robuchon**, European Commission, JRC.D.6 Knowledge for Sustainable Development and Food Security, Ispra, IT

**Christine Estreguil**, European Commission, JRC.D.6 Knowledge for Sustainable Development and Food Security, Ispra, IT

**Alexandra Marques**, European Commission, JRC.D.3 Land Resources Unit, Ispra, IT

#### Chapter 14: EARTHQUAKES

**Maria Luísa Sousa**, European Commission, JRC.E.4 Safety and Security of Buildings, Ispra, IT

**Georgios Tsionis**, European Commission, JRC.E.4 Safety and Security of Buildings, Ispra, IT

#### Chapter 15: VOLCANO ERUPTIONS

**Costanza Bonadonna**, Department of Earth Sciences, University of Geneva, CH,

**Corine Frischknecht** Department of Earth Sciences, University of Geneva, CH,

**Susan C. Loughlin**, British Geological Survey, UK,

**Domenico Mangione**, National Civil Protection Department, IT

**Scira Menoni**, Department of Architecture, Built Environment and Construction Engineering, Politecnico di Milano, IT

#### Chapter 16: BIOLOGICAL DISASTERS

**Anne Sophie Lequarre**, European Commission, JRC.E.7 Knowledge for Security and Migration, Brussels, BE

#### Chapter 17: NATECH ACCIDENTS

**Serkan Girgin**, European Commission, JRC.E.2 Technology Innovation in Security Unit, Ispra, IT

**Amos Necci**, European Commission, JRC.E.2 Technology Innovation in Security Unit, Ispra, IT

**Elisabeth Krausmann**, European Commission, JRC.E.2 Technology Innovation in Security Unit, Ispra, IT

#### Chapter 18: CHEMICAL ACCIDENTS

**Maureen Wood**, European Commission, JRC.E.2 Technology Innovation in Security Unit, Ispra, IT

**Richard Gowland**, an independent consultant and expert in process safety, Peterborough, UK

#### Chapter 19: NUCLEAR ACCIDENTS

**Miguel Angel Hernandez Ceballos**, European Commission, JRC.G.10 Knowledge for Nuclear Security and Safety Unit, Ispra, IT

**Cristina Trueba Alonso**, Research Centre for Energy, Environment and Technology (CIEMAT), Department of Environment, Radiation Protection of Public and Environment Unit, Madrid, ES

**Milagros Montero Prieto**, Research Centre for Energy, Environment and Technology (CIEMAT), Department of Environment, Radiation Protection of Public and Environment Unit, Madrid, ES

**Giorgia Iurlaro**, Italian National Agency for New Technologies, Energy and Sustainable Economic Development (ENEA), Radiation Protection Institute, Ispra, IT

**Marco Sangiorgi**, European Commission, JRC.G.10 Knowledge for Nuclear Security and Safety Unit, Ispra, IT



**Blanca García Puerta**, Research Centre for Energy, Environment and Technology (CIEMAT), Department of Environment, Radiation Protection of Public and Environment Unit, Madrid, ES

Chapter 20: TERRORIST ATTACKS

**Martin Larcher**, European Commission, JRC.E.4 Safety and Security of Buildings, Ispra, IT

**Vasileios Karlos**, European Commission, JRC.E.4 Safety and Security of Buildings, Ispra, IT

Chapter 21: CRITICAL INFRASTRUCTURE DISRUPTIONS

**Marianthi Theocharidou**, European Union Agency for Cybersecurity (ENISA), Network and Information Security, Athens, GR

**Luca Galbusera**, European Commission, JRC.E.2 Technology Innovation in Security Unit, Ispra, IT

**Georgios Giannopoulos**, European Commission, JRC.E.2 Technology Innovation in Security Unit, Ispra, IT

Chapter 22: CYBERSECURITY THREATS

**Georgios Kambourakis**, European Commission, JRC.E.3, Cyber and Digital Citizens' Security Unit, Ispra, IT

Chapter 23: HYBRID THREATS

**Georgios Giannopoulos**, European Commission, JRC.E.2 Technology Innovation in Security Unit, Ispra, IT

**Georgios Theodoridis**, European Commission, JRC.E.2 Technology Innovation in Security Unit, Ispra, IT

**Marianthi Theocharidou**, European Union Agency for Cybersecurity (ENISA), Network and Information Security, Athens, GR

**Luca Galbusera**, European Commission, JRC.E.2 Technology Innovation in Security Unit, Ispra, IT

**Reviewers of Version 0 of the “Recommendations for National Risk Assessment for Disaster Risk Management in EU: Approaches for Identifying, Analysing and Evaluating Risks (Poljanšek et. al, 2019)**

**Elisa Vargas Amelin**, European Commission, ENV.C.1 Clean Water, Brussels, BE

**Helen Crowley**, EUCENTRE, Pavia, IT

**Silvia Dimova**, European Commission, JRC.E.4 Safety and Security of Buildings, Ispra, IT

**Luc Feyen**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Morten Lomholt Korslund**, Danish Emergency Management Agency, Crisis Management Division, Birkerød, DK

**Leanne Roche**, European Commission, ENV.C.1 Clean Water, Brussels, BE

**Fabio Taucer**, JRC.A.5 Scientific Development, Brussels, BE

**Reviewers of Version 1 of the “Recommendations for National Risk Assessment for Disaster Risk Management in EU: Where Science and Policy Meet**

**Christofer Ahlgren**, European Commission, CLIMA.A.3 Adaptation to Climate Change, Brussels, BE

**Paulo Barbosa**, European Commission, JRC.E.1 Disaster Risk Management Unit, Ispra, IT

**Christina Brailescu**, European Commission, ENV.D.1 Land Use & Management, Brussels, BE

**Laura Indriliunaite**, European Commission, ECHO.B.2 Prevention and Disaster Risk Management, Brussels, BE

**Ioannis Kavvadas**, European Commission, ENV.C.1 Clean Water, Brussels, BE

## Executive summary

The European Commission Joint Research Centre joins National, Regional and Global efforts **to acquire better risk governance levels through evidences, science and knowledge management**. This report is the second in the series of reports "*Recommendations for National Risk Assessment for Disaster Risk Management*". The aim of this series of reports is to build-up a network of experts involved in the different aspects of the national risk assessment process. They are invited to co-develop, with a sequential approach imposed by the complexity of the task, a reference document that will contribute to filling the gap between scientific knowledge and their practical usability.

Version 0 of this series was focused mainly on how to do National Risk Assessment from the scientific perspective to provide enough evidences to Risk Managers for better understanding and, hence, managing risk. In Version 1, the national risk assessment is positioned at the heart of the policy cycle for the implementation of integrated disaster risk management. This perspective highlights the imperative need for policy-makers, practitioners and scientists to work hand-in-hand towards a more resilient, and hence sustainable, future.

## Policy context

Member States are, since 2013 (**UCPM Decision No 1313/2013/EU**), required to report to the Commission on their disaster risk management activities to support formulating an EU risk management policy that would complement and enhance the national ones.

The amendment of the Union Civil Protection Mechanism (UCPM) of March 2019 (Decision (EU) 2019/420) introduced new requirements for reporting under Article 6, combining elements of (1) **national risk assessment (NRA)**, (2) **risk management capability assessment (RMCA)** and (3) **information on the priority prevention and preparedness measures** with a focus on (a) key risks with cross-border impacts, and, where appropriate, (b) low probability risks with a high impact.

The purpose of the Version 1 of the *Recommendations for NRA for Disaster Risk Management*, prepared by 50 scientists, is to support the use of the new "**Reporting Guidelines on Disaster Risk Management**, Art. 6(1) of Decision No.1313/2013/EU2019/C 428/07" by relevant authorities of the Participating States to the EUCPM.

The final scope of this collective effort is to **contribute to establishing an appropriate risk governance** that is flexible and adaptable to new evidences, knowledge and situations. A risk governance that facilitates risk assessment processes as proper evidence to drive disaster risk management planning and the implementation of **adequate measures all along the risk management cycle**, from adaptation and mitigation to response and recovery phases.

## Key conclusions

**Better national risk governance with a legal framework and integrated disaster risk management approach is a must.** The implementation of integrated DRM is seen as evidence-based policy cycle compound of NRA, DRM planning and the implementation of prevention and preparedness measures.

- **NRA produces the evidence to reach a common understanding** and the relative importance of the risks due to the different drivers faced in a country **and** presents a core of evidence-based policy-making which adds to successful implementation of effective and efficient integrated disaster risk management.
- **Risk management capability assessment** strives to set up an efficient, flexible and systematic risk governance structure covering the whole policy cycle that places NRA as an essential part of disaster risk reduction strategy and facilitates from the beginning to the end the implementation of the measures in different phases of disaster risk management for different hazard.

**Reporting outcomes** to be submitted to the European Commission are **a summary of the national activities related to NRA and RMCA** that are also relevant to the EU context. NRA and RMCA processes must be comprehensive and tailored to the national context to serve the specific national goals. Furthermore, their overall aim is very much the same, i.e., **to support the identification and definition of disaster risk reduction strategies**, which will result in less disasters and/or disasters with less impacts and increase of overall EU resilience.

It can be considered that these processes are national enablers of (a) the development of **a common understanding** on risk, its drivers, interlinks and options for reducing it while (b) they promote and facilitate the exchange of **good practices and lessons learned** to speed up the risk reduction processes. By submitting the summaries to the Commission and, thanks to the “*Overview of Natural and Man-Made Disaster Risks that the EU May Face*” series of publications prepared by Commission, the fulfilment of these two objectives is eased **at the European level**.

**Regular RMCA is a driver** of sustainable development of capabilities for the implementation of the integrated DRM and also an opportunity to continuously adapt to changing risk landscape (i.e., climate change as well as new and emergent risks) as well as development strategies with relevant capabilities.

The policy cycle for the implementation of integrated disaster risk management should have capacity to **integrate climate change adaptation strategies** and efficiently consider adaptation measures during DRM planning.

The policy cycle for the implementation of integrated disaster risk management is a mechanism that fill the gaps revealed in NRA process with the DRM actions in place. Therefore it is important to **prioritize the development of national risk assessment capability to improve the country's resilience** against the disaster risk.

## Main findings

The report evidences that the implementation of integrated disaster risk management is a challenging process in terms of expertise and data, resources, time and diversity of stakeholders involved. It requires a support of national authorities at all levels.

The report highlights the importance of the **evidences produced by NRA** to facilitate DRM planning and implementation of adequate measure that results in efficient integrated DRM. Based on the results of NRA national authorities (1) decide which risks can sufficiently harm well-being and security of citizens in a short or long term to be put on agenda of DRM planning, (2) understand which disaster risk drivers to be addressed to identify adequate measure to reduce risk all along the RM cycle.

The scientific approaches in NRA can be of tremendous support in this challenging task. Risk landscape is not only dynamic, but it is also expanding with increasing awareness and better understanding of different risks. Risk identification is partially based on evidence and partially on our perception regarding what we should be afraid of.

Furthermore, **different risks of different origins require very different methods** of risk assessment, not only due to diversity of phenomena, but also due to different availability of data and knowledge. Realistically, harmonisation of the risk assessment process shall remain at the level of terminology, data, risk concept, standardized steps of risk assessment process and presentation of the results. The main goal is to understand the risk and drivers behind as well as to assess the risk in terms of the level and probability in a way **to make risks comparable**.

Finally, **EU policies related to different risks are essential for fostering comparability** in approaches to risk assessment and data collection to achieve a more comprehensive picture of risks across Europe as well as for encouraging knowledge sharing and other NRA capabilities building. DRM policies are working on the exploitation of synergies across the whole DRM cycle for the implementation of an integrated risk governance.

## Related and future JRC work

This version of the “Recommendations” is part of a series of reports that collects the scientific contributions from the wider JRC scientific disaster risk community and beyond. It is a key activity of the **EC Disaster Risk Management Centre (DRMCC)**, which supports international, national and local authorities involved in DRM processes.

EC DRMCC has been recognized as a potential nucleus of scientific pillar of Union Civil Protection Knowledge Network<sup>1</sup>. The EC DRMCC proposes **opportunities for co-developing collective scientific knowledge** through a number of activities, such as a platform for news, publications, calendar of events and tools

---

<sup>1</sup>UCPM Decision No 1313/2013/EU acknowledges the pivotal role of scientific knowledge in Article 3(e), which calls for an increase in “the availability and use of scientific knowledge on disasters”, and in Article 13 for establishing the Union Civil Protection Knowledge Network

(DRMKC website<sup>2</sup>), the database of DRM related research projects and results (Projects Explorer<sup>3</sup> and Gaps Explorer<sup>4</sup>), the periodic publication of Science reports (Science for DRM<sup>5</sup>), the holistic repository of disaster risk and impacts data (Risk Data Hub<sup>6</sup>), the hub for the global assessment of the risk of having humanitarian crisis and the assessment of crisis severity (INFORM suite<sup>7</sup>) and the early warnings systems for Public health related issues (EIOS<sup>8</sup>) and conflicts (CAAS-CEWS), both based on Artificial Intelligence tools and on building-up communities of practice.

## Quick guide

The report explains the purpose and objective of each step of the reporting to give meaning and motivation to demanding risk governance processes. It collects also the contributions of **fourteen expert teams that** prepared short step by step description of disaster risk assessment approaches specific for the chosen hazard/asset usable in the context of a national risk assessment exercise and addressed national risk assessment capability to be further developed.

A special focus is dedicated to capability needed to **tackle climate change** with presenting possibilities how to ensure closer synergies between the disaster risk reduction and climate change adaptation agendas.

The risks covered in this document are of natural, anthropogenic and socio-natural origin: floods, droughts, wildfires, biodiversity loss, earthquakes, volcano eruptions, biological disasters, Natech accidents, chemical accidents, nuclear accidents, terrorist attacks, critical infrastructure disruptions, cybersecurity and hybrid threats.

---

<sup>2</sup> <https://drmkc.jrc.ec.europa.eu/>

<sup>3</sup> <https://drmkc.jrc.ec.europa.eu/Knowledge/Project-Explorer>

<sup>4</sup> <https://drmkc.jrc.ec.europa.eu/Knowledge/Gaps-Explorer>

<sup>5</sup> <https://drmkc.jrc.ec.europa.eu/knowledge/Challenges-Sharing>

<sup>6</sup> <https://drmkc.jrc.ec.europa.eu/risk-data-hub/>

<sup>7</sup> <https://drmkc.jrc.ec.europa.eu/inform-index>

<sup>8</sup> <https://drmkc.jrc.ec.europa.eu/Innovation/Epidemic-Intelligence-from-Open-Sources-EIOS#documents/1033/list>

# 1 Introduction

This report is a follow up of Version 0 of the “Recommendations for National Risk Assessment for Disaster Risk Management in EU: Approaches for identifying, analysing and evaluating risks (Poljansek et al, 2019) published in May 2019. This previous version was produced in collaboration with more than 20 scientists and was then open for public consultation until the end of October 2019. **Version 1 considers the comments received from experts and potential users. It also includes new chapters of scientific guidance on risks not yet addressed in Version 0.** The aim of this series of reports is to gradually invite other expert groups involved in the national risk assessment (NRA) exercise into the process to co-develop a document that will better fit users' needs.

**During the preparation of Version 1, two events have happened that have strongly increased the importance of how Europe can prevent and prepare for emergencies<sup>9</sup>.**

Firstly, Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a **Union Civil Protection Mechanism (UCPM) was amended** by [Decision No 2019/420/EU](#) of 13 March 2019. This amendment has introduced new requirements for reporting of Member States to the Commission on disaster risk management activities under Article 6. Member States are now required to provide: (1) summaries of the relevant elements of their risk assessment, focusing on key risks (2) summaries of the assessment of their risk management capability, focusing on key risks, and (3) information on the priority prevention and preparedness measures needed to address key risks with cross-border impacts, and, where appropriate, low probability risks with a high impact. To facilitate the reporting, “Reporting Guidelines on Disaster Risk Management, Art. 6(1)d of Decision No.1313/2013/EU” (2019/C 428/07) ([Commission Notice, 2019](#)) have been adopted and officially published on 20 December 2019.

Secondly, year 2020 will be always known by the coronavirus **COVID-19 pandemic** health crisis, one of the greatest challenges the world is facing since World War II. Since its first awareness<sup>10</sup> in China late 2019, the virus has spread in a matter of weeks to other continents and quickly overwhelmed the health systems in Europe and North America first and then all around the world. We have seen how vulnerable our health care systems are. By the end of March 2020 more than a third of the planet's population have been ordered to remain at home as governments have been forced to take extreme measures to release the pressure on the country's health systems and protect their populations. The US, France, Italy, Spain and the UK, among others, had all experienced shortages of doctors, hospital beds, ventilators, personal protective equipment and testing capacity. As of end of May 2020, in Europe the reports of new cases declined and deaths slowed, many Member States were easing the restriction. However, the big picture has remained questionable, there have been more and more confirmed cases and deaths worldwide. In September 2020 Europe has been caught in the grip of the second wave and another round of lockdowns.

All attention has been focused on science. We have witnessed a flood of prediction models, more or less complicated, to understand how bad these would really get, as well as volume of data about the spread of the virus being collected. However, different countries have been collecting data in a different way. It was obvious that without harmonized data collection and reporting process around the globe on such global issues, uncertainty introduced in the models was uncontrollable. Everybody has been striving to make the models less wrong and useful in the moment to support timely decisions on extreme measures. Eventually, it seems that only a vaccine can end the Covid-19 pandemic. In January 2021 the transmission of SARS-CoV-2 virus in Europe is still widespread and at the same time EU countries are facing the challenge of the appearance of SARS-CoV-2 variants of concern. European Commission set out actions accelerate the rollout of vaccination campaigns across the EU (COM/2021/35) and by the end of January at least 22 countries (ECDC, 2021) reported having started administering the COVID-19 Vaccine<sup>11</sup>.

The Commission had published the **Country Health Profiles**<sup>12</sup> in October 2019, which already contained some important signals regarding the status of vulnerability of our Health systems in particular considering current and future **demographic changes**<sup>13</sup>. The **EU4Health 2021-2027** program<sup>14</sup> is EU's response to

<sup>9</sup> This includes supporting Member States in developing national and local disaster risk strategies, if not already in place, and improving access to early warning systems. (from [https://ec.europa.eu/commission/commissioners/sites/comm-cwt2019/files/commissioner\\_mission\\_letters/mission-letter-janez-lenarcic\\_en.pdf](https://ec.europa.eu/commission/commissioners/sites/comm-cwt2019/files/commissioner_mission_letters/mission-letter-janez-lenarcic_en.pdf))

<sup>10</sup> The discussion of the origin of the virus and since when the virus has been among the population is still on going.

<sup>11</sup> The first vaccine administered has been developed by Moderna. Additional brands (e.g., BioNTech-Pfizer, AstraZeneca) will be introduced as soon as authorised for use.

<sup>12</sup> [https://ec.europa.eu/health/state/country\\_profiles\\_en](https://ec.europa.eu/health/state/country_profiles_en)

<sup>13</sup> [https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/impact-demographic-change-europe\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/impact-demographic-change-europe_en)

<sup>14</sup> [https://ec.europa.eu/health/funding/eu4health\\_en](https://ec.europa.eu/health/funding/eu4health_en)

COVID-19, which has had a major impact on medical and healthcare staff, patients and health systems in Europe. By investing €5.1 billion<sup>15</sup>, therefore becoming the largest health programme ever in monetary terms, EU4Health will provide funding to EU countries, health organizations and NGOs. Furthermore, UCPM has expanded rescEU capacities to include a strategic stockpile of medical equipment and the Emergency Support Instrument<sup>16</sup> will help Member States in their efforts to mitigate the immediate consequences of the pandemic and anticipate the needs related to the exit and recovery. However, the grip of pandemic has emerged many programmes and initiatives at EU level to support Member States based on the principle of solidarity and pools efforts and resources to quickly address shared strategic needs.

COVID-19 pandemic has shown the compound effect of the negative side of globalization as well as systemic nature of risk. The consequences of globalization are more complex than we have ever imagined. In terms of the basic flows, it embodies increasing interaction among countries. It is about sharing ideas, technologies, skills, goods and services, finance with other countries which defines the beneficial part of globalization and has shown a positive impact on development and thus on reducing poverty. However, globalization is an opportunity not only for spreading good things, but also spreading the bad ones. There are also other examples such as the financial crisis in 2008, cyber security issues and the consequences of rapid growth like climate change. In order to let the good things spread globally and to keep the bad things local, the risk of globalization will have to be properly managed.

Globalization brings risks, and these have become increasingly systemic. Systemic risk can be realized as a compound of failure of infrastructure, financial crisis, food insecurity or species extinction (GAR, 2019) as a cascade across interconnected socioeconomic and environmental systems. For example, the COVID-19 pandemic has affected multiple geographies and sectors at the same time, creating multiple “epicenters” of shocks.

COVID-19, as well as already existing climate and ecological crises, have revealed that human society is increasingly struggling to understand the relation of the humans with the environment and to manage the generated or existing risks. Even if science and policies are making good progress into the right direction, the parallel growth of complexity seems to be still one step ahead of us. Under conditions of extreme impact of COVID-19 pandemic, we have the unique opportunity to learn and to become stronger. We have to change deeply embedded values that define our behaviour in disaster risk management. We have to be more proactive and not wait anymore for a shift from managing disasters to managing risks (UNDRR, 2015). Now it is the moment to act.

We have to adapt and be adaptive to new and continuously changing reality before it is catching us unprepared. The question is do we know how this new reality does or will look like? A new understanding of the dynamic nature of systemic risks is a must and it is as challenging as complex the phenomena is. It is not only about awareness of the latest scientific knowledge and data collected. The more interconnected the knowledge is, the better linked the data are, the better complex nature of systemic risk is explained. It will be inevitable to combine what we know with the use of artificial or machine intelligence and all available processing capacity. Next step is to develop risk governance structures of at different levels that can effectively introduce this contextual understanding and its uncertainty in decision making process. Even more, we need a risk governance capable of connecting disciplines, sectors, policies, geographical scales, organisations and citizen

However, with systemic risk it has become obvious that risk is much easier to be managed in early stages. In prevention, adaptation, mitigation and preparedness phases the risk we manage is smaller and is still confined within one system and in many cases still local. In prevention, adaptation and mitigation phase it is essential to understand the role of risk drivers. In preparedness phase it is critical to develop and implement monitoring to identify any anomalies in system behaviours to reduce and avoid discontinuities in critical interdependent systems. Furthermore, preparedness phase has to clearly define the thresholds and the mechanisms to timely trigger the response phase. Any missed opportunities or failed timely interventions allow the risk to grow, escalate and cascade into major whole-of-society problem with a snow-ball effect that increases the potential for both, economic, environmental and human losses. Societies along the planet are all part of the same chain. Early identification and proper management of the fragile link of the chain has become a must.

---

<sup>15</sup> [https://ec.europa.eu/health/funding/eu4health\\_en](https://ec.europa.eu/health/funding/eu4health_en)

<sup>16</sup> [https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/emergency-support-instrument\\_en](https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/emergency-support-instrument_en)

## 1.1 From Version 0 to Version 1

Past experiences are showing us why it is important to start building resilience with proper evidence of how to reduce risk and prevent disasters, prepare for and when necessary, adequately respond. In addition, these experiences are highlighting the need to join forces across all sectors to be able to address the challenges from a multi-perspective approach.

Art. 6 of **UCPM Decision No 1313/2013/EU** is paving the way for Member States how to establish risk governance that would cover the whole disaster risk management framework, from preparing disaster risk strategies, that are flexible and adaptable to new knowledge and new situations to implementing prevention and preparedness measures.

Version 0 was focused mainly on how to do national risk assessment (NRA) to provide enough evidence for understanding and managing risk. While version 1 would like to position NRA as the most critical part of policy cycle for the implementation of integrated disaster risk management and to show that the implementation of integrated disaster risk management is a process of capacity development.

### 1.1.1 The purpose, content and outcome of Version 0

The purpose of Version 0 was to collect scientific contributions to facilitate better use of the guidelines "EU Risk Assessment and mapping guidelines for disaster risk management" ([Commission Staff Working Paper, 2010](#)). Version 0 is referenced in the recently adopted and officially published "Reporting Guidelines on Disaster Risk Management, Art. 6(1) of Decision No.1313/2013/EU2019/C 428/07" ([Commission Notice, 2019](#)).

Version 0 provided scientific support to UCPM participant countries in terms of the governance structure needed to do NRA and step-by-step instruction for risk assessment processes for risks related to different hazards and assets (droughts, earthquakes, floods, terrorist attacks, biological disasters, critical infrastructure disruptions, chemical accidents, nuclear accidents and Natech accidents):

- to improve coherence and consistency among the risk assessment outputs (by hazards, by sectors, by regions) undertaken in the Member States at national level
- to highlight the links of the national risk assessment with disaster risk management planning and
- to make NRAs more comparable between the Member States, which would allow having a more comprehensive picture at EU level about risk drivers and corresponding potential losses.

The outcome of Version 0 was the identification of two major scientific inputs for disaster risk management: addressing **risk comparability** and understanding of **risk drivers and required capacities**. The overall aim is to maximize the national capacity of a country in achieving the objectives NRA process. NRAs should define the relative importance of different risks (potential impacts) in the country as well as identify disaster risk drivers to act upon with a range of measures able to reduce risk in any phase of the disaster risk management.

Knowing the differences among risk assessment approaches related to different hazards/assets will eventually help us to find the framework covering all in terms of terminology, set of methodologies, risk metrics, data needed and results required for further treatment of risk. In majority of cases the science can, at the moment, provide advice for risk assessment in a single-hazard framework. Rare are the cases with more advanced level of risk assessment considering more than one hazard, hazard interactions or even vulnerability interactions. They are usually driven by the strong presence of industry, where the asset is the virtue, such as critical infrastructure disruptions, chemical and Natech accidents. These latter examples become the model for the way forward. Risk comparability should be treated in the context of risks in a multilayer single-hazard risk assessment.

To improve the understanding of underlying risk drivers and needed capacities can be dealt with the better knowledge base of risk, availability of data to describe hazard, exposure and vulnerability as well as development of the risk analysis methodologies that enables to model links between underlying risk drivers and capacities, risk components and risk levels. The disaster loss databases are of major importance. For example, using past even losses, it is possible to identify and quantify a wide range of socio-politic-economic drivers associated with the vulnerability.



### 1.1.2 The purpose and objectives of Version 1

The purpose of Version 1 is to reinforce the use of the new “**Reporting Guidelines on Disaster Risk Management**, Art. 6(1) of Decision No.1313/2013/EU2019/C 428/07” among MS. The target audience of this document are the national authorities of the EU Member States and UCPM participating states responsible for the reporting to the Commission on disaster risk management under Article 6 of the UCPM Decision 1313/2013.

The reporting guidelines are voluntary in nature. They specify template for information to be provided to the Commission based on two existing prevention blocks, **national risk assessment (NRA)** and **risk management capability assessment (RMCA)**, as well as on the priority prevention and preparedness measures for key risks with cross-border impacts and low probability risks with a high impact.

However, the reporting outcomes **are only a tip of the iceberg of the real activities related to DRM**. Therefore, Version 1 is much broader in this context and it explains the real motivation behind risk assessment process and risk management capability assessment, which have been proven essential for evidence based **disaster risk management (DRM) planning and the implementation of prevention and preparedness measures**, what capabilities have to be developed for effective DRM governance from a policy cycle perspective and it proposes an integrated approach for successfully and effectively managing disaster risk.

**Integrated disaster risk management (iDRM)** considers various drivers of risk, and possible prevention and mitigation options ranging from structural to non-structural measures, preparedness and response options from early warning system to emergency management and risk transfer such as insurance (Wouter Botzen W.J. et al., 2019). An important step lies in application of risk assessment when deciding about the risk management strategies. Risk assessment provide evidence for cost-benefit analysis of risk management options which identifies economically optimal strategies and consideration of acceptable risk levels for different risks identified to see when to prevent damages pays-off managing the damages themselves. Successful disaster risk management will require also integration across different hazards as well as different disciplines, stakeholders, different level of governments as well as global, regional, national, local, and individual efforts.

The objectives of Version 1 are to:

- address new hazards, emergent and increasing risks,
- advice on how to address climate change as cross-cutting issue,
- provide additional information to assess potential impacts,
- provide better insights into risk factors that drive the risk level and can be act upon,
- provide risk metrics to make risks arising from different hazards/regions/assets comparable to facilitate prioritizing,
- identify risk management capabilities needed for the implementation of integrated disaster risk management.

## 1.2 The structure of the Report

In order to facilitate the learning part of the reporting process and useful results of the new reporting guidelines ([Commission Notice, 2019](#)), the report will explain the purpose and objective of each step of reporting to give meaning and motivation to demanding DRM governance processes.

First, the report describes the evolution of reporting process and the efforts of European Commission and Member States to share experience and knowledge at EU level for a better prevention of and preparedness for disasters.

Then, the report explains the importance of **national risk assessment (NRA)** and **risk management capability assessment (RMCA)** as well as the **interdependency of the two processes**, for example where RMCA identifies the capabilities to be developed to integrate NRA as a core of scientific evidence into policy cycle of implementation of integrated disaster risk management.

Next, a special focus is dedicated to capability needed to **tackle climate change** with presenting possibilities how to ensure better synergies between disaster risk reduction and climate change adaptation strategies as well as **new emergent risks** that are continuously changing the risk landscape.

Last, the report presents the expert contribution on the assessment of risk related to floods, droughts, wildfires, biodiversity loss, earthquakes, volcano eruptions, biological disasters, Natech accidents, chemical accidents, nuclear accidents, terrorist attacks, critical infrastructure disruptions, cybersecurity and hybrid threats.

## 2 Towards a better understanding of disaster risks in the EU: an evolution of reporting process

**The purpose of the reporting process is to support formulating an EU prevention policy framework that would complement and enhance the national one.**

The initiative for an overall European approach to the prevention of disasters (COM/2009/82) was the origin of the reporting process. In this context, the EU seeks to reduce the impact of disasters within the EU by:

- the development of knowledge based disaster prevention policies at all levels of government;
- linking the relevant actors and policies throughout the disaster management cycle;
- improving the effectiveness of existing policy instruments with regard to disaster prevention.

**The main objective of reporting process is to have a more comprehensive view of disaster risks in the EU and a better evidence basis for EU policies for addressing those risks.** However, this is not a straight forward process. Since 2009 the objectives of the reporting process have been aligning to the outcomes of the preceding reporting, e.g.:

- to create a common knowledge base on disasters, identify the research gap and encourage the research activities,
- to promote the exchange of good practices among the relevant administrative levels in the Member States as well within the Union Mechanism and develop guidelines on risk mapping and risk management capabilities to build on common aspects,
- to develop a catalogue of prevention measures that could be considered by the Member States for EU funding,
- to exchange good practices in implementation of risk assessment, risk management capabilities and prevention and preparedness measures.

### 2.1 The beginnings of an overall European approach to the prevention of disasters

The Union Civil Protection Mechanism (UCPM) was established in 2001 (Council Decision 2001/792/EC) to improve the **EU response** to natural and man-made disasters inside and outside Europe. Today it is governed by Decision No 1313/2013/EU of the European Parliament and of the Council. But it has not been before 23 February 2009 when the Commission for the first time adopted two Communications **related to disaster prevention and reduction**. The Communication COM/2009/82 discussed creating a Community approach to reducing the impact of natural and man-made disasters within the EU, whereas the Communication COM(2009)84 presented a strategy for supporting disaster risk reduction in developing countries. These Communications supported **two global initiatives**: the implementation of the Hyogo Framework for Action 2005-2015 (ISDR, 2007) and the achievement of the Millennium Development Goals<sup>17</sup> (MDGs) from 2000, succeeded by Sendai Framework for Disaster Risk Reduction 2015-2030 and Sustainable Development Goals<sup>18</sup> (SDGs) set in 2015, respectively.

Communication (COM/2009/82) set out an initiative for an overall European approach to the prevention of disasters based on identified areas for action and defined specific measures to boost disaster prevention. Member States already had, to varying degrees, policies aimed at the prevention of disasters. Action at the Community level should complement national actions and should focus on areas where a common approach is more effective than separate national approaches. A better understanding of disasters and existing prevention policies on EU ground was seen as a pre-requisite for developing efficient disaster prevention policies. **Member States were invited to share** and make available to the Commission (Council Conclusion, 2009) best practices, lessons learnt and relevant **data and information on disasters**, whenever available including the social, economic and environmental impacts of these disasters, with a view to providing policy-relevant information to European and national policy makers. Before the end of 2011 also Member States

---

<sup>17</sup> United Nations Millennium Development Goals website, retrieved 19/8/2020.  
<https://www.un.org/millenniumgoals/bkgd.shtml>

<sup>18</sup> United Nations Sustainable Development Goals website, retrieved 19/8/2020.  
<https://sustainabledevelopment.un.org/resourcelibrary>

were invited to further **develop national approaches and procedures to risk management** including **risk analyses**, covering the potential major natural and manmade disasters, **taking into account the future impact of climate change**. Meanwhile the Commission (COM/2010/600) started to explore mechanisms for regular reviews of Member States' prevention and preparedness policies.

The Council Conclusions on Further Developing Risk Assessment for Disaster Management within the European Union (2011) emphasized the importance of **risk assessment** for the integrated disaster risk management at the national level. It enhances the basis for the analysis of **prevention and preparedness measures** as well as for **capacity analysis and capability planning**, and is a continuous and necessary **building block for the development of a coherent risk management policy**.

**The reporting process** was finally set out in 2013 with the New Union Civil Protection Mechanism legislation (Decision No 1313/2013/EU) which required Member States to periodically develop their risk assessment, first by 2015 and every 3 years thereafter. It also required Member States to make available to the Commission their Risk Management Capability Assessment every three years following the finalisation of the guidelines. In parallel, the Commission with the experts from EU Member States and UCPM participating states published Risk Assessment and Mapping Guidelines for Disaster Management in 2010 ([Commission Staff Working Paper, 2010](#)) and Risk Management Capability Assessment Guidelines ([Commission Notice, 2015](#)) in 2015.

Commission **guidelines** are not binding but they help national authorities to prepare National Risk Assessments and Risk Management Capability Assessments as required by the UCPM legislation.

## 2.2 First steps of the reporting process and lessons learned

The timeline of all consequent events is presented in **Table 1**: In 2013, a number of Member States voluntarily shared information on the hazards and impacts facing their countries. Member States and UCPM Participating States shared the main results and conclusions of their national risk assessments in two following rounds: in 2015 and in 2018.

Risk Assessment and Mapping Guidelines for Disaster Management in 2010 ([Commission Staff Working Paper, 2010](#)) suggests to make NRA a three step process: risk identification, risk analysis and risk evaluation. The aim is to objectively assess potential impacts by hazards and assets in comparative way and present the results in risk matrix to strategically define which risks should be prioritised for action. Intermediate outputs of the full exercise can provide better insights into risk factors that drive the risk level and can be used to better define the actual measures that would serve to reduce risk, and consequently reinforce the capacities.

Based on the information provided by EU Member States and UCPM participating states, the European Commission prepared the overviews of the risks facing the EU in the years 2014, 2017 and 2020 ([Commission Staff Working Paper, 2014](#); [Commission Staff Working Paper, 2017](#); [Commission Staff Working Paper, 2020](#)). The idea behind those documents is not only to present the risk landscape in Europe, but also to share good practices, methodologies, assumptions and decisions on how to carry out the risk assessment, trying to link its outcomes to the management of risk. The last round of the NRAs submitted to the Commission has shown the **huge progress** made by countries over the last years. In particular the most notable improvements are:

- the continuously enlarged spectrum of hazards and threats addressed in the assessments (including natural, biological, technological and malicious);
- the inclusion of climate change considerations in all the NRAs (including interactions among hazards such as the impact of climate change in nuclear facilities);
- the long-term view complementing the initial short-term perspectives (shifting from the reactive to the planning mode);
- the networking approach in which research institutions are more and more involved in risk assessment.

**Table 1:** History of reporting process for national risk assessment and risk management capability assessment

Year	National Risk Assessment	Risk Management Capability Assessment
2010	Risk Assessment and Mapping <b>Guidelines</b> for Disaster Management (Commission Staff Working Paper, 2010)	
2011		
2012		
2013	<b>First exercise</b> on voluntary basis	New Union Civil Protection Mechanism (Decision No 1313/2013/EU) <b>legislation</b> requires Member states to make available their <b>risk management capability assessment every three years</b> following the finalization of the guidelines
	New Union Civil Protection Mechanism (Decision No 1313/2013/EU) <b>legislation</b> requires Member states to periodically develop <b>risk assessment</b> , first by <b>2015 and every 3 years thereafter</b>	
2014	<b>Overview</b> of Natural and Manmade Disaster Risks in the EU ( <a href="#">Commission Staff Working Document (2014)134</a> )	
2015	<b>Second sharing</b> of the summary of NRAs	Risk Management Capability Assessment <b>Guidelines</b> ( <a href="#">Commission Notice, 2015</a> )
2016		
2017	<b>Overview</b> of Natural and Man-made Disaster Risks the European Union May Face ( <a href="#">Commission Staff Working Document (2017) 176</a> )	
2018	<b>Third sharing</b> of the summary of NRAs	First RMCA exercise
2019		<b>EU Overview</b> of Risk Management Capabilities (2019 <sup>19</sup> )
	<b>In 2019</b> , Decision No 1313/2013/EU on the Union Civil Protection Mechanism <b>was amended</b> by Decision No 2019/420/EU, whereby the <b>requirements for reporting under Article 6 were changed</b> . In line with the new provisions, Member States are required to make available to the Commission a <b>(combined) summary of NRA an RMCA, focusing on key risks</b> . Moreover, Member States have to provide information on <b>priority prevention and preparedness measures for key risks</b> having cross-border impacts and, where appropriate, for low probability risks with a high impact. This information had to be provided to the Commission for the <b>first time by 31 December 2020, and then every three years</b> or whenever there are important changes.	
		Reporting <b>Guidelines</b> on Disaster Risk Management, Art. 6(1)d of Decision No 1313/2013/EU (Commission Notice, 2019/C 428/07)
2020	<b>Overview</b> of Natural and Man-made Disaster Risks the European Union May Face following reporting in 2018 (Commission Staff Working Document(2020)330)	

Source: Authors

<sup>19</sup> The document has remained internal working document for European Commission and authorities due to the sensitive content.

As regards the risk management capability assessment, EU Member States and UCPM participating states shared the results of the first exercise in 2015. Based on these submissions, the Commission prepared the Overview of EU Risk Management Capabilities in 2019<sup>20</sup>.

Risk Management Capability Assessment Guidelines ([Commission Notice, 2015](#)) identifies three types of capacities: technical, administrative and financial, that governmental structures should be able to mobilize and exploit available resources to implement integrated disaster risk management. Implementation of integrated disaster risk management is seen as three step policy cycle: Risk Assessment, Risks Management Planning and Implementing Risk prevention and preparedness measures. The guidelines are designed as self-assessment questionnaire of 51 questions to cover the whole process.

The questionnaire fostered a common understanding of the elements to be checked. It was built to be easily responded with a score (from 1 to 4) and with short argumentations. The quantitative ranking allowed to quickly see if the capacity was in place and which was its level of development, being 1 when “work has not yet started” and 4 when “the capacity was embedded in the system”.

This approach served to highlight the crucial elements for disaster risk management to work in practice and it stressed the need for learning and constant improvement. Nonetheless, some **lessons learned** after the first round concluded that the complexity of the DRM cycle would require (a) the questions to be even more specific, so to say, to target unique and relevant capacities for further work, and (b) to provide a ranking system with more defined criteria that would guide countries in their capacity building activities and facilitate comparisons among hazards, regions and, when necessary, among countries.

Finally, the experience gained showed that both NRA and RMCA complement each other: the first identifies the risk necessary to be managed and define risk drivers to be acted upon, while the other tries to detect which elements should be reinforced in the governance structure to make sure that the right risk reduction measures are planned and implemented to reach the expected objectives

## 2.3 Reporting process today

**In 2019** Decision No 1313/2013/EU on the Union Civil Protection Mechanism **was amended** by Decision No 2019/420/EU, whereby the **requirements for reporting under Article 6 were changed**. In line with the new provisions, Member States are required to make available to the Commission a (combined) summary of NRA an RMCA, focusing on key risks. Moreover, Member States have to provide information on priority prevention and preparedness measures for key risks having cross-border impacts and, where appropriate, for low probability risks with a high impact. This information had to be provided to the Commission for the first time by 31 December 2020, and then every three years or whenever there are important changes.

To support Member States with the reporting exercise, the same year the Commission issued Reporting Guidelines on Disaster Risk Management ([Commission Notice, 2019](#)) replacing the Risk Management Capability Assessment Guidelines ([Commission Notice, 2015](#)).

These non-binding guidelines were designed to facilitate reporting by Member States and provide the Commission with the information needed for it to fulfil its obligations in prevention. Obtaining harmonized information is vital to have a more accurate picture of the gaps and needs at European level. The new reporting guidelines contain a questionnaire of 24 questions (**Table 2**) split in three sections:

1. risk assessments,
2. risk management capability assessment,
3. priority prevention and preparedness measures.

All the questions are addressing **key risks only**. The understanding of key risks in new reporting guidelines covers risks that have particularly adverse consequences, however, a special attention should be payed to the **cross-border** nature of risks and to risks related to the events that are rare but could have important impacts (**HILP**).

---

<sup>20</sup> The document has remained internal working document for European Commission and authorities due to the sensitive content.

**Box 1: Reporting on disaster risk management under Article 6 of the Decision No 1313/2013 on the Union Civil Protection Mechanism, as amended by Decision No 2019/420/EU**

In order to promote an effective and coherent approach to the prevention of and preparedness for disasters by sharing non-sensitive information, namely information disclosure of which would not be contrary to the essential interests of Member States' security, and to promote the exchange of best practices within the Union Mechanism, Member States shall:

- a) further develop risk assessments at national or appropriate sub-national level;
- b) further develop the assessment of risk management capability at national or appropriate sub-national level;
- c) further develop and refine disaster risk management planning at national or appropriate sub-national level;
- d) make available to the Commission a summary of the relevant elements of the assessments referred to in points (a) and (b), focusing on key risks. For key risks having cross-border impacts as well as, where appropriate, for low probability risks with a high impact, Member States shall describe priority prevention and preparedness measures. The summary shall be provided to the Commission by 31 December 2020 and every three years thereafter and whenever there are important changes;

**Table 2:** Questions in Reporting Guidelines on Disaster Risk Management ([Commission Notice, 2019](#)) addressing risk assessments, risk management capability assessment and priority prevention and preparedness measures.

Risk Assessments	Risk Management Capability Assessment	Priority Prevention And Preparedness Measures
1. Risk assessment process	9. Legislative, procedural and/or institutional framework	21. Key risks with cross-border impacts
2. Consultation with relevant authorities and stakeholders	10. Roles and responsibilities of the competent authorities	22. Priority prevention and preparedness measures
3. Identifying the key risks at national or sub-national level	11. Roles of relevant stakeholders	23. Low probability risks with a high impact
4. Identifying climate change impacts	12. Procedures and measures at national, sub-national and local level	24. Priority prevention and preparedness measures
5. Risk analysis	13. Procedures and measures at cross-border, inter-regional and international level	
6. Risk mapping	14. Focus on climate change adaptation measures	
7. Monitoring and reviewing risk assessment	15. Focus on critical infrastructure protection measures	
8. Communicating risk assessment results	16. Source(s) of financing	
	17. Infrastructure, assets and equipment	
	18. Focus on disaster loss data collection and procedures	
	19. Focus on early warning systems equipment and procedures	
	20. Risk information and communication to raise public awareness	

Source: Authors

**Reporting outcomes are only a summary of the real activities related to NRA and RMCA in the country.** NRA and RMCA processes are much more comprehensive and tailored to the national context to serve the national goals than aspects addressed with questions. The proposed questions are designed to foster a shared understanding of the aspects that NRA and RMCA should include and are not relevant only for national context but also EU one. Such aspects are activities at cross-border, inter-regional and international level, climate change adaptation, critical infrastructure protection and disaster loss data collection. **However, the overall aim is very much the same, i.e., to implement disaster risk reduction strategies which should result in less disasters and/or disasters with less impacts and increase of overall EU resilience.**



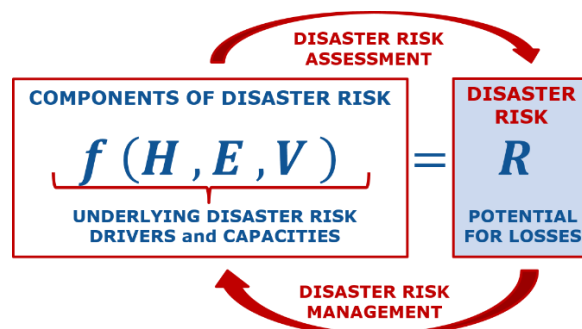
### 3 National Risk Assessment

#### 3.1 The purpose and objectives of national risk assessment process

**The purpose of national risk assessment is to reach a common understanding of the risks faced in a country. The outcome of risk assessment facilitates stakeholders to know the relative importance of the risks and identify risks to prioritize action for.**

According to the reporting guidelines (Commission Notice, 2019) definition of the key risks is prerogative of the Member States. Further guidance how to identify key risks is not given. **Risk assessment is a tool to identify key risks** in terms what we should be most afraid of, how likely it is to happen and can we do something about it. However, risk is multi-faceted and there are many aspects to consider to separate the wheat from the chaff that is to identify those risks which we need to manage and those we cannot or are not so relevant to be managed. For example one type of hazardous event (sometimes referred to as danger or threat) can cause impact in different sector or on different assets. One asset or sector can be harmed differently by different hazards. Furthermore, in the country there are some hazards that are more frequent or more severe or both than others. Also there are some assets or sectors in the country, which are more important than others and need to be protected with priority. NRA pinpoints the most relevant risks considering most exposed, most vulnerable and most important assets doing the scanning through different sector and different hazards. For that purpose NRA should be **multi hazard** and **multi sectorial** where assets or sectors are predefined due to importance they have for the security and well-being of society. However, the information collected from the past events and the knowledge of emergent and new risks are of great help to do this efficiently.

**Figure 1:** Risk assessment provides an opportunity to better understanding of the underlying disaster risk drivers and informs disaster risk management measures (H: Hazard, E: Exposure, V: Vulnerability, R: Risk).



Source: Authors

**The objectives of a national risk assessment are to obtain the following information that could be helpful in further DRM planning (Figure 1):**

- assess levels and related probabilities of identified risks,
- understand the relations between risk and risk drivers and capacities to act upon,
- prioritize risks arising from different hazards, different regions, different assets.

In order to achieve these objectives consistently and comparably over time and geographical scale the National Risk Assessment process needs a governance model that follows a standardized format, such as ISO 31010.

#### 3.2 Governance of National Risk Assessment Process

National risk assessment is a compound of many processes of risk assessment. Different hazards as well as different assets require very different analysis of their risk.

The multi-disciplinary nature of the disaster risk assessment requires information and knowledge of many parties from different communities to conduct the comprehensive process of NRA. A robust and flexible **governance model of NRA** in which **one authority has the mandate** to coordinate all parties involved is essential. The goal of the governance model of NRA is to enhance coherence across portfolios, to create a working environment based on the same set of evidences, provide harmonized results and take care of the communication to stakeholders, authorities and public.

The governance model of NRA should consist of **a number of working groups** for different types of natural and man-made hazards as well as for different assets consisting of scientific experts, practitioners and representatives from all relevant sectors and governments departments or agencies responsible for DRM planning. The goal is to have at the same table data providers, end-users, and all technical support. The National Platforms for Disaster Risk Reduction as promoted by the UNISDR (2017a), are an example of a national mechanism for coordination and policy guidance on disaster risk reduction that is multi-sectoral and inter-disciplinary in nature, with public, private and civil society participation involving all concerned entities within a country. It is often the case that national platforms are also the best suited to link the Sendai Framework for Disaster Risk Reduction with other strategies, such as the Sustainable Development Goals (SDG, 2015), the UNFCCC Paris Agreement (UN, 2015), and the Covenant of Mayors (2008).

Top down coordination is important to establish priorities but bottom up approaches should not be neglected either. Each process of risk assessment is performed by a technical team that **should not work in isolation**. Each process of risk assessment should be conducted collaboratively with stakeholders and interested parties, including central and regional levels of government and specialised departments and drawn on the knowledge and views of all involved. Only then the risk assessment processes can be carried in the context of NRA. It is a matter of:

- getting relevant, appropriate and up-to-date information and input data for the analysis;
- identifying risk, applying **risk metrics** to ensure comparability and be aware of risk criteria (acceptable risk) which is largely a political decision;
- understanding which are the assets to be protected and which are the potential impacts that are of main concern;
- supporting the design of realistic risk scenarios and
- providing useful and usable results.

In an ideal case technical teams should be fully aware of national sustainable development strategies, they should address all relevant issues and EU directives/policies and they should enjoy the support of all stakeholders/sectors from the beginning of the risk assessment process. Examples of relevant EU risk management policies include, among others (Marin Ferrer et. al, 2018):

- The EU Flood directive (Directive 2007/60/EC),
- The Seveso III directive (Directive 2012/18/EU),
- The European programme for Critical Infrastructure (EPCIP) (COM/2006/786) and The Protecting Critical Infrastructure directive (Council Directive 2008/114/EC)<sup>21</sup>,
- EU Solidarity Fund (Council Regulation (EC) No 1212/2002),
- EU strategy on adaptation to climate change (COM/2013/216)<sup>22</sup>,
- Directive on serious cross-border threats to health (Decision No 1082/2013/EU)<sup>23</sup>.

### 3.3 ISO 31010 format of National Risk Assessment Process

ISO 31030 (ISO, 2018) provides a common and very general approach to managing any type of risk. It is not hazard or asset specific. It divides the risk assessment process (**Figure 2**) into three stages: **risk**

---

<sup>21</sup> Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities, COM/2020/829 final

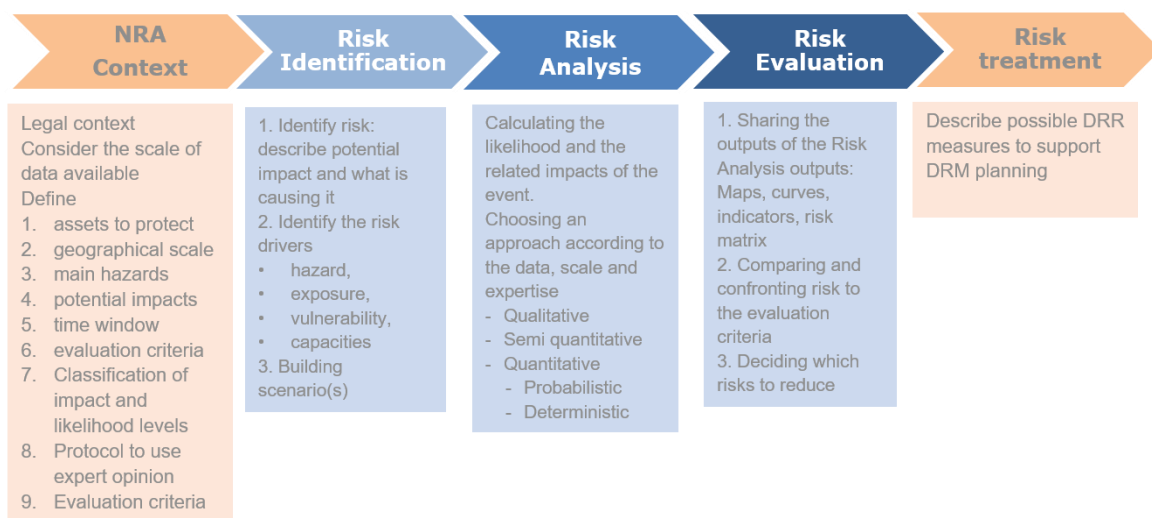
<sup>22</sup> New EU strategy on adaptation to climate change expected in February 2021

<sup>23</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on serious cross-border threats to health and repealing Decision No 1082/2013/EU, COM/2020/727 final

**identification, risk analysis and risk evaluation.** There are several advantages when risk assessment processes follow the same format within the NRA context:

- helping target readers/users to find themselves around (where to start, what to expect) in topics perceived as complex and tackled with a variety of different approaches.
- helping experts to fit their expertise into predefined modules, thus transforming the complex phenomena into complicated process, that is into a set of feasible tasks, that are normally executed by different actors to reach the desired results.
- facilitating the usage of the same terminology.
- supporting the documentation of the whole process to assure transparency and consistency.

**Figure 2:** Stages of Risk Assessment process according to ISO 31010



Source: Authors

### 3.3.1 Context of National Risk Assessment

The NRA governance identifies the context with the support of all involved stakeholders. The context defines the commonalities of all risk assessment processes related to all stages and assures the consistency and comparability of results. All parties involved should at the start of the process agree on:

1. **What needs to be protected in the country** – the list of assets that should be considered in the risk assessment processes, such as population, buildings, infrastructure, environment, etc., that are broken down to a **level of detail** meaningful for making decisions and allowing to assign vulnerabilities.
2. **Which are the hazards that the country is exposed to** – the set of scenario for different hazards and different probabilities (likelihood) of occurrence (discrete values). Consideration should be given to both, extensive, frequent, low-impact and intensive, occasional, high impact events.
3. **Which are the risks to be considered, that is, the potential impacts**, direct and indirect, and what are the risk metrics to measure them: human impact, economic impact, environmental impact and political/social impact. The criteria for selection are based on the assets to be protected and the values they present.
4. **What is the time window for the potential impacts to be considered** – the temporal horizon of risks to be assessed is decided. The process should consider risks that may occur in the immediate future (2, 5 or 10 years) and in the long term (15 or 25 years) to accommodate the prioritisation of

high probability/low impact events and low probability/high impact events, respectively. Long term periods are also considered to identify emerging risks, driven by climate change, also cyber security, volatility of geopolitical landscape, etc.<sup>24</sup>. With enlarging the time window for the scenarios also more distant direct and indirect impacts should be covered, and with considering more than one time window, information can be included to propose prevention and recovery measures.

5. **Classification** of impact and likelihood levels should be defined. The choice of the criteria for classes is largely a political decision. The selection of criteria is related to the risk tolerance in the country. For example, one country might define "insignificant" a human impact of 10 fatalities while the other no fatalities. The number of classes depends on the expected uncertainties introduced mainly through different risk assessment approaches: higher the uncertainties, smaller the number of classes introduced. The impact classes are defined for each type of impact and are derived from impact criteria. In case of likelihood levels it is recommended to carefully select a likelihood scale that can effectively cover the risks of intensive as well as extensive disasters.
6. **Quality criteria** in terms of acceptable levels of uncertainty arising from the input data and models used in different stages of risk assessment should be framed (Zio and Aven, 2013). Uncertainty, though, can provide interesting information for the exercise and for future actions to implement the management of risk. Some frameworks can be found in the literature to guide scientists and other stakeholders to deal with it (Refsgaard et al., 2007; van der Sluij, 2005; Walker et al, 2003).
7. Design of a **protocol for the use of expert opinion** and for the design of a procedure to document the whole process of the risk assessment process to assure **transparency and consistency**.
8. **Risk criteria** need to be agreed on in order to be used in the risk evaluation stage (Chapter 3.3.4) as a term of reference against which the significance of a risk is evaluated and determine whether the risk assessed is acceptable or not. However, partial knowledge of risk criteria should be known in advance as they dictate the risk metrics and level of detail (resolution).

With periodic reporting (every three years) the context should be updated. Risk is dynamic and it should be treated as such. The start of the new NRA process is also the opportunity for improvements:

- to introduce experiences gained from previous NRAs,
- further development in the datasets and risk assessment methodologies,
- changing hazard landscape due to climate change and emerging risks as well as
- considering increased DRM capacities due to implemented risk prevention and preparedness measures
- the occurrence of disastrous event provided new insights, while reconstruction was an opportunity to build back better and to adapt to new risks.

### 3.3.2 Risk Identification

According to ISO 31030 (ISO, 2018) the purpose of risk identification is to **find, recognize** and **describe risks** that a country would like to reduce using existing risk information. The main task here is to collect relevant, appropriate and up-to-date risk information from national and international sources and to use different approaches for finding and recognizing risks, such as:

4. *The DRMKC Risk Data Hub database* (Antofie et al., 2019) has been designed to collect risk and loss data from natural and technological hazards. The Risk Data Hub covers floods, forest fire, earthquake, landslide and subsidence, and soon windstorms, heat waves, cold waves, volcano activity, droughts, oil spills and radiological dispersion. However loss and risk data comparability is still an issue to make the information useful for disaster risk assessment. Harmonization or even standardization of loss data gathering is needed to bring such information to the next level.

---

<sup>24</sup> Insurance and reinsurance companies monitors the evolution of the risk landscape on a continuous basis (Swiss Re SONAR: New emerging risk insights) protect their clients and themselves against undue uncertainties, but many of identified future risks unveiled could be also of national concern

5. *Loss and damage databases*, which informs about the occurrence, magnitude and losses suffered. The data recorded after an event not only indicates the level of exposure of a society but also helps identifying the key drivers of losses (De Groeve et al, 2013). The collection of disaggregated loss data is essential for the empirical identification of the physical vulnerabilities of different assets under different hazards. For example, there are national disaster loss database, European platform of risk data Risk Data Hub<sup>25</sup> or online database with global coverage EMDAT<sup>26</sup>. Gathering of loss data (De Groeve et al, 2014) is comprised of data model, data collection (which data has to be collected and how), data recording (processing, aggregation and storing) to have the overview of situations that are strongly context related.
6. Hazard identification techniques, which are quite common in the industrial sector, such as HAZOP studies, fault trees, checklists, etc. (Mannan, 2012). Some methods can serve to describe the causes and conditions that favour hazard to happen.
7. The risk identification stage is directly linked with the formulation of (a) problem, and as pointed out by Powell et al. (2016), the use of *soft Operations Research* methods can be useful to structure and formulate complex problems, where different stakeholders have different interests and require different expertise to describe these problems.
8. *Accident investigations or post-disaster reports*, including documents containing lessons learned. These documents and the experience of those engaged in responding and recovering from past disasters can support the understanding of the underlying causes leading to consequences. These reports usually serve in taking corrective actions and improving protocols, and in displaying changes in risk factors. For example, some industries, such as aviation and chemical processing, commonly record near-miss events, which are a valuable source of learning from the past (Phimister et al, 2003).
9. *Map of relevant research projects* (Project Explorer<sup>27</sup>) and other repositories of scientific article.
10. *Loss projections* that were used in past as efforts of risk assessments within the country (past NRA exercises 2013 and 2015). Besides learning from the past, and considering the effect that climate change will have on disaster risk, it is necessary to consider the potential future losses due to changes in assets' exposure, vulnerability and the nature of the hazard.
11. International efforts related to *national risk profiling* (INFORM<sup>28</sup>).
12. *Monitoring and Early Warning Systems* in place. These are constantly collecting and analysing data of precursors of risk. Detecting trends and changes in the data collected can facilitate the team engaged in the RA to picture how risk is or is changing. Besides the traditional and operational warning systems for protecting people's lives and properties, the team can also exploit foresight approaches, citizen sciences and media monitoring (DG ENV, 2016).

According to "EU Risk Assessment and mapping guidelines for disaster risk management" ([Commission Staff Working Paper, 2010](#)) there are four different categories of potential impacts: human impacts, economic impacts, environmental impacts and political/social impacts (including security). **Risk description** can be of different format strongly dependent on the existing knowledge. It ranges from qualitative to quantitative description. Qualitative description is used for intangible impacts, e.g., on cultural heritage, or the impacts related to new and emergent risk, which is often difficult to identify, detect and attribute and consequently address them. Quantitative description is feasible for tangible impacts that we can measure or model and relate to risk metrics. If risk metric used has its counterpart among loss indicator we can align it with the goals, targets and reporting guidelines of the Sendai Framework for Disaster Risk reduction.

For each of the risks to be studied, it is necessary to gather the available **information on the risk components** relevant to the NRA context (Chapter 3.3.1) to prepare:

- hazard models,
- exposure models,
- vulnerability models and

<sup>25</sup> <https://drmkc.jrc.ec.europa.eu/risk-data-hub>

<sup>26</sup> <https://www.cred.be/projects/EM-DAT>

<sup>27</sup> <https://drmkc.jrc.ec.europa.eu/knowledge/Projects-Explorer#project-explorer/631/projects/list>

<sup>28</sup> <http://www.inform-index.org/Countries/Country-Profile-Map>

- relevant selection of risk drivers and capacities.

It is necessary to **study which are the causal mechanisms of risk** (Powel et al, 2016): characterize the activities and conditions that trigger the hazard; the factors that drive the assets' exposure and vulnerability; and which are the capacities (at the level of asset but also beyond it).

It is also important to identify also the risks (e.g., emerging risks, cross-border risks) which sources are not under control and that can result in a variety of tangible and intangible consequences. This is also an opportunity to address issues such as lack of data, limitation of knowledge, reliability of information and corresponding uncertainties.

All the information produced in the stage of risk identification is actually the formulation of a problem, which will help risk analysts to design a model or methodology to obtain the outcomes of the potential impacts with their probability of occurrence on the assets at risk.

### 3.3.2.1 Scenario Building

The scenarios have become a form of **communication model** and help bridge the theoretical models and the needs to solve practical problems (Alexander, 2000).

At the first place scenarios are a replacement for describing future disaster events in terms of their magnitude and probabilities which can be based solely on known science. Instead the information about what can happen in the future disaster can be better described with **sets of scenarios**. These scenarios comprise the triggering events together with the description of possible consequences from cascading events to the impacts on societal systems while considering the capacities in place. Therefore, the scenario building process requires input from scientists, practitioners, policymakers and different parts of communities that complements with community's experience of past events and knowledge of social, cultural, economic and political context.

This co-development process (Davies et al., 2015) is beneficial not just because such engagement allows mutual learning, the sharing of existing knowledge and the co-production of new knowledge, but also because the knowledge that emerges is much more likely to have societal and scientific consents, because it will be perceived as relevant by all involved (Mercer, 2012; Wistow et al. 2015)

Scenarios can be used for modelling all phases of the disaster risk management cycle. For the purpose of emergency preparedness, recovery and reconstruction planning the "maximum credible" or "plausible worst case" scenarios are of interest. For the purpose of the risk assessment process their aim is to analyse the potential impacts and their likelihood. Therefore, it is recommended to have **multiple scenarios with various likelihoods of occurrence** to obtain a more complete picture of risk (UNISDR, 2017).

A scenario presents just *a* possible future, but should be internally consistent and plausible (Börjeson et al, 2006), covering all possible events and related effects so as to reach the desired information of risk impact. Shoemaker (1995) proposes three tests to ensure internal consistency and plausibility: compatibility of trends, outcome combinations and reactions of major stakeholders. There would always be events and their characteristics that will remain *unknown unknowns*, but we reduce this by having relevant stakeholders on board (Aven, 2015). Assumptions are an inherent part of the scenario building, as such should be examined and reported.

### 3.3.3 Risk Analysis

Risk analysis is the process of combining the risk components of hazard, exposure and vulnerability to determine the level of risk. For every risk and risk scenario identified in the risk identification stage, risk analysis determines the potential impacts and the probability of occurrence. Risk analysis approaches vary in various degrees of detail depending on the purpose of the analysis and data available as well as on how they address uncertainties arising in different stages of the RA process. Each risk analysis approach has different limitations as well as advantages. They differ among **qualitative, semi-quantitative** (risk matrix and indicator based) and **quantitative** (deterministic and probabilistic) methods. The most suitable methodology should be chosen based on:

- purpose of the analysis (prioritization, planning, analysing the effect of changes, etc.);

- the agreed level of detail;
- the time span of the assessment;
- the agreed level of uncertainty;
- the availability and reliability of information;
- the existing models to produce these results;
- the resources at hand (in terms of time, money, expertise, etc.) for the exercise.

Here it is worth mentioning that the knowledge base of risk, as inherently uncertain (Covello and Merkhofer, 1994), can be limited. It is often the case that the knowledge base is decisive in deciding the approach for the analysis. Ideally, quantitative approaches would be favoured in front of qualitative ones and probabilistic models instead of deterministic analysis, to ensure that the outcomes of the analysis are objective and replicable.

**Qualitative risk analyses** are risk narratives based on expert judgment. They are commonly used for screening risks to determine whether they merit further investigation. Sometimes it is the only option when almost all components of risk are not quantifiable or have a very large degree of uncertainty. It may be the case that a qualitative assessment provides the risk manager or policy-maker with all the information they require. For example, if there are obvious sources of risk that can be eliminated, one does not need to wait for the results of a full quantitative risk assessment to implement risk management actions. An important criticism for qualitative approaches is its subjectivity, which affects its reliability. In order to facilitate its replicability, the processes need to be clear and structured, so different experts can repeat the analysis.

**Semi-quantitative** risk analysis seeks to categorize risks by comparative scores (e.g., tolerable, intermediate, intolerable). They permit to classify risks based on expert knowledge with limited quantitative data (Haimes, 2008; Jaboyedoff et al., 2014). They can be a useful stepping stone towards a full quantitative approach, particularly where detailed data are lacking and can be used as a means to capture subjective opinion which makes it a good basis for discussing risk reduction measures (Simmons et al., 2017).

**Risk matrix** is a mean to communicate the results of a semi-quantitative analysis. The risk matrix is made of classes of frequency of the hazardous events on one axis, and the consequences (or expected losses) on the other axis.

Following the limitations of risk scoring systems (Cox et al., 2005), if some data is available, even rough, it is recommended to use quantitative methods in order to recognize uncertainty and the correlations existing between the components of risk (hazard, exposure and impact). In the case of high uncertainties, by trying to quantify them and identifying their contributors, it is possible to not only increase the knowledge base, but also to better allocate funds and resources for future research developments (Apostolakis, 2004). Nonetheless, expert judgement could be necessary when the underlying mechanisms are not well understood (Abrahamsson, 2018).

Another semi-quantitative approach to measure risk is based on the methodology of composite indicators. Such **indicator-based approach** is useful when there is not enough data to quantify all the components of risk over large areas to carry out a quantitative analysis, but also as a follow-up of a quantitative analysis, as it allows taking into account other aspects than just physical damage. As a matter of fact, the indicator-based approach is the only method that allows carrying out a holistic risk assessment, including social, economic and environmental vulnerability and capacity. Indicator-based approaches allow incorporating the risk concept where each risk component (hazard, exposure, vulnerability and capacity) is composed by risk drivers defining it and presented by indicators. Data for each of these indicators are collected at a particular spatial level, for instance by administrative units. These indicators are then standardized (e.g. by reclassifying them between 0 and 10), weighted internally and composed with arithmetic or geometric average. Although the individual indicators normally consist of quantitative data (e.g. population statistics), the resulting hazard, exposure, vulnerability, and risk results are scaled between 0 and 10. These relative data allows comparing the indicators and indices (i.e., composite indicator) for the various administrative units. These methods can be carried out at different levels, even at communities (e.g. INFORM subnational risk index<sup>29</sup>). **The resulting risk is relative** and doesn't provide information on the level and probability of the potential losses.

---

<sup>29</sup> <http://www.inform-index.org/Subnational>

**Quantitative risk assessment** can assess potential impacts in two ways: deterministically or probabilistically.

**Deterministic risk assessment** estimates impacts from a single hypothetical scenario or combination of scenarios but do not necessarily consider neither the probability of the events in quantitative terms nor guarantee that all possible events are captured within a deterministic scenario set. Even though the probability of the events is not considered, risk analysis can still quantify **the uncertainties** that permeate the different steps of the computations. It can take into account uncertainties from the input parameters and models related to exposure and vulnerabilities to get the ranges of risk estimates for each scenario. The distribution of these risk estimates can be queried with statistical procedures to arrive at quantitative probabilities that can be assigned to the risk levels. Therefore, the probability of impacts differs from the probability of an event.

**Probabilistic risk assessment** attempts to associate probability distributions to frequency and severity of hazards and then run many thousands of simulated events in order to assess the likelihood of impacts at different levels.

Probabilistic approaches face their particular challenges. Some decision-makers may be reluctant to change approach if the education of probability is not widespread enough, especially among those making the final decision (Lund, 2008). It is necessary to communicate these model results in a specific, judicious and unambiguous way with sufficient scientific evidence and uncertainty (Jansen et al, 2017). Lund (2008) also indicates that the costs of probabilistic risk analysis may be higher than other methods, and is recommended in situations where large expenditures need to be studied or when the impacts of disaster would have very large consequences.

The outcomes of the risk analysis are the potential impacts over an agreed period of time. This result is linked to a particular uncertainty level that ideally has been aggregated from different sources of uncertainty. A sensitivity analysis provides information about the parameters of the model or other assumptions taken, determining their weight in the final outcomes obtained, facilitating to identify pitfalls while helping to verify and validate the model (Frey and Patil, 2002).

### 3.3.4 Risk Evaluation

According to ISO 31010 (2018) risk evaluation is the process of comparing the results of risk analysis with risk criteria to determine whether further action is required.

**Preparing outcomes of risk assessment process for responsible DRM planning is crucial.** Experts involved in risk assessment process should have a control also over the "evaluating risk" stage, in spite of not being the experts those who advocate the risk criteria. However, partial knowledge of risk criteria should be known in advance as it dictates the risk metrics and the level of detail (resolution). This is the stage when the outputs of risk analysis are prepared for communication outside the expert group. This is a very delicate step because the **experts are not only communicating the results but also the responsibilities to the users of the results**. Therefore the results should be accompanied with the instruction for use. The results should be understood correctly among all DRM responsible parties, only then the comparison and prioritization is possible as well as the risk criteria established. For example, the scale (resolution) of input data dictate also the scope of the results and their suitability for the decision making process at national, subnational or local levels. Or for example, the information on the time window considered can be important to determine whether climate change effects can be reflected in the results. The outcomes should be presented considering that the mentioned audience may not have a technical background, so risk should be represented in different and suitable ways: percentages, "natural frequencies", bar charts, pie charts, among others (Riesch, 2013). The tools, such as maps, matrices, indices and curves, showing risk and the components of risk, as well as different aspects of it.

The outcomes provided must be **accompanied also with the overall uncertainty**, that should have been aggregated from the different phases and limitations of the methods used: due to the context, input data, models structure and outcomes, and the model parameters (Walker et al, 2003). The uncertainties can be again represented in various ways depending on the approach. Quantify uncertainty as much as possible, in order to avoid linguistic ambiguity. A particular quantification of uncertainty can be provided together with a description of the non-quantified uncertainties. Expert judgment may be used if necessary, but it must be openly reported. Explicitly stating the uncertainty and limitations of the outcomes of risk analyses helps



decision-makers to agree in additional actions regarding the exercise (such as investing more time and money to collect new data or revise the model, if results are not good enough for decision makers) while boosting future research in the areas that should be further developed.

**Risk metric is the common point.** The challenge is to assure the comparability of the risks obtained from different RA process. The outcomes of each risk assessment should fit in the aggregation process where the outputs from various analyses are merged into a common format for evaluating and comparing risk and communicating results.

The outcomes of the analysis are then presented to decision-makers, to compare and confront them to a set of criteria to **reduce risk to an acceptable or tolerable level**<sup>30</sup>. In the context of NRA, the risk criteria reckon with the socio-economic and political context of the country, such as:

- Costs, in monetary terms of the potential impacts, versus the benefits gained from taking the risk.
- Legislation in place, codes or standards of practice.
- Reversibility of impact – the possibility to reverse the negative consequences.
- Immediate effects on critical services.
- Controllability of consequences.
- Societal Perception, as "people respond to the hazard they perceive" (Slovic et al 1982). This information can be extracted from social surveys, attitude surveys and behavioural intentions and psychometric scaling techniques (Gough, 1990). Some of the dimensions underlying perceived riskiness listed by Vlek (1966) can actually be used as evaluation criteria, such as social distribution of risks and benefits or the voluntariness of exposure.

The results of the risk evaluation can lead to decision whether not to do nothing further, consider risk treatment options or to do further analysis to better understand the risk.

### 3.3.5 Risk Treatments

The final outputs of the NRA is to map the risk and declared the risks that are "**non-acceptable**" or "non-tolerable", and need **to be managed**. The purpose of risk treatment is to select **integrated disaster risk management options** for reducing risk tackling related risk factors with actions in different phases of disaster risk management: prevention, mitigation, preparedness, recovery and reconstruction or adaption options. There is **no one-approach-fit-all-the-risk**. For each hazard or asset related risk there are different solutions efficient in different phases of the DRM cycle. Risk treatment is an iterative process of formulating and selecting risk treatment option, assessing the effectiveness of that treatment, deciding whether the remaining risks acceptable and if not looking for further options.

Furthermore, the selection of risk management options is dictated also by of their economic efficiency that is dependent on frequency and severity of the events. This, so called risk layering (Mechler et al., 2014), where frequent events (low layer risks) are avoided through risk reduction, medium-layer risks are treated with risk reduction and risk-financing instruments that transfer residual risk. However, insurers are reluctant to cover risks from rare events when public and donor post-disaster assistances are necessary while for very rare events (very high-level risk layer) even the capacity of international aid agencies can be exceeded and it might be good to consider prevention and adaption risk management options related to governments incentives to reduce risk.

The objective(s) to be reached, which would shape the strategies and policies to implement, would be politically and even socially discussed, which would depend on the values, beliefs, alternatives and resources in place to manage and reduce the risk (Fischhoff et al, 1980; Plattner, 2005) that are inherent part of disaster risk management planning.

---

<sup>30</sup> Tolerable risk is defined as the level of risk that society is ready to live with as long as the risk is managed to reduce it, while acceptable risk represents the level to which society is prepared to accept without any risk management option put in place (Bell et al, 2005)

### **3.4 Key Messages**

**NRA together with DRM planning and the implementation of prevention and preparedness measures formulates the policy cycle for the implementation of integrated disaster risk management.**

NRA is an essential part of that policy cycle and, therefore, it needs a proper governance with a legal framework and standard approach for risk assessment, to create a working environment based on the same set of evidences, enhance coherence across portfolios, provide harmonized results and take care of the communication to stakeholders, authorities and public to strengthen the community awareness.

**NRA establish a common understanding among stakeholders, authorities and public of risks that the country has to face.**

NRA is a result of collaborative work of many parties involved is the process that bring at the same table data-providers, technical support and end users. They are scientific experts from different fields, practitioners and representatives from all relevant sectors and governments departments as well as participants from public and private entities. As such NRA paves the way to consensus process in defining priorities and preparation of disaster risk reduction strategies.

**NRA exploits the existing information and knowledge at the global to local level and mobilize national experts for better understanding of risk and mechanisms between risk and risk drivers as well as capacities of communities, governments and international organizations.**

The NRA reveals the issues of lack of data, knowledge gaps, reliability of information and corresponding uncertainties. NRA advocates further development of monitoring and early warning systems, implementation of loss and damage databases to validate risk modelling, strengthening of financial mechanisms within the governmental institutions and to facilitate market-based instruments to transfer risk. NRA defines lines of research to be funded and the partnerships to be built, specially cross-border and across-levels.

**NRA provides an essential technical information for the integrated disaster risk management**

NRA examines various drivers of risk and enhances the basis for the analysis of prevention and mitigation measures, from structural to non-structural measures, preparedness and response options from early warning system to emergency management, risk transfer such as insurance, as well as for capacity analysis and capability planning. It contributes to reviews of existing disaster risk management plans and actions taken, regular updates of recovery and reconstruction plans considering the new adaptation, mitigation and preventive options available in time. As such it presents a continuous and necessary building block for the development of a coherent risk management policy. Risk Management Capability Assessment

## 4 Risk Management Capability Assessment

### 4.1 The purpose and objectives of Risk Management Capability Assessment

**Risk management capabilities addressed are capabilities required for the successful implementation of integrated disaster risk management. The implementation of integrated disaster risk management is the process seen as policy cycle.**

The assessment of risk management capability covers the whole risk management cycle, i.e. (a) risk assessment, (b) risk management planning for prevention and preparedness and (c) the implementation of risk prevention and preparedness measures (Commission Notice, 2015). The whole risk management cycle of RMCA guidelines refers to **evidence-based policy cycle**<sup>31</sup> (Figure 3) for the implementation of integrated disaster risk management. This fact is of major importance when thinking of capabilities to be built for the purpose. Herein, **the capabilities should be understood as means to an end and not as an end result.**

#### **Box 2: What is Risk Management Capability in the framework of the UCPM (Decision No 1313/2013/EU)**

**Risk management capability** (Decision No 1313/2013/EU) means the **ability** of a Member State or its regions to reduce, adapt to or mitigate risks (impacts and likelihood of a disaster), identified in its risk assessments to levels that are acceptable in that Member State. Risk management capability is assessed in terms of the technical, financial and administrative **capacity** to carry out adequate:

- (a) risk assessments;
- (b) risk management planning for prevention and preparedness; and
- (c) risk prevention and preparedness measures;

Ability, capability, and capacity are synonyms in many of their uses<sup>32</sup> and as such are often used interchangeably. All are frequently used to refer to one's power to perform an action. However, more careful treatment of the terms can actually lead to some useful breakthroughs for a country, organization or an individual working through change. In an individual it is accepted that **an ability** is the skill or competency to perform a task. **A capability** can refer to an ability that exists in an individual but can be improved upon. A capability is a collaborative process (in organization) that can be deployed and through which individual abilities can be applied and exploited. **A capacity** on the other hand is the maximum ability to perform. Capacity is the time or manpower having to perform a task. Capacity tends to relate to volumes and quantities. When discussing capacity, it is important to ask "How much do we have?", "How much is needed?" and "When do we need it?" The organization's productivity is determined by its levels of capability and capacity. A capacity is the ability that exists at present whilst capability refers to the higher level of ability that could be demonstrated under the right conditions.<sup>33</sup> There is an interesting interplay between capacity and capability building. They can compensate each other but the tendency is towards high capability and high capacity when you have high value skills to produce high value product reliably and consistently. In many cases, building capability by increasing a team's knowledge and skills can actually help expand capacity. This is, in essence, the idea of working smarter, not harder.<sup>34</sup>

**The purpose of the assessment of risk management capability is to set up an efficient, flexible and systematic process [structure] for the implementation of integrated disaster risk management. This is achieved through regular assessments which ensure continuous improvement in risk management capability.**

<sup>31</sup> A policy cycle is a systematic process [structure] showing how societal issues or public problems are acknowledged followed by step-by-step sequences depicting how the identified problem issues should be solved. The policy cycle, or sequenced policy process, was initially proposed by Harold Lasswell in 1950s (Howlett and Ramesh, 2003:11-2) and the cycle was subsequently adopted by others.

<sup>32</sup> <https://grammarist.com/usage/ability-capability-capacity/>

<sup>33</sup> As an example:

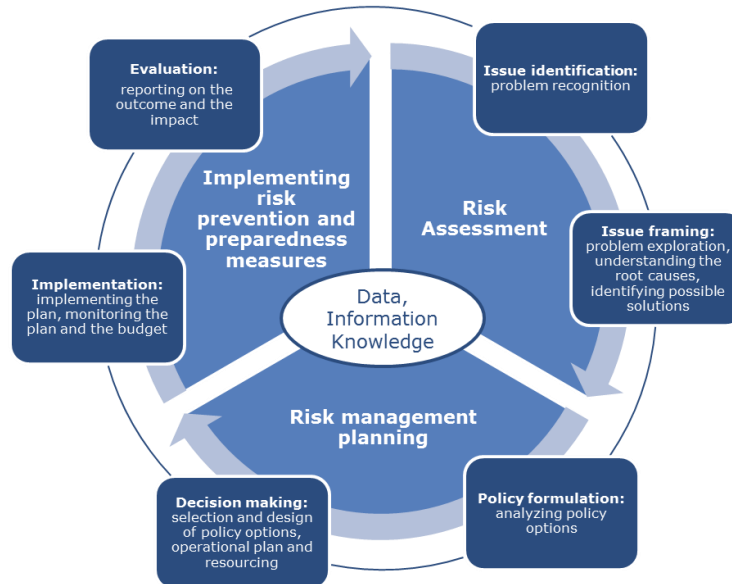
- I have the ability to run.
- I have the capacity to run a 100m race in 18 seconds.
- I have the capability to improve my capacity through training to 15 seconds.

<sup>34</sup> <https://www.resultsmap.com/blog/capacity-vs-capability-whats-the-difference/>

**The objective of the assessment of risk management capability is:**

1. to know the policy cycle for the implementation of integrated disaster risk management
2. to identify the existing and desired capabilities
3. build up awareness of potential strengths and weaknesses and initiate the process of improvement

**Figure 3:** DRM cycle as suggested in RMCA guidelines (Commission notice, 2015) vs. classical 6 stage evidence based policy cycle.



Source: Authors

## 4.2 A link between capability assessment and capability development

The concept of the link between a capability assessment and a capability development is not new (UNDP, 2008b; FAO, 2004). It is clear from the beginning that putting this concept into practice is not a simple process. It can be broken down into five steps:

1. **Where are we now:** assessing the existing capabilities can be most straightforward step and can produce much useful results, since capability development can be only effective when it is built upon existing capabilities.
2. **Where do we want to go:** identifying the desired capabilities, that is the vision of what capabilities are required and depends largely on policies and strategies for future development and these are not always as clear as they should be.
3. **How do we get there:** comparing the existing capabilities with the desired one, assessing the gaps, defining activities/strategies to fill these gaps and lead as to the desired goals
4. **What actions do we take:** implementation of the planned strategies and activities.
5. **How do we stay there:** monitoring and evaluation of the outcome to feedback experiences and lessons learnt into the planning phase which are essential to sustain the process.

**We can say that a risk management capability assessment is a driver of sustainable integrated disaster risk management development.**

There is no unique framework to be followed as there are no formulas for capability needs that will work in all contexts. Therefore countries need to lead their own process for the implementation of integrated disaster risk management which requires a lot of effort from many parties to be fully embedded and maintained.

However, to achieve a sustainable capability development all the actors involved should know their roles and follow common strategy for developing the capabilities that are needed. Capability development is an ongoing process of change that needs to take place over time while the capacity issues and priorities will depend on a country's own level and path of development, capacity issues are multi-dimensional and complex in nature and relate as much to broader societal challenges and systemic issues as they do to training, skills development and technology transfer. **Interestingly, capability assessment promotes, for the sake of its prime concept, self-assessment approach (Chapter 4.4). However, UCPM promotes also peer-review of risk management capability as opposed to evaluation by third parties that are often conditionality based.**

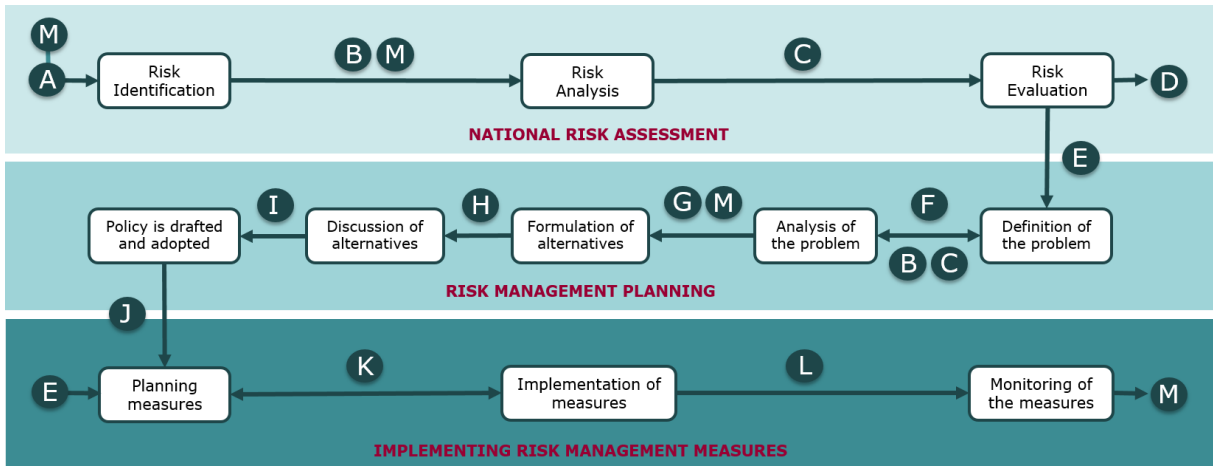
## 4.3 Implementation of integrated DRM

### 4.3.1 Knowing the process

The understanding of the DRM policy cycle process is essential for defining the needed capabilities. The policy cycle for the implementation of integrated disaster risk management is divided into three phases:

1. **Risk Assessment**, a phase that serves to identify and frame the problem, from problem recognition, problem exploration, understanding the root causes and identifying possible solutions:
  - to identify the risk that is to detect which disastrous events could potentially lead to losses and damages to the assets that the system would like to protect or to boost resilience of, trying to describe the event and the conditions and elements that lead to them;
  - to analyse the consequences (impacts) of the materialization of the identified events in time and space and to reach a common understanding with all relevant stakeholders, of the risk faced and to suggest possible solutions to manage it;
  - to map and prioritise risks, based on the needs, objectives to achieve and any other criteria to consider if agreed.
2. **Risk management planning**, a phase that formulates the policy from analysing different policy options and makes decision on selection and designing the policy options, operational plans and options. It is drawn on the results of the risk assessment:
  - identifies and leads to a selection of suitable and concrete prevention and preparedness measures taking into account the existing situation and the desired one;
  - involves into decision making process stakeholders to obtain a good understanding of the measures, their necessity and their priority in order to ensure broad support;
  - assigns appropriate responsibilities and indicates the required resources and timelines.
3. **Implementing risk prevention and preparedness measures**, a phase that implements and evaluates plans that has been decided upon in the risk management planning. The final aim is to reduce disaster risk with an integrated disaster risk management approach:
  - assess the ability to implement the measures identified in risk management planning;
  - include the allocation of responsibilities and resources, the monitoring duties as well as evaluation and lesson learned process.

**Figure 4:** Policy cycle for the implementation of integrated disaster risk management



<b>A</b>	Loss and damage data, Projections, Research projects, Contextual information, etc.
<b>B</b>	Risk components are analysed, drivers and conditions that lead to impact are well stated
<b>C</b>	Likelihood of events and their related impacts (direct and indirect)
<b>D</b>	National Risk Report (public)
<b>E</b>	National Risk Report, with the risks to prioritise (full version)
<b>F</b>	Disaster risk to treat is defined with clear objectives to be reached
<b>G</b>	Causes, background information, interest at stake, relevant actors in decision-making, etc.
<b>H</b>	Alternatives are formulated in order to reach the objective(s)
<b>I</b>	Preferred alternative(s) of action are selected and ranked
<b>J</b>	Measures are drafted in order to reach the policy objective(s)
<b>K</b>	The resources and times for each of the measures are allocated and documented
<b>L</b>	The indicators for monitoring the implementation of the measures are designed
<b>M</b>	The values of the indicators on the outcomes and the impact of the measures planned

Source: Authors

Policy-making is usually described as a continuous linear process although many factors may interfere so the process is much more interdependent and some parts may happen simultaneously. In that sense, the European Commission (2017a) has described four qualities for good policy-making:

- Policy design
- Data insights to solve policy problems
- Forward thinking
- Consultation and co-responsibility

In the case of DRM policy cycle (**Figure 4**), and as considered by the Risk Management Capability Assessment **Guidelines** (Commission Notice, 2015), the **risk assessment** produces the "evidence" that would serve for planning and implementation. According to Howlett (2009) **evidence-based policy-making** is an effort to avoid policy failures and enhance the potential for policy success through policy learning. It is expected that enhancing the information basis of policy decisions will improve the policies formulated and later implemented, while iterative monitoring and evaluation of results in the field will allow errors to be caught and corrected. If evidence-based policy-making is to be achieved governmental bodies and other stakeholders require a level of human, financial, network and knowledge resources enabling them to perform the tasks of collection, analysis, storage and use of data and information in the course of the policy-making activities (Howlett, 2009).

Following Poljanšek et al. (2018), due to the nature of disaster risk and its main purpose, the Risk Assessment produced should be multi-hazard, multi-sectorial and related to a set of defined assets, selected at the beginning of the process, due to the importance that they have for the security and well-being of society.

All these require having different multi-disciplinary groups and stakeholders contributing to the three steps of a risk assessment: risk identification, risk analysis and risk evaluation. Expertise and coordination among teams are critical factors to ensure good results. Moreover, to facilitate the use of risk evaluation outputs into the policy-making process, it is recommended that:

- the methodology should be stated and clear for everybody participating, and
- one organization takes the lead of the process.

Once the priorities are clear, the process enters into the **risk management planning** phase, where policy-makers work to define lines of action to move from the current situation of risk to and the foreseeable one. The expected benefits and impacts should be well-linked with the measures planned.

Policy-making processes change from country to country. All countries have a process established, related to specific policy planning documents, usually establishing a hierarchy among them and determining the information to include, and a set of procedures that need to be followed. In general though, the policy-making process starts by stating the problem to later compare alternatives for action (possible solutions).

Furthermore, policies may be tackling one single-hazard or single-asset, or even a part of these. The governance system of the country has an important effect on the final policies that will be drafted, and how these will be transformed in to programs, procedures or regulations for its implementation. These are commonly assigned to different groups. Here what it may be critical is ensuring a framework or mechanisms in place that exploits synergies and tries to avoid overlapping, conflict and omissions.

In order to ensure that the consequences of the law or regulation are duly considered, institutions may perform an impact assessment (IA) covering economic, social and environmental possible consequences. The EC (2017) recommends considering that the regulation/law produced is non-overlapping and consistent with other regulations covering the policy area, in order to reduce the negative consequences and burden to the different stakeholders that would apply it.

Ministerial bureaucracy and civil servants play an important role in policy formulation together with other actors through formal and informal discussions, in a complex social process (Sidney, 2007). The Guide to Policy Analysis (ETF, 2018) explains that framing and understanding the problem is followed by evidence collection (based on its availability, relevance and reliability) and analyses, so the problem is properly interpreted and updated. Here, the information and insights collected during the identification and analysis of risk are a direct input.

The investigation of policy alternatives is not easy, and different groups take part and assist decision-makers in selecting a preferred course of action. Therefore, choices should be well documented and explained, considering the uncertain or ambiguous conditions.

The chosen option(s), based on the resources at hand, the priorities of the country and other criteria established, would be described, assigned to institutions to implement them, and plan the main steps to follow. There should be reporting and evaluation procedure.

Like for the risk assessment, this step would require engaging different groups and stakeholders. At the same time, policy needs have to count on citizens participation as well as contribution.

When decisions for planning are made the process continuous into **the implementation phase** involving the institutions and group in charge, with the aim of reaching the goals and objectives set by the policy decision. Because the policies may be broad, administrative agencies are often delegated with the issue, structuring the policy and making it more specific. Therefore, the measures are usually planned in detail the form of plans or projects, in order to consider well the context.

During implementation, an idea (policy) is transformed into behaviour, expressed in social action (Paudel, 2009). Literature shows that there are traditionally two approaches in obtaining outputs based on the policy formulated: top-down and bottom-up (O'Toole, 2000; Paudel, 2009). Although recognized as critical, research does not agree in an ideal implementation process and stresses the idea that implementation strategy is very much contextual that it is useless to propose a unique strategy for any kind of topic (Matland, 1995). Nonetheless, four big activities could be considered based on Meyers et al. (2012):

1. Initial considerations

2. Creating a structure for implementation
3. Ongoing implementation support strategies
4. Learning from experience

The first two are part of the stage "planning measures", including:

- Conducting a study of the measures to be implemented, based on the needs, resources and capacities in place.
- Developing a plan for implementation (responsibilities, processes, objectives, etc.)
- Recruiting staff and planning capacity building strategies.

During the actual implementation stage, two elements emerge as critical: communication among teams and feedback mechanism, to evaluate the activities and allocate the resources, administrative mechanisms, and assistance needed (in-service training or coaching for example) (Fixsen et al., 2005; Fixsen et al. 2009, Meyers et al, 2012). Besides these, Gunn (1978) lists common obstacles that make implementation fail:

- constraining external circumstances,
- inadequate time and insufficient resources available,
- the relationship between cause and effects sought is not valid or indirect, and there are multiple intervening links,
- there is poor agreement on the objectives to reach, or even disagreement,
- tasks are not clearly specified and effectively planned,
- the agencies are unable to demand or obtain compliance.

It should be stated what resources are needed (budget, personnel, supplies, etc.) to complete the actions, with defined timelines. The measures implemented are simply outputs, so from that moment on, there should be resources planned to collect data systematically to review if the outcomes and impacts were achieved. These should have been built in the planning process.

DeGroff and Cargo (2009) present three factors that affect implementation processes that should be considered in the evaluation of the DR policy-making process.

- The need for coordination across multiple organizational actors and implementers. In that sense,
- Socio-political aspects and the democratic turn.
- The achievement of outcomes, and not just outputs.

Financial resources should be planned and available to ensure that every step counts with the relevant capacities in place and ready to be engaged in any step of the policy cycle described.

The system should be adaptive and try to learn from taken actions, so monitoring/evaluation must be tackled for each of the three DRM policy cycle steps, considering the different types of knowledge and in particular the "practical" one that can serve policy-makers and practitioners (Sanderson, 2010).

In the case of the NRA, the outputs and also the limitations should be made available to the public, as they can use that information in their daily activities. Either the institutions engaged or any other research organization may fund projects and policies for future risk assessments to be more robust and complete.

Finally, we would like to touch upon some **limitation of the suggested framework**. We are aware that scientific input is one of many, so policies would be "evidence-influenced" or "evidence-aware", as said by Nutley et al. (2002). With this in mind:

- Agenda setting is a trigger of risk assessment but also of the formulation of policies and the implementation of actions.
- Stakeholders participation and engagement is expected in many of the stages of the Framework presented.



### 4.3.2 Identifying the capabilities

To set up a structure described in Chapter 4.3 there are many dimension of capabilities required. UCPM (Decision No 1313/2013/EU) defines risk management capabilities in terms of **administrative, technical, and financial capacities** relevant for each phase of the policy cycle (**Table 3**).

However, administrative and financial capacities are more cross-cutting capacities that are relevant for different phases of policy cycle and are not associated with one particular sector or theme. They are the management capacities needed to formulate, implement and review policies, strategies, programmes and projects. In UNDP (2008a) Capacity Assessment framework they were identified as capacity to:

- assess a situation and define a vision and mandate;
- formulate policies and strategies;
- engage stakeholders;
- budget, manage and implement; and
- evaluate.

While technical capacities are those associated with particular areas of expertise and practice in specific sectors or thematic areas. When thinking about implementation of integrated DRM the technical capacities are climate change adaptation measures, critical infrastructure protection measure, loss data collection and procedures, conducting risk assessment, operating early warning systems, cross border issues etc., depending on the phase of policy cycle addressed. The challenge is how to promote focus on administrative and financial capacities which are essential to develop and maintain technical capacities.

**Table 3:** Dimensions of capability applicable to different capacities in different phases of DRM policy cycle

<b>Administrative capacities</b>	Capacity to assess a situation and define a vision and mandate
	Capacity to formulate policies and strategies
	Capacity to engage stakeholders
	Capacity to learn and improve
<b>Technical capacities</b>	Expertise
	Data
	Methodologies
	Equipment and technical systems
<b>Financial capacities</b>	Capacity to budget
	Capacity to manage and implement

Source: Authors

Furthermore, different capacities belong to different levels, such as **enabling environment, organizational and individual level** (UNDP, 2008), which makes it clear whose capacities are addressed. Capacities at the level of the enabling environment relate to policies, legislation, institutional arrangements, leadership, political processes and power relations and social norms (values, incentives, motivation, trust, legitimacy, transparency) which govern the mandates, priorities, modes of operation and civil engagement across different parts of society. The organizational level of capacity comprises the internal policies, arrangements, procedures and frameworks that allow an organization (in this case, institution engaged in DRM) to operate and deliver on its mandate, and that enable the coming together of individual capacities to work together and achieve goals. The individual level capacities are the skills and knowledge that are invested in people.

Eventually, there are four areas of potential improvement of each capacity which eventually define the scope of capability assessment and drive a capacity development: **institutional strengthening and development, leadership, knowledge and accountability** (UNDP, 2008). They are also the core issues of evidence base policy cycle which whole DRM cycle can be considered to be. Not all the aspects are equally relevant for all the capacities.

#### 4.4 Risk Management Assessment methodology

Capability assessment requires a lot of effort from the Member States. Therefore it is important:

- to **be concisely designed** to reflect the development priorities as articulated in the development strategies of a country combined with the identified list of critical capabilities that would need to be developed.
- to **be conducted** at national and subnational level with involvement of the main actors
- to **be focused** on key risks and sectors to be protected or maybe even a sequence of exercises with different focus can be established.
- to **be able to summarize the results** to be useful for decision making in capability development: to compare the level desired capacity against the level of existing capacity, to pinpoint the strengths and weaknesses and see where to focus future activities, provides information for setting realistic goals and helps planning the next steps as well as tracks the progress if the results are comparable over time by providing a common template and a ranking scheme.

Techniques to obtain the necessary data & information include semi-structured and one-on-one interviews, questionnaires, focus groups, client satisfaction surveys and scorecards, workshops, case studies and self-assessment instruments.

**Self-assessment questionnaire** such as Risk Management Capability Assessment Guidelines (Commission Notice, 2015) is a good example of structured and analytical approach to reach the objectives (Chapter 4.1) of the process. However, maybe too broad for the EU reporting purposes. It provides a common template and ranking scheme, demonstrates some desired capabilities for DRM policy cycle and gives information on direction of further improvements, creates positive learning mind-set of self-assessment process which is essential driver for the improvements of performance and also ensures that the process is driven from inside and owned by appointed actors and relevant stakeholders which guarantee the compilation of a feasible list of capacity development actions. Though the Guidelines are no longer used for the EU reporting purposes, they could still serve as a useful tool or an inspiration guiding national risk management capability assessment processes.

**Questions should be limited and still preserve the structure of the capability needs for DRM policy cycle.** This would require a further discussion on which capabilities are crucial for capacity developments and maybe, if necessary, narrow down the scope of the capability assessment or to establish a sequence of exercises with different focus to address the different aspects in a more detailed and concrete manner.

**A capacity assessment should ideally generate a quantitative ranking of capability and qualitative information to support the ranking. Both information are needed for the formulation of appropriate capability development responses.**

In case of **quantitative approach**, a ranking scheme needs to be designed to determine the level of desired capability and assess the level of existing capability. It should provide enough stages in the development of the capacity to support capacity development with feasible goals when moving to the next levels. For example (adapted from UNDP, 2008):

- **n/a** - capacity not considered applicable to be developed,
- **0** - capacity not considered to be developed,
- **1** - capacity considered applicable — work has not yet started – strategy/policy in place,
- **2** - Anecdotal evidence of capacity - initial progress achieved – pilot projects to be detected,

- **3** - Partially developed capacity – not covering fully any of the dimensions but mechanism is developed and it is functional,
- **4** - Widespread, but not comprehensive, evidence of capacity – covering fully at least one dimension mentioned above,
- **5** - Fully developed capacity and being improved.

It is very **useful to introduce rubrics** into ranking schema. Rubrics are a set of criteria to assess the level of existing capacity. Rubrics

- are recognized to ensure higher level of objectivity because they communicate the expectations directly, clearly and concisely.
- demonstrate the development response because they describe the stages in the development.
- provide, to be most effective, comparability over time and follow the progress towards the future needs.
- can even take over the role of the explanation of the question.

An example for a ranking schema with rubrics is shown in **Table 4**. Within the rubric for each ranking the level of development for different capacities, administrative, technical or financial are described.

**Table 4:** Possible rubrics for Loss data collection and reporting capability

Ranking schema supported with rubrics	Capacity not considered applicable to be developed	Capacity not considered to be developed	Capacity considered applicable — work has not yet started	Anecdotal evidence of capacity - initial progress achieved	Partially developed capacity	Widespread, but not comprehensive, evidence of capacity	Fully developed capacity and being improved
<b>Criteria</b> <b>Are methods for damage and human loss reporting developed and are the costs of the damages estimated, documented and stored?</b>	n/a	0 There is no evidence of loss database because it has not been considered to be developed	1 There are legal or procedural mechanisms in place: mandated organization is identified. funds are reserved for that. Coordination among sectors and institutions is identified	2 Loss data model developed, triggering mechanism identified, assessment techniques determined. Personnel trained to collect, understand and use data	3 Loss Data collection in place for some hazards. Relevant sectors and institutions involved,	4 Multi-hazard databases exist and are ready for use: the information management system developed and maintained, data collected, processed and aggregated	5 Damages are regularly documented and stored for all type of hazards, the reports are made available to the public
<b>Explanation</b>	Describe which methods for damage and human loss reporting are developed, if this data is shared with stakeholders and citizens, if stakeholders contribute to the damage reporting and/or to the estimation of costs, if the damages are regularly or occasionally documented and stored, what time period is covered and if these reports are made available to the public.						

Source: Authors

**Qualitative information are important to justify the selected ranking as well as to identify good practices and being able to assess their feasibility to be applied elsewhere.** The information provided should cover a broad range of aspects such as:

- description of the capacities with all the strengths, attributes and resources in place
- the contextual information within such a capacity would provide expected results
- the gap that it meant to close,
- the most difficult challenges that had to be overcome to get the capacity in place,
- the efforts related to further development and maintenance.

**The downside of self-assessment questionnaires are strong generalization of the findings and high level of subjectivity.**

Due to the complexity of the DRM policy cycle (covering different risks, entities at local to national levels, involving different sectors and stakeholders) some questions **requires strong generalization of the findings**. Ideally the consensus in scores should be achieved through participatory dialogue and information sharing which might not be always feasible. However, when possible generalization should be replaced by aggregation and it should be clear along which dimension has been done or was asked for when providing the score. For the way forward we should know which dimensions are the weakest in covering the issue. In the case of DRM cycle possible dimensions are

- **by hazard:** multi-hazard should refer to comprehensive set of natural and man-made (unintentional, e.g., technological and intentional, e.g., terrorist attacks) hazard;
- **by sectors:** cross-sectorial dimension that covers all the sectors affected by the impacts;
- **by institutions:** ministries, agencies, local and subnational government;
- **by territorial levels:** national or subnational (i.e., regional and local); this is of major difference when comparing the system in place in countries of different sizes. It is often the case that subnational levels are independent from the national levels in terms of resources as well in terms of strategies.
- **by stakeholders:** education and research institutions, private sector (insurance companies) and professional organizations, nongovernmental and civil-society organizations, media, households and individuals;
- **by DRM phases:** adaptation, mitigation, prevention, preparedness, response, impact assessment, recovery, restoration;
- **by DRM policy cycle:** risk assessment, planning, implementation;

Furthermore, the same ranking may be interpreted differently by different people. These individual perceptions are influenced by many factors. Such **a high level of subjectivity** might be acceptable in the self-assessment process if not too many actors are involved. Otherwise it might endanger the comparability of the result over time and the tracking of the process if the justifications of the scores are not properly documented.

## **4.5 Key messages**

**Risk management capability assessment is a driver of sustainable development of capabilities for the implementation of the integrated DRM.**

The implementation of integrated disaster risk management requires many capabilities that country needs to develop. Capability development is an on-going process of change that takes place over time. The country can use risk management capability assessment as a GPS and compass of this development. Shortly, risk management capability assessment defines where the country is, which direction the country should go and what is a very next step to reach the desired goals aligned with the development strategies. Therefore, risk

management capability assessment should be regular, focused, nationally owned and led. If these desired capabilities are not defined properly and in advance, the capability assessment is of limited use in designing the solution.

**Risk management capability assessment is holistic. It covers the whole DRM policy cycle and as such can facilitate from the beginning to the end the implementation of the measures in different phases of disaster risk management for different hazard**

Risk management capability assessment raises an awareness of complexity of the process of implementation of integrated DRM. RMCA addresses different hazards, risks and sectors, different phases of policy cycle, different stages of integrated DRM, involving different actors from local to national entities, private and public. Capacity issues are multi-dimensional and complex in nature, they can be cross-cutting or specific to particular sector, hazard, or other thematic area. Capability development along different dimension has a different pace of change over the time, sometimes dependent or independent among each other. For the way forward RMCA should discover the level of development along different dimensions, identify the weakest one as well as discover good practices that can be transferred into other dimensions.

**With a regular risk management capability assessment there is an opportunity to continuously adapt to changing risk landscape as well as development strategies with relevant capabilities.**

Capability development is an organic process of growth and development involving experimentation and learning as it proceeds. Flexibility to change a direction and adaptability to new goals are two essential features of on-going process dependent on existing and new evidences as well as governance structure dependent on people and local context. New evidences improve the understanding of key risks and risk drivers that suggest a need of different capabilities while risk governance that usually works in one society might not in other and as such is sensitive to societal and economic changes.

Furthermore, the key risks can change over time due to different reasons. One could define key risks those materializing with higher frequency (even if with low/relatively low impact) and to address them as first priority. Or one could define that key risks are those emerging risks because new capacities need to be developed to properly address them. One could as well consider that key risks are those classified as high impact low probability considering the possibility to reduce even more their probability after accurate analysis of them.

Any approach is valid but the most valuable one would consist on a wise combination of them. One possibility would be to adopt a consecutive and gradual approach consisting in addressing first those risks having more developed capacities and taking stoke from the expertise to move them to more complex situations.

**The implementation of integrated DRM is seen as evidence-based policy cycle.**

A policy cycle approach defines the level of importance that integrated DRM has for the safety and security of the country. It demonstrates the enhanced risk culture that covers the mind-sets and behaviors of national authorities. Based on evidence provided through NRA process a shared understanding is fostered of key risks and risk management with national leaders acting as role models followed by subnational and local institutions.

### 5 Linking the NRA and RMCA

**RMCA covers the policy cycle for the implementation of integrated disaster risk management that places NRA as an essential part of disaster risk reduction strategy realized through the integrated DRM approach.**

**Risk assessment (Chapter 3)** produces the "evidence" that would serve for planning and implementation phase (**Figure 5**) and as such represents a core of evidence-based policy-making which adds to successful implementation of effective and efficient integrated disaster risk management.

With other words, the policy cycle for the implementation of integrated disaster risk management is a mechanism that fill the gaps revealed in NRA process with the DRM actions in place.

Therefore it is important to prioritize the development of national risk assessment capability to improve the country's resilience against the disaster risk.

**Risk management capability assessment (Chapter 4)** covers the administrative, technical and financial capacity (Commission Notice, 2015; Decision No 1313/2013/EU) to carry out national risk assessment (**Table 5**).

**Figure 5:** The interaction between the policy cycle covered by RMCA and the integrated DRM



Source: Authors

**Table 5:** Conceptual framework for capability needs of the risk assessment phase

RISK ASSESSMENT		
Administrative	<b>Capacity to assess a situation and define a vision and mandate</b>	<p>There is a framework in place for new actors and actions to be carried in order to cover new needs</p> <p>Institutions have the mandate to learn and adopt suitable changes based on the evaluation of the NRA process</p>
	<b>Capacity to formulate policies and strategies</b>	<p>There is a legal and/or procedural framework in place with the main objectives of the NRA and its expected outputs, linking these with the planning of DRM measures. The framework serves to coordinate relevant entities to be engaged in the NRA</p>
	<b>Capacity to engage stakeholders</b>	<p>The legal and/or procedural framework for the NRA exercise establishes actions to engage stakeholders and integrate their insight.</p> <p>Outputs of the NRA are adequately and periodically communicated to citizens.</p>
	<b>Capacity to learn and improve</b>	<p>The participants of the NRA are trained in the uses and possibilities of the exercise</p> <p>The NRA exercise is carried out periodically to update the DR situation</p> <p>The NRA outputs and process are evaluated; gaps are linked with research strategies.</p>
Technical	<b>Expertise</b>	<p>Relevant entities (with relevant knowledge) are engaged in the NRAs</p> <p>Experts from relevant sectors and disciplines are engaged in the exercise</p>
	<b>Data</b>	<p>Loss data are used in risk identification and risk analysis</p> <p>Risk identification and risk analysis are carried out based on hazard projections and projected changes and data about the drivers of risk.</p> <p>If new data is required for the NRA, it is studied its feasibility to be obtained or collected.</p>
	<b>Methodologies</b>	<p>The approach of the NRA exercise is multi-sectorial and multi-hazard, trying to consider cascading events.</p> <p>Risk is calculated for common list of assets, so results of different scenarios are comparable (critical infrastructures being one of these).</p> <p>Risk identification and Risk analysis considers the cross-border nature of hazards and their effects.</p> <p>There is a set of criteria agreed to prioritise and discard risk.</p>
	<b>Equipment and technical systems</b>	<p>The participants carrying out the NRA have the required ICT equipment.</p>
Financial	<b>Capacity to budget</b>	<p>Different sources of financing are identified and mobilized for enough and timely funds to be available for the NRA exercise.</p>
	<b>Capacity to manage and implement</b>	<p>The process methodology of the NRA is structured and stated in a document, indicating objectives, competences required and intermediate and final outputs. This information is communicated to all participants.</p> <p>The main conclusions and results of the NRA are documented and communicated to different public authorities</p> <p>Different authorities (including if necessary, from neighborhood countries) and levels of governance are identified and engaged throughout the NRA process</p> <p>There is a leading agency for the NRA process, managing teams and resources.</p> <p>The NRA final report and overall methodology are disclosed to citizens (except restricted information).</p>

Source: Authors



The needs defined in **Table 5** covers also the capabilities (**Table 2**) addressed in Reporting Guidelines on Disaster Risk Management (Commission Notice, 2019). The national approach cannot be done anymore without considering also issues relevant to the EU as a whole. First, rare are the disasters that can be efficiently stopped at the border and, second, sometimes a common action can be the only one to manage their risk effectively.

## 6 Climate Change and Disaster Risk Management

The most recent PESETA<sup>35</sup> IV study (Feyen et al., 2020) concludes that climate change will induce a broad range of environmental and socio-economic impacts across Europe if not managed. However, there is a clear geographical north-south divide: countries in the south will be impacted more negatively by global warming compared with the northern parts of Europe. This is clearly the case for the effects on heat-related human mortality, water resources, habitat loss, energy demand for cooling and forest fires, where the Mediterranean area appears to be the most vulnerable to climate change.

Climate change will increase the disaster risk. It is one of the risk drivers linked to a rise of the average temperature at global level which is aggravating with time and will, therefore, tremendously affect (IPCC, 2014; Feyen et al., 2020) the future risk landscape. It is not only increasing the hazard, due to an increased frequency and severity of extreme events, but at the same time steadily increasing the vulnerability and decreasing the resilience of exposed population. Climate change is closely linked to a number of other risk drivers (e.g., poverty, urbanisation, environmental degradation, etc) and as such has become the most important link between international mechanisms: UNFCCC Paris Agreement, the Sendai Framework and the Sustainable Development Goals (SDGs).

Although transversal by nature, climate change has emerged as a sector in itself at the national, regional and international levels, with its own institutional arrangements, global framework, and funding mechanisms.

**The objective of this chapter is to show the synergies between the two processes; climate change adaptation (CCA) and disaster risk reduction strategies, with:**

1. presenting the EU Strategy on adaptation to climate change, the process how countries are encouraged to prepare their national climate change adaptation strategies and the Commission's further work towards its objectives,
2. explaining the opportunities where CCA strategies and DRM planning should complement and use adaptation and mitigation as one of the tools to reduce risk.

### 6.1 EU Strategy on adaptation to climate change

To make Europe more climate resilient, the European Commission adopted the EU Strategy on adaptation to climate change (COM/2013/0216) in April 2013. It sets out a framework and mechanisms to support three main priorities (**Box 3**).

#### **Box 3: EU Strategy on adaptation to climate change (COM/2013/0216)**

The EU Adaptation Strategy has three priorities.

Priority 1: Promoting action by Member States: helping countries to adopt their own adaptation strategies at national level and providing funding to help countries to take action, through the frames of LIFE funding and the commitments related to the Covenant of Mayors.

Priority 2: Promoting better informed decision-making: by bridging the gap in data and knowledge for action through the identification of gaps, reinforcing the interface between science, policy making and businesses; and improving the access to information and interaction with Climate-ADAPT and other relevant platforms.

Priority 3: Promoting adaptation in key vulnerable sectors: mainstreaming climate adaptation measures into EU policies and programs, and in particular in: Common Agricultural Policy (CAP), the Cohesion Policy and the Common Fisheries Policy (CFP); in the field of critical infrastructures; and facilitating the penetration of natural disaster insurance and other financial products for resilient investment and business decisions

The Commission encourages all Member States to adopt comprehensive adaptation strategies and provided guidance (SWD/2013/0134 final) and funding to help them build up their adaptation capacities and take action. The Commission published an evaluation of the strategy (SWD/2018/461 final) in November 2018. The analysis resulted in a report on lessons learned (COM/2018/738 final) and reflections on improvements for future action, accompanied by a staff working document (SWD/2018/461 final) presenting the evaluation in detail. Overall, the strategy has delivered on its objectives, with progress recorded against each of its eight

<sup>35</sup> PESETA is a series of research projects (PESETA-Projection of economic impacts of climate change in sectors of the European Union based on bottom-up analysis) led by the Joint Research Centre of the European Commission (JRC) focused on improving understanding of future implications and the costs of climate change specifically for the EU.

individual actions. As of today all Member States have their national adaptation strategy or plan<sup>36</sup>. The strategy has contributed to improve adaptation knowledge and to share it to inform decision-making. Through the strategy, adaptation has permeated and guided a wide range of the EU's own key policies and funding programmes, and reinforced links with disaster risk reduction, infrastructure resilience and the financial sector. The strategy has been a reference point to prepare Europe for the climate impacts to come, at all levels. The evaluation also suggests areas where more work needs to be done to prepare vulnerable regions and sectors.

**The evaluation of the strategy concluded that adaptation can and should be a powerful ally of sustainable development and disaster risk reduction efforts. EU policy must seek to create synergies among all those three policies, climate change adaptation, sustainable development and disaster risk reduction, to avoid future damage and provide for long-term economic and social welfare in Europe and in partner countries.**

Meanwhile, the new reporting requirements under the Governance of Energy Union and Climate Action (Regulation (EU) 2018/1999) have been put in place (**Box 4**) and asking Member States for regular reporting on their climate change adaptation activities.

**Box 4: Article 19(1) of Governance of Energy Union and Climate Action (Regulation (EU) 2018/1999)**

By 15 March 2021, and every two years thereafter, Member States shall report to the Commission information on their national climate change adaptation planning and strategies, outlining their implemented and planned actions to facilitate adaptation to climate change, including the information specified in Part 1 of Annex VIII and in accordance with the reporting requirements agreed upon under the UNFCCC and the Paris Agreement.

Part 1 of ANNEX VIII: [Member States'] Reporting on adaptation actions

Information to be included in the reports referred to in Article 19(1):

- (a) the main goals, objectives and institutional framework for adaptation;
- (b) climate change projections, including weather extremes, climate-change impacts, assessment of climate vulnerability and risks and key climate hazards;
- (c) adaptive capacity;
- (d) adaptation plans and strategies;
- (e) monitoring and evaluation framework;
- (f) progress made in implementation, including good practices and changes to governance.

In December 2019 Commission presented the **European Green Deal** (COM/2019/640), a plan for a transition of EU's economy for sustainable future. The Green Deal is a package of measures aiming to make Europe the world's first climate neutral continent by 2050, i.e. an economy with net-zero greenhouse gas emissions in line with the EU's commitment to global climate action under the Paris Agreement. Furthermore, on 29 January 2020 the European Commission published a new 2020 work programme with a European Green Deal under the first priority (COM/2020/37 final). The Programme was adjusted in May 2020 (COM/2020/440 final), as part of Europe's Recovery Plan (COM/2020/456 final) to the COVID-19 pandemic. The EU's recovery aims to guide and build a more sustainable, resilient and fairer Europe for the next generation. The green and digital transitions are considered even more important challenges after the COVID-19 crisis started.

Therefore, the Commission will adopt **a new and more ambitious strategy on adaptation to climate change** in the first quarter of 2021 based on the findings of evaluation. Pending on the forthcoming publication of the new strategy it can already be said that it will have the goal of stepping up action across society to increase climate resilience and adaptation to the unavoidable impacts of climate change (**Box 5**). The Strategy will be mainstreamed in many EU sectorial policies and initiatives, such as EU Biodiversity Strategy (COM/2020/380 final), the Farm to Fork Strategy (COM/2020/381) and the future Forest Strategy<sup>37</sup>.

<sup>36</sup> <https://climate-adapt.eea.europa.eu/countries-regions/countries>

<sup>37</sup> <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12674-Forests-new-EU-strategy>

**Box 5: The priorities of The New EU Strategy on Adaptation to Climate Change<sup>38</sup>:**

The New EU Adaptation Strategy has four priorities:

**Priority 1:** Improve knowledge of climate impacts and solutions;

**Priority 2:** Reinforce planning and climate risk assessment;

**Priority 3:** Accelerate adaptation action and

**Priority 4:** Strengthen climate resilience globally.

To conclude, European Commission proposed the **European Climate Law** (COM/2020/80) to reach the goals set in the European green Deal. The key elements are (1) a legally binding target of net zero greenhouse gas emissions by 2050, (2) measures to keep track of progress and adjust accordingly, and (3) necessary steps to get to the 2050 target. However, it will introduce also additional requirements for national climate change adaptation strategies that should include comprehensive risk management frameworks (**Box 6**).

**Box 6: Article 4 of the Commission's proposal for the first European Climate Law (COM/2020/80)**

Adaptation to climate change

1. The relevant Union institutions and the Member States shall ensure continuous progress in enhancing adaptive capacity, strengthening resilience and reducing vulnerability to climate change in accordance with Article 7 of the Paris Agreement.

2. Member States shall develop and implement adaptation strategies and plans that include comprehensive risk management frameworks, based on robust climate and vulnerability baselines and progress assessments.

## 6.2 Synergies among the two processes; CCA and DRR strategies

**Disaster risk governance structure (Chapter 4.1) should be robust and flexible to effectively acknowledge changes in risk landscape due to climate change, new knowledge and initiatives such as climate change adaptation strategies and efficiently consider adaptation measures during DRM planning.**

Reporting Guidelines on Disaster Risk Management (Commission Notice, 2019) is envisaging structural changes to risk governance approaches to allow acknowledging and introducing climate change related dynamic in risk management.

The European Commission advocates a horizontal coordination, i.e., a cross sectoral approach, among competent authorities related to different policy areas that may address or affect disaster prevention and taking due account of the likely impacts of climate change (e.g., Integration of climate change adaptation). Under the UN Framework Convention on Climate Change<sup>39</sup>, national adaptation strategies and plans are the recommended instrument for adaptation policies and actions. Reporting Guidelines on Disaster Risk Management (Commission Notice, 2019) ask Member States to take into consideration national and sub-national climate change adaptation strategies and/or action plans and describe if and how these are integrated with the planning of national disaster risk prevention and preparedness measures or vice-versa.

### National Risk Assessments are serving CCA and DRR purposes

Climate change adaptation strategy and disaster risk strategy are fundamentally very similar processes with the same goal. They are both trying to manage and reduce the risk of future disasters. They are following the same risk concepts (**Figure 6**) and risk assessment processes to gain evidence for further planning and implementation of risk reduction or adaptation measures, respectively.

National Adaptation Strategy should be part of the national risk assessment context and key climate change related future and emerging risks at national and subnational level that are consistent with the risks indicated

<sup>38</sup> Adaptation to Climate Change Blueprint for a new, more ambitious EU strategy.

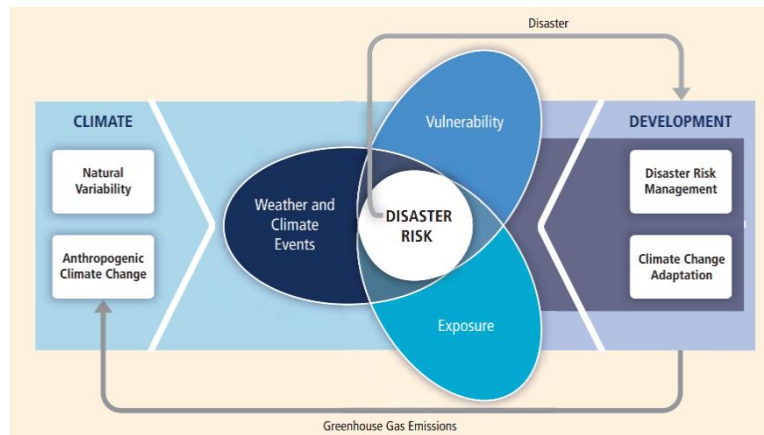
[https://ec.europa.eu/clima/sites/clima/files/consultations/docs/0037/blueprint\\_en.pdf](https://ec.europa.eu/clima/sites/clima/files/consultations/docs/0037/blueprint_en.pdf)

<sup>39</sup> <https://unfccc.int/topics/resilience/workstreams/national-adaptation-plans/overview>

in the National Adaptation Strategy should be put on the agenda of national risk assessment process (**Figure 2**).

Furthermore where appropriate, the risk identification should take into account of climate change projections and scenarios based on the Intergovernmental Panel on Climate Change (IPCC) reports, or on other validated scientific sources. Where existing, national climate risks and vulnerability assessments provide relevant projections of climate hazards and risks. The future climate scenarios used could be short-term (2030); medium-term (2050) and long-term (2100) knowing that short term scenarios tend to have a very large uncertainty.

**Figure 6:** The common risk concept involved in disaster risk management and climate change adaptation, and the interaction of these with sustainable development.



Source: IPCC, 2012

Risk analysis should look for new knowledge and the methods, models and techniques to capture the dynamic nature and various interactions of the risk-related processes driven by both climate change and social, economic, environmental and demographic parameters and to estimate the related uncertainties introduced.

Risk evaluation will then give more realistic and future looking estimation of how much action will be required to reduce risk to an acceptable level. Suggested risk treatment and its planning should follow integrated disaster risk management approach and using options in all phases of disaster risk management, where adaptation<sup>40</sup> and mitigation<sup>41</sup> actions are already considered to be part of it (**Figure 5**).

Because of aggravating effects of climate change many adaptation and other DRR measures might not be able to reduce the risk to the acceptable levels. Mitigation actions aimed at reducing the greenhouse gas emissions are inevitable (**Box 7**) and they require a global effort compared to many of the adaptation measures that are local by nature. NRA can raise awareness of the importance of the country's engagement at global platforms, forums and initiatives to support the mitigation actions in each and every country in the world. Models (IPCC, 2014b) are showing that risks are tremendously reduced using scenario with the lowest temperature projections (RCP2.6 – low emissions) compared to the highest temperature projections (RCP8.5 – high emissions). Therefore the overall risks of climate change impacts can be reduced by limiting the rate and magnitude of climate change which would also consequently lower the requirements for adaptation measures.

The on-going revisions of the UCPM legislation (COM/2020/220) includes a greater emphasis on the importance of addressing the impacts of climate change on disaster risk, highlights the need for a cross-sectoral approach and close coordination with climate change policies. It is also highlighting greater *synergies between disaster risk reduction and climate change adaptation measures*, with a strong emphasis on nature-based solutions that are established at national or sub-national level (as appropriate) for the identified key risks that are linked to climate change.

<sup>40</sup>[https://ec.europa.eu/info/horizon-europe/missions-horizon-europe/adaptation-climate-change-including-societal-transformation\\_en](https://ec.europa.eu/info/horizon-europe/missions-horizon-europe/adaptation-climate-change-including-societal-transformation_en)

<sup>41</sup> [https://ec.europa.eu/info/horizon-europe/missions-horizon-europe/climate-neutral-and-smart-cities\\_en](https://ec.europa.eu/info/horizon-europe/missions-horizon-europe/climate-neutral-and-smart-cities_en)

### Box 7: Adaptation to climate change impacts vs. mitigation of climate change (IPCC, 2014a)

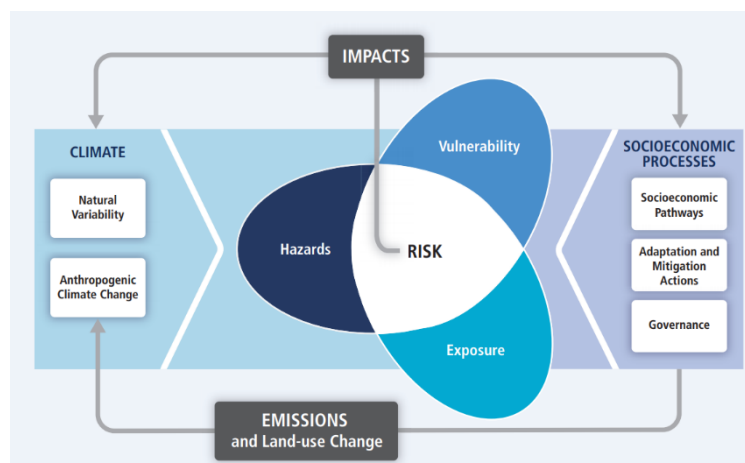
**Adaptation to climate change impacts:** The process of adjustment to actual or expected climate and its effects. In human systems, adaptation seeks to moderate or avoid harm or exploit beneficial opportunities. In some natural systems, human intervention may facilitate adjustment to expected climate and its effects.

**Mitigation of climate change:** A human intervention to reduce the sources or enhance the sinks of greenhouse gases (GHGs). IPCC Synthesis report (2014a) also assesses human interventions to reduce the sources of other substances which may contribute directly or indirectly to limiting climate change, including, for example, the reduction of particulate matter emissions that can directly alter the radiation balance (e.g., black carbon) or measures that control emissions of carbon monoxide, nitrogen oxides, Volatile Organic Compounds and other pollutants that can alter the concentration of tropospheric ozone which has an indirect effect on the climate.

### The synergies between DRR and CCA should go beyond weather and climate events and related risks

Assessment of weather and climate hazards and related risks is an area that has long stimulated the building of common grounds between CCA and DRR. The NRA has to utilize an approach which covers all hazards that the country is facing. However, climate change, when introduced in the disaster risk assessment, is influencing many risk drivers behind hazard, exposure (e.g., urbanisation) and vulnerability (e.g., poverty) dimension (**Figure 7**). The climate change has, therefore, much more far-reaching consequences in the field of disaster risk reduction including creation of new risks.

**Figure 7:** Risk of climate-related impacts results from changes in any of the dimensions of the risk concept due to the climate change: hazard, exposure or vulnerability of human and natural systems



Source: IPCC, 2014b

Many of these new risks are, on one side, related to the exposure and vulnerability of interlinked human-natural systems and how they behave in the light of socio-economic processes (e.g., socio economic pathways in **Box 8**), while others are related to a systemic and compound nature of risk since they are emerging in particular sector or are result of the cascading effects. Both aspects are still under-presented in risk assessment models while they can be slowly introduced in risk scenarios as much as understanding allows.

### Box 8: Shared socio-economic pathways

Socio-Economic Scenario<sup>42</sup> describes a possible future in terms of population, education, economic growth (GDP), urbanisation, inequality and other socio-economic factors up to 2100 relevant to understanding the implications of climate change. The latest generation of socioeconomic scenarios are based on the Shared Socio-Economic Pathways (SSPs) and are the result of the joint community effort over the last year. The pathways offer a systematic exploration of possible socioeconomic futures in terms of widely different predispositions to mitigate and adapt to climate change as well as facilitate the integrated, multidisciplinary analysis of future climate impacts.

**Figure B5:** The SSPs are based on five narratives and a set of driving forces (Riahi et al., 2017):

- **SSP1:** Sustainability (Taking the Green Road)
- **SSP2:** Middle of the Road
- **SSP3:** Regional Rivalry (A Rocky Road)
- **SSP4:** Inequality (A Road divided)
- **SSP5:** Fossil-fueled Development (Taking the Highway)

They are used to help produce the IPCC Sixth Assessment Report on climate change, due in 2021.



Source: [https://commons.wikimedia.org/wiki/File:Shared\\_Socioeconomic\\_Pathways.svg#metadata](https://commons.wikimedia.org/wiki/File:Shared_Socioeconomic_Pathways.svg#metadata)

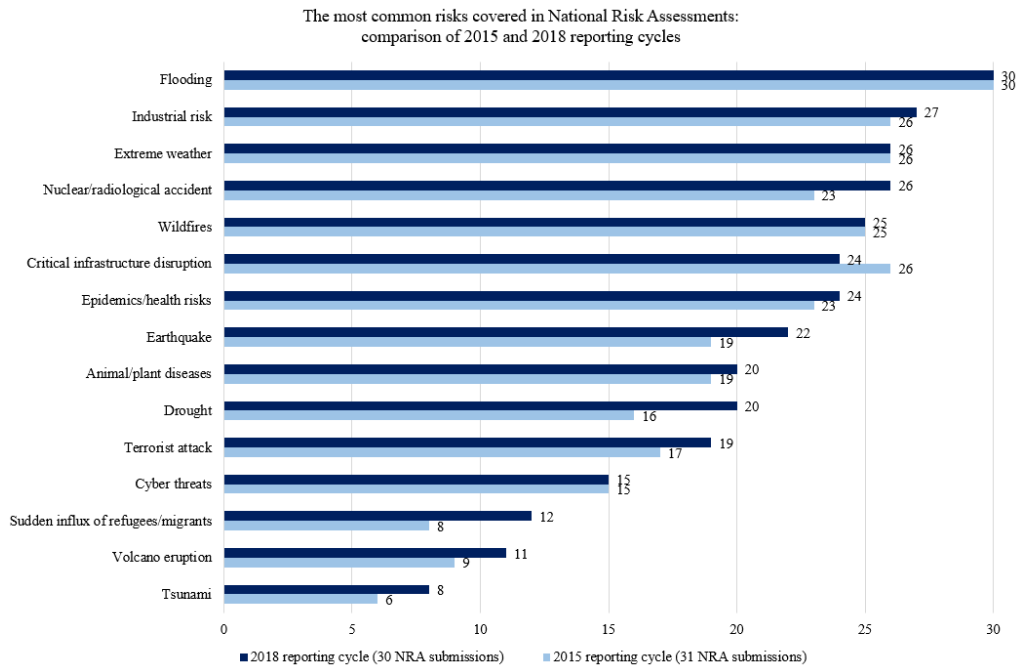
However, global SSPs would need revised versions for regional or local assessment, which is the so-called extended version, because global narratives may lack region-specific important drivers, national policy perspectives, and unification of data for each nation. Thus, it is necessary to construct scenarios that can be used for governments in response to the SSPs to reflect national and sub-national unique situations (Chen et al., 2020; Mitter et al., 2019).

<sup>42</sup> [https://www.ipcc-data.org/guidelines/pages/glossary/glossary\\_s.html](https://www.ipcc-data.org/guidelines/pages/glossary/glossary_s.html)

## 7 Introduction to contributions

Following the objectives of the Report, **fourteen teams** with expertise on specific hazards or assets prepared short contributions to describe approaches to be used in the context of a national risk assessment exercise. The teams also provided information on measures to manage the risk described and the areas in research that should be further developed.

**Figure 8:** The most common risks in national risk assessments (NRAs) in 2015 and 2018<sup>43</sup> reporting cycles



Source: Commission Staff Working Document, SWD(2020)330

The topics covered are:

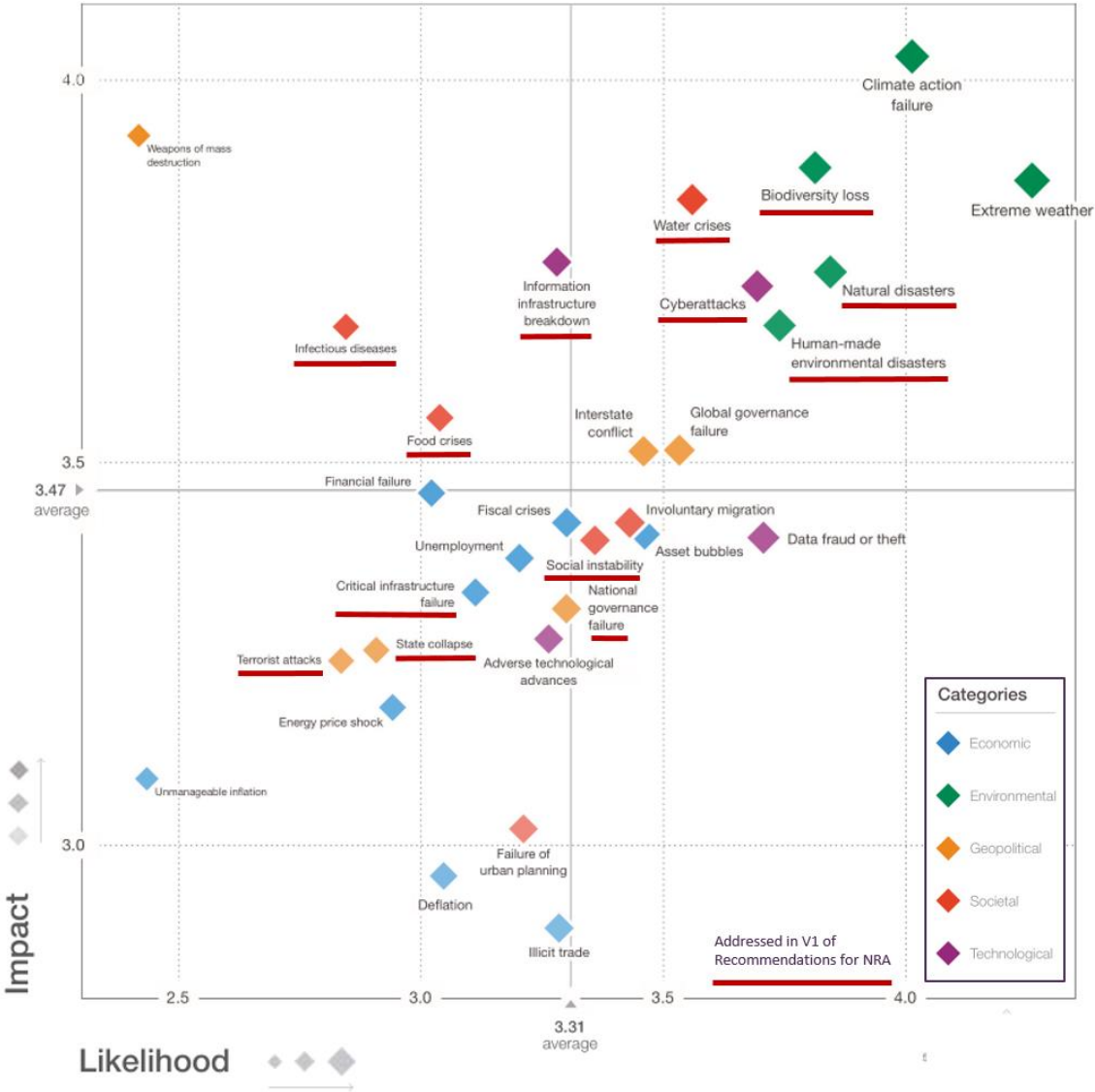
1. floods,
2. droughts,
3. wildfires
4. biodiversity loss
5. earthquakes,
6. volcano eruptions
7. biological disasters,
8. Natech accidents
9. chemical accidents
10. nuclear accidents
11. terrorist attacks,
12. critical infrastructure disruptions,
13. cybersecurity threats
14. hybrid threats

<sup>43</sup> In the 2018 reporting cycle, 26 EU Member States and 4 participating states to the Union Civil Protection Mechanism submitted summaries or full national risk assessments



This is not an exhaustive selection of risks and depending mainly on availability of experts to contribute. There are many other pertinent risks that would require consideration at the national level in EU (Figure 8), e.g., extreme weather, sudden influx of refugees and migrants, and tsunamis. Figure 8 also shows the comparison of national risk assessments shared with the Commission in 2015 and 2018 reporting where some risks are seeing increasing attention, such as geophysical risks (earthquakes, tsunamis and volcanic eruptions), drought, the risk of nuclear or radiological accidents, a sudden influx of refugees and migrants. However, many of risks covered in this report are one of the most relevant one according to Figure 9 that shows the overlapping with global perception of risk landscape based on the survey done by Global Risk Report<sup>44</sup>.

Figure 9: The global risk landscape 2020<sup>45</sup> with the risk addressed in this V1 of Recommendation for NRA



Source: Authors after World Economic Forum Global Risks Perception Survey 2019-2020

Authors were asked to

- structure the contributions in a harmonized way, as much as appropriate, and to follow ISO 31030 for the stages of the risk assessment process: risk identification, risk analysis and risk evaluation (Chapter 3.3).

<sup>44</sup> [http://www3.weforum.org/docs/WEF\\_Global\\_Risk\\_Report\\_2020.pdf](http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf)  
<sup>45</sup> World Economic Forum Global Risks Perception Survey 2019-2020

- follow the UNISDR terminology<sup>46</sup> regarding the risk concept.
- ensure that the content follows the EU guidelines on risk assessment and mapping (Commission Staff Working Paper, 2010)

Objective of the contributions is to explain disaster risk assessment approaches specific risk related to chosen hazard/asset step by step that are usable in national risk assessment exercise and useful for disaster risk management planning. The purpose is to maximize the national capacity of a country in achieving the objectives national risk assessment process. The objectives of (NRA) are to reach a common understanding with all relevant stakeholders, of the risks faced and their relative priority.

Risks related to different hazards as well as different assets require very different analysis of risk. The harmonisation of the risk assessment process has to remain at the level of terminology, data, risk concept, general steps and presentation of the results. For each field the experts provide more insightful guidance on:

- identifying the key risks in terms of what we should be afraid considering most exposed, most vulnerable and most important assets as well as indicating the EU policies that are related to them. For the purpose of NRA such assets or sectors are predefined due to importance they have for the security and well-being of society.
- using existing risk assessment methodologies, terminology used for their understanding, data, knowledge and software needed for the analysis
- what results can be expected for each of the methodologies aiming for quantifying risk with level of potential impacts with probabilities/likelihoods and whenever feasible providing risk metrics to make risks arising from different hazards/regions/assets comparable
- how to address climate change in risk assessment,
- how to identify disaster risk drivers to address a range of measure to reduce risk and link the results of the NRA with the following DRM planning For each hazard or asset related risk there are different solutions efficient in different phases of the DRM cycle often dependent on the nature of hazard, knowledge on hazard modelling, predictability and level of risk as well as cost of measures. Risk treatment is an iterative process of formulating and selecting risk treatment option, assessing the effectiveness of that treatment, deciding whether the remaining risks acceptable and if not looking for further options.
- on identifying capabilities needed for NRA fit for the purpose in the country (legal framework in place, relevant strategies, which networks and groups to involve to join technical team preparing risk assessment, i.e. different actors, stakeholders from relevant sectors to conduct risk assessment drawn on the knowledge and views of all involved, training, identifying research gaps, governance of data and loss database, ...)

---

<sup>46</sup> <https://www.unisdr.org/we/inform/terminology>

## **8 Main findings from contributions and conclusions**

### **8.1 Main findings from contributions**

From the scientific contributions the following findings have been extracted. They are not mutually exclusive, in fact, they are closely interlinked but they are found essential for risk assessment process. The findings presented are highly visible, on the other side, they are only a few of the many real problems:

#### **Availability and better quality risk and loss data**

The more information is available, the more realistically we can identify risks by different hazards and see which sectors are most affected by particular hazard. We can justify and advocate which risks should be put on agenda of national risk assessment. It facilitates preparation of more holistic risk scenarios that are taking into account the country's capacities and actions of different stakeholders on different phases of DRM. It is also an opportunity to introduce some aspects of compound risk, i.e., including the potential for considerable adverse consequences in different sectors or cascading effects, even though later analysed independently. Furthermore, more information supports a design of the whole range of scenarios, from more probable and low impact as well as less probable and high impact events.

Risk assessment models have a large demand of data for input parameters and results validation. Data are one of the major source of uncertainty in risk assessment analysis and one of the challenges is to improve the quality of data. In the past, the data needs were addressed in ad-hoc basis. However, the data cannot be automatically considered as a fact anymore. We need to know which data is gathered and how as well as whether the data is gathered the same way. The quality of data should be measured with the consistency and sustainability of data collection process and data management systems in place (e.g., disaster loss database, exposure data, inventory of species, European platform of risk data Risk Data Hub<sup>47</sup>, etc.).

#### **Improvement of risk assessment methodology used**

The main goal of the risk assessment is to assess the potential impacts and related probabilities of their occurrences. Therefore the experts strive to improve the models and reduce the uncertainties as well as move from qualitative, semi-quantitative to quantitative risk analysis.

The challenges differ among hazards and risks addressed. The fields of new emerging risks, such as hybrid threats and cybersecurity, are in the stage of developing the conceptual models which would be based on accepted risk concepts but are still mainly focused on vulnerability issues. While Natech, Critical Infrastructure and biodiversity loss fields that are by definition triggered by the impact of another hazard try to better understand these dependences and introduce them into the models as first attempts to deal with systemic risks. General requirement for the improvement of models are availability of better risk data (e.g., hazard occurrence, georeferenced exposure data, vulnerability of assets at the local level, vulnerability of population and economy, vulnerability of equipment) as well as loss data for better understanding of risk drivers to improve models and the validation of the models output. Considering the fact that models are only approximations to reality they are another source of uncertainty in risk assessment. Better understanding of risk reflects in more accurate mathematical models

On the other side, some models for probabilistic risk assessment might be rather complex to provide eventually better result. They require complicated software and highly qualified experts, with more data to process with time consuming algorithms. Such increasing complexity introduces numerical errors and numerical approximations and are another source of uncertainty (i.e., numerical uncertainty).

The selection of the method is still mainly dependent on knowledge and data availability, therefore the possibility of assessing the uncertainties is important and if possible being also a decisive factor as well as part of the reporting process.

However, the results of risk assessment should fit the purpose. Maybe, probabilistic risk assessment is not always needed when we just need a relative importance of risks arising from different hazard or an insight into main risk drivers. For example, some risks can be assessed with probabilistic methods while others are only possible to assess with semi-quantitative methods. In such cases, the results of probabilistic risk assessment probabilistic methods has to be "downgraded" to be comparable with the results of semi-quantitative methods.

---

<sup>47</sup> <https://drmkc.jrc.ec.europa.eu/risk-data-hub>

### **Better understanding of risk driver**

Understanding of risk drivers and how they affect the level of risk is important for the risk assessment models improvement but also to identify disaster risk reduction measures to act upon. Within integrated DRM we have to consider various drivers of risk and provide options of prevention and mitigation actions ranging from structural to non-structural measures as well as preparedness and response actions from early warning system to emergency management and risk transfer such as insurance.

In case of risks when advance risk assessment methods are already available, risk management strategies can be supported with cost-benefit analysis of risk management options to identify economically optimal options in the light of the acceptable risk levels and have evidence when to prevent/reduce damages pays-off managing the damages themselves

However, when we are still struggling to assess the risk identified in quantitative terms and the stakes are high, it is still important to know what options of reducing risks exist in different stages of disaster risk management and according to available knowledge implement the most effective ones, e.g. reduce vulnerability of the most important and/or exposed assets as much as we can, put efforts in early detection to respond better and if possible contain the damages in one system and prevent cascading events.

The important source of knowledge on mechanism between risk drivers and risk are lessons learned from the past experiences in the form of loss databases, accident investigations (e.g., multiform activities in nuclear fields), incident databases and post-disaster reports. These are opportunities for collaboration among scientists and practitioners, across disciplines and stakeholders and, above all, bidirectional exchange of knowledge gained through research on one side and through experiences on the other side.

In case of understanding climate change as a risk driver, it is becoming obvious that a collaboration among two big scientific communities, climate change adaptation and disaster risk reduction, is inevitable. Integrated disaster risk management should have capacity to integrate climate change adaptation strategies and efficiently consider adaptation measures during DRM planning.

### **Harmonization of risk metrics**

The harmonization of risk metric would allow the comparison of risks across hazards, regions, time, assets or sectors. These would allow aggregation of risks arising from the same hazard and understanding of relative importance of different risks for prioritization of DRM actions. It would establish a common understanding of risks that country is facing when consulting among each other. It would pave the way to the multi hazard risk assessment, introducing interactions and cascading effects in modelling as well as provide some analytical interpretations of compound and systemic risks.

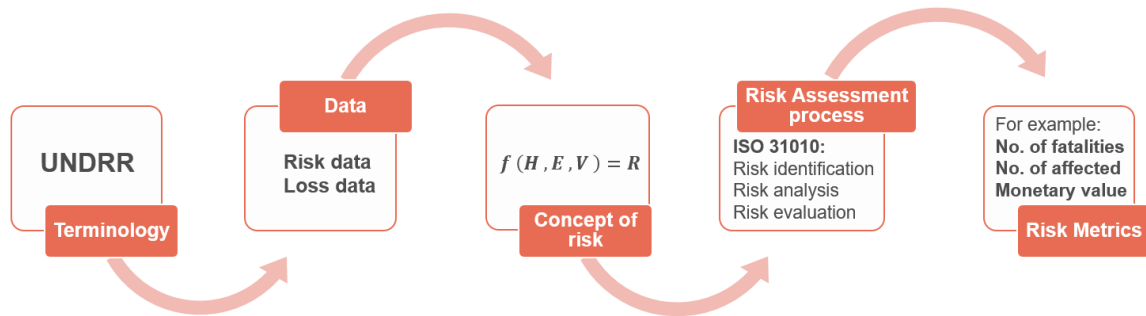
There is a long way from identifying and describing risk to measure it. Qualitative description is not reserved only for intangible impacts but also for the potential impacts of new and emergent risk (e.g., terrorist attacks, cybersecurity and hybrid threats) which is difficult to detect, address and especially measure. When quantitative description is available the metrics used is dependent on the asset affected and how it is affected. Final goal is to assign risk metrics that have its counterpart in loss indicators to compare the progress against the national goals as well as to validate risk models with loss data.

## **8.2 Overall conclusion**

**National risk assessment** is placed at the heart of the policy cycle to implement an integrated disaster risk management. NRA has an important role of providing evidence for though decision making process with many stakeholders involved. **Risk management capability assessment** aims to set up a risk governance structure that facilitates policy cycle from NRA, DRM planning to the implementation of prevention and preparedness measures. **NRA and RMCA** should be tailored to the national context and serve the specific national goals. The ultimate goal is to have less disasters and/or disaster with less impacts and increase the overall resilience.

Key issue in evidence based policy making is **comparability** of evidence. Comparability brings evidence to the next level. Harmonization is a process that increases comparability while respects particularities of the individual approaches and promotes working together on the areas that are complementary and focusing on common goals. It is important to get the harmonization right. Harmonization is introducing uniformity where needed in order to turn diversity into strength.

**Figure 10:** Harmonization of risk assessment process



Source: Authors

The harmonization of the risk assessment process has to remain (**Figure 10**) at the level of:

- terminology,
- data,
- risk concept,
- general steps of the risk assessment process and
- presentation of the results with the common risk metrics.

While different risks (different hazards, different assets) are affected by different risk drivers in a different way and, therefore, require very different analysis.

In 2009, EU started the initiative for an overall European approach to the prevention of disasters. It started with the sharing of risk information with the first reporting exercise taking place in 2013. The reporting process is **a summary of the national activities related to NRA and RMCA** that are relevant in the EU context and it is on a good way to reach its purpose. Information shared at EU level feeds into the EU policy-making and helps:

- to prepare and **improve guidelines as well as EU policies related to different risks** to tackle the harmonization challenge: within and among the countries;
- to **build common understanding of risk issues** relevant at cross-border, inter-regional and international level as well as facilitate the exchange of **good practices and lessons learned** to speed up the risk reduction processes thanks to the “*Overview of Risks that EU may face*” series of publications prepared by Commission based on the outcomes of the reporting process;
- to support formulating an EU prevention policy framework that would complement and enhance the national one and promoting better national risk governance with a legal framework and integrated disaster risk management approach;
- to have **a transparent approach** to allocate the resources among the countries.

Finally, at the national level it is important to focus on:

#### **Development of national risk assessment capability**

The policy cycle for the implementation of integrated disaster risk management is a mechanism that fill the gaps revealed in NRA process with the DRM actions in place. Therefore it is important to prioritize the development of national risk assessment capability to improve the country's resilience against the disaster risk.

#### **Regular risk management capability assessment**

Regular RMCA is a driver of sustainable development of capabilities for the implementation of the integrated DRM and also an opportunity to continuously adapt to changing risk landscape (i.e., climate change, new and emergent risks) as well as development strategies with relevant capabilities.

**Consider climate change adaptation strategies**

The policy cycle for the implementation of integrated disaster risk management should have capacity to integrate climate change adaptation strategies and efficiently consider adaptation measures during DRM planning.

## 9 References

- Abrahamsson, M. (2002). Uncertainty in Quantitative Risk Analysis – Characterisation and Methods of Treatment [Online]. Available: [portal.research.lu.se/portal/files/4448408/642162.pdf](http://portal.research.lu.se/portal/files/4448408/642162.pdf). [Accessed 09 08 2018].
- Alexander, D., 2000. Scenario methodology for teaching principles of emergency management. *Disaster Prevention and Management* 9(2): 89-97. Alexander, D. 2002. Principles of Emergency Planning and Management. Oxford University Press, New York, 365 pp.
- Antofie, T, E., Luoni, S., Faiella, A., Marin Ferrer, M., Risk Data Hub – web platform to facilitate management of disaster risks, EUR 29700 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-01385-3, doi:10.2760/68372, PUBSY No. JRC114120.
- Apostolakis, G.E. (2004). How useful is quantitative risk assessment?, *Risk Analysis*, 24(3), pp. 515-520.
- Aven, T., and Renn, O. 2009. The Role of Quantitative Risk Assessments for Characterizing Risk and Uncertainty and Delineating Appropriate Risk Management Options, with Special Emphasis on Terrorism Risk. *Risk Analysis*, 29(4): 587-600
- CADRI, 2011. Basics of capacity development for disaster risk reduction. Capacity for Disaster Reduction Initiative.
- Chen, H., Matsushashi, K., Takahashi, K. et al. Adapting global shared socio-economic pathways for national scenarios in Japan. *Sustain Sci* 15, 985–1000 (2020). <https://doi.org/10.1007/s11625-019-00780-y>
- Cirella, G.T., Semenzin, E., Critto, A. and Marcomini, A., Natural hazard Risk Assessment and Management Methodologies Review: Europe, In: Linkov, I (ed.), Sustainable Cities and Military Installations: climate change impacts on energy and environmental security, pp 329-358.
- COM/2006/0786 final, Communication from the Commission on a European Programme for Critical Infrastructure Protection
- COM/2009/82 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Community approach on the prevention of natural and man-made disasters, 23.2.2009
- COM/2009/84 final, Communication from the Commission to the Council and the European Parliament: EU strategy for supporting disaster risk reduction in developing countries, 23.2.2009.
- COM/2010/600 final, Communication from the Commission to the European Parliament and the Council: Towards a stronger European disaster response: the role of civil protection and humanitarian assistance  
COM/2010/600 final, 26.10.2010
- COM/2013/0216 final. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS An EU Strategy on adaptation to climate change
- COM/2018/738 final. REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of the EU Strategy on adaptation to climate change.
- COM/2019/640 final. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS The European Green Deal
- COM/2020/220 final. Proposal for a DECISION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism
- COM/2020/37 final. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Commission Work Programme 2020 A Union that strives for more
- COM/2020/380 final. EU Biodiversity Strategy for 2030, from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions
- COM/2020/381 final. Farm to Fork Strategy, from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.

COM/2020/440 final. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Adjusted Commission Work Programme 2020

COM/2020/456 final. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Europe's moment: Repair and Prepare for the Next Generation

COM/2020/80 final. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the framework for achieving climate neutrality and amending Regulation (EU) 2018/1999 (European Climate Law)

COM/2021/35 final. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. A united front to beat COVID-19. 19 January 2021. EC: Brussels; 2021. Available from: [https://ec.europa.eu/info/sites/info/files/communication-united-frontbeat-covid-19\\_en.pdf](https://ec.europa.eu/info/sites/info/files/communication-united-frontbeat-covid-19_en.pdf)

Commission notice, 2015. Risk Management Capability Assessment Guidelines. OJ C 261, 8.8.2015, p. 5–24

Commission Notice, 2019. Reporting Guidelines on Disaster Risk Management, Art. 6(1)d of Decision No 1313/2013/EU2019/C 428/07 C/2019/8929, OJ C 428, 20.12.2019, p. 8–33.

Commission Staff Working Document, 2014. Overview of natural and man-made disaster risks in the EU. SWD(2014)134 final, 8.4.2014.

Commission Staff Working Document, 2017. Overview of Natural and Man-made Disaster Risks the European Union may face. SWD(2017)176 final, 23.5.2017.

Commission Staff Working Document, 2020. Overview of Natural and Man-made Disaster Risks the European Union may face. SWD(2020)330 final, Brussels, 30.11.2020.

Commission Staff Working Paper, 2010. Risk Assessment and Mapping Guidelines for Disaster Management. SEC(2010)1626 final, 21.12.2010, p.24.

Council Conclusions on a Community framework on disaster prevention within the EU COUNCIL OF THE EUROPEAN UNION Brussels, 12 November 2009, 15394/09

Council Conclusions on Further Developing Risk Assessment for Disaster Management within the European Union 3081st JUSTICE and HOME AFFAIRS Council meeting Luxembourg, 11 and 12 April 2011.

Council Decision 2001/792/EC, Euratom of 23 October 2001 establishing a Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions (OJ L 297, 15.11.2001, p. 7)

Covello, V.T. and Merkhoher, M. W. (1993). Risk Assessment Methods, Plenum Press, New York.

Cox, L.A., Babayev, D. and Huber, W. (2005). Some Limitations of Qualitative Risk Rating Systems, Risk Analysis, 25(3), pp. 651-662.

Davies T., Beaven S., Conradson D., Densmore A., Gaillard JC, Johnston D, Milledge D., Owen K., Petley D., Rigg J., Robinson T., Rosser N., Wilson T., 2015. Towards disaster resilience: A scenario-based approach to co-producing and integrating hazard and risk knowledge. International Journal of Disaster Risk Reduction 13, 242-247.

De Groeve, T., Poljansek, K., Ehrlich, D., 2013. Recording Disaster Losses: Recommendations for a European approach. Report by the Joint Research Centre of the European Commission 10/2013, doi: 10.2788/98653.

De Groeve, T., Poljansek, K., Ehrlich, D. and Corbane, C., 2014. Current status and best practices for disaster loss data recording in EU Member States, Publications Office of the European Union, Luxembourg.

Decision (EU) 2019/420 of the European Parliament and of the Council of 13 March 2019 amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism. PE/90/2018/REV/1. OJ L 771, 20.3.2019, p. 1–15.

Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism Text with EEA relevance. OJ L 347, 20.12.2013, pp. 924–947.

DeGroff, A., & Cargo, M. (2009). Policy implementation: Implications for evaluation. In J. M. Ottoson & P. Hawe (Eds.), Knowledge utilization, diffusion, implementation, transfer, and translation: Implications for evaluation. New Directions for Evaluation, 124, 47–60.



- EEA, 2017. Climate change adaptation and disaster risk reduction in Europe – Enhancing coherence of the knowledge base, policies and practices, European Environment Agency, No. 15/2017, ISBN: 978-92-9213-893-6
- EEA, 2018. National climate change vulnerability and risk assessments in Europe. European Environment Agency, No. 1/2018, ISSN 1977-8449
- ETF – European Training Foundation. 2018. Guide to Policy Analysis. TA-04-18-136-EN-N. [https://www.etf.europa.eu/sites/default/files/m/72B7424E26ADE1AFC12582520051E25E\\_Guide%20to%20policy%20analysis.pdf](https://www.etf.europa.eu/sites/default/files/m/72B7424E26ADE1AFC12582520051E25E_Guide%20to%20policy%20analysis.pdf)
- European Centre for Disease Prevention and Control. Overview of the implementation of COVID-19 vaccination strategies and vaccine deployment plans in the EU/EEA – 1 February 2021. ECDC: Stockholm; 2021.
- European Commission. 2017a. Quality of Public Administration: A Toolbox for Practitioners. Theme 1: Policy-making, implementation and innovation. Publications Office of the European Union, Luxembourg.
- FAO. 2004. Capacity development in irrigation and drainage issues, challenges and the way ahead.
- Feyen L., Ciscar J.C., Gosling S., Ibarreta D., Soria A. (editors) (2020). Climate change impacts and adaptation in Europe. JRC PESETA IV final report. EUR 30180EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-18123-1, doi:10.2760/171121, JRC119178.
- Fischhoff, B., Lichtenstein, S., Slovic, P., Keeney, R., and Derby, S., 1980. Approaches to Acceptable Risk: A Critical Guide (NUREG/CR-1614). Oak Ridge, Tennessee: Oak Ridge National Laboratories.
- Fixsen, Dean L., Karen A. Blase, Sandra F. Naoom, and Frances Wallace. 2009. Core Implementation Components. *Research on Social Work Practice* 19 (5): 531–40.
- Fixsen, Dean L., Sandra F. Naoom, Karen A. Blase, and Robert M. Friedman. 2005. “
- Frey, H.C. and Patil, S.R. (2003). Identification and review of sensitivity analysis methods. *Risk Analysis*, 22(3), 553-578.
- GAR, 2019. Chapter 2: Systemic risks, the Sendai Framework and the 2030 Agenda.
- Gunn LA (1978) Why is implementation so difficult? *Management Services in Government*, 33: 169-76.
- Haimes YY (2009) *Risk Modeling, Assessment, and Management*. 3rd Edition. John Wiley & Sons, 1009 p
- Howlett M (2012) The lessons of failure: Learning and blame avoidance in public policy-making. *International Political Science Review* 33(5): 539–555
- Howlett, M., & Ramesh M., (2003), *Studying Public Policy: Policy Cycles and Policy Subsystems*, Second Edition, Oxford University Press, Canada
- IPCC, 2012: Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation. A Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change [Field, C.B., V. Barros, T.F. Stocker, D. Qin, D.J. Dokken, K.L. Ebi, M.D. Mastrandrea, K.J. Mach, G.-K. Plattner, S.K. Allen, M. Tignor, and P.M. Midgley (eds.)]. Cambridge University Press, Cambridge, UK, and New York, NY, USA, 582 pp
- IPCC, 2014a. Climate Change 2014: Synthesis Report. Contribution of Working Groups I, II and III to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change [Core Writing Team, R.K. Pachauri and L.A. Meyer (eds.)]. IPCC, Geneva, Switzerland, 151 pp.
- IPCC, 2014b, Climate change 2014 — Impacts, adaptation, and vulnerability. Part A — Global and sectoral aspects. Contribution of Working Group II to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change, Cambridge University Press, Cambridge, UK.
- ISDR, 2007. Hyogo Framework for Action 2005-2015: Building the Resilience of Nations and Communities to Disasters, International Strategy for Disaster Reduction.
- Jansen, T., Claassen, L., van Poll, R., van Kamp, I. and Timmermans, D. R.(2017). Breaking down uncertain risks for risk communication: a conceptual review of the environmental health communication, *Risk, hazards & crisis in public policy*, 9(1), pp. 4 - 38.
- Mannan, S. (2012). *Lees' Loss Prevention in the Process Industries (Fourth Edition)*, Woburn, United States: Elsevier - Health Sciences Division.

- Matland, R.E., 1995. "Synthesizing the Implementation Literature: The Ambiguity Conflict Model of Policy Implementation. *Journal of Public Administration Research and Theory* 5 (2): 145-174.
- Mechler, R., Bouwer, L., Linnerooth-Bayer, J. et al. Managing unnatural disaster risk from climate extremes. *Nature Clim Change* 4, 235–237 (2014). <https://doi.org/10.1038/nclimate2137>
- Mercer J., 2012. Knowledge and disaster risk reduction. B. Wisner, J.C. Gaillard, I. Kelman (Eds.), *Handbook of Hazards and Disaster Risk Reduction*, Routledge, London (2012), pp. 97-108
- Meyer D.C., Durlak, J. A. and Wandersman, A. 2012. The Quality implementation Framework: a synthesis of Critical Steps in the implementation process
- Mitter, H., Techen, A., Sinabell, F., Helming, K., Kok, K., Priess, J., Schmid, E., Bodirsky, B., Holman, I., Lehtonen, H., Leip, A., Le Mouel, C., Mathijs, E., Mehdi, B., Michetti, M., Mittenzwei, K., Mora, O., Oygarden, L., Reidsma, P., Schaldach, R. and Schoenhart, M., A protocol to develop Shared Socio-economic Pathways for European agriculture, *JOURNAL OF ENVIRONMENTAL MANAGEMENT*, ISSN 0301-4797 (online), 252, 2019, p. 109701, JRC118279.
- Nutley, S., Davies, H. & Walter, I. 2002, Evidence based policy and practice: cross sector lessons from the UK, keynote paper for the Social Policy Research and Evaluation Conference, Wellington, New Zealand, 2–3 July.
- Onencan, A.M, Liu, L.E., van de Walle, B. 2020. Design for Societal Resilience: The Risk Evaluation Diversity-Aiding Approach (RED-A), *Sustainability* 12, 5461; doi:10.3390/su12135461.
- O'toole, L. J. 2000. Research on Policy Implementation: Assessment and Prospects. *Journal of Public Administration Research and Theory* 2: 263 – 288.  
<https://ris.utwente.nl/ws/files/7053582/J%20Public%20Adm%20Res%20Theory-2000-O'Toole-263-88.pdf>
- Paudel, N. R. (2009). A Critical Account of Policy Implementation Theories: Status and Reconsideration. *Nepalese J Public Policy*, 2:36–54.  
<https://pdfs.semanticscholar.org/96cb/1a5f553dfe89767763005fa65f474af8e6d3.pdf>
- Phimister, J. R., Oktem, U., Kleindorfer, P. R., and Kunreuther, H. (2003). Near-Miss Incident Management in the Chemical Process Industry, *Risk Analysis*, 23(3), 445- 459.
- Plattner, T. 2005. Modelling public risk evaluation of natural hazards: a conceptual approach. *Natural Hazards and Earth System Science*, Copernicus Publications on behalf of the European Geosciences Union, 2005, 5 (3), pp. 357-366.
- Poljanšek, K., Casajus Valles, A., Marin Ferrer, M., De Jager, A., Dottori, F., Galbusera, L., Garcia Puerta, B., Giannopoulos, G., Girgin, S., Hernandez Ceballos, M., Iurlaro, G., Karlos, V., Krausmann, E., Larcher, M., Lequarre, A., Theocharidou, M., Montero Prieto, M., Naumann, G., Necci, A., Salamon, P., Sangiorgi, M., Sousa, M. L., Trueba Alonso, C., Tsionis, G., Vogt, J., and Wood, M., 2019. Recommendations for National Risk Assessment for Disaster Risk Management in EU, EUR 29557 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-79-98366-5 (online), doi:10.2760/084707 (online), JRC114650.
- Regulation (EU) 2018/1999 of the European Parliament and of the Council of 11 December 2018 on the Governance of the Energy Union and Climate Action, amending Regulations (EC) No 663/2009 and (EC) No 715/2009 of the European Parliament and of the Council, Directives 94/22/EC, 98/70/EC, 2009/31/EC, 2009/73/EC, 2010/31/EU, 2012/27/EU and 2013/30/EU of the European Parliament and of the Council, Council Directives 2009/119/EC and (EU) 2015/652 and repealing Regulation (EU) No 525/2013 of the European Parliament and of the Council (Text with EEA relevance.). PE/55/2018/REV/1. OJ L 328, 21.12.2018, p. 1–77
- Regulation (EU) 2018/1999 of the European Parliament and of the Council of 11 December 2018 on the Governance of the Energy Union and Climate Action, amending Regulations (EC) No 663/2009 and (EC) No 715/2009 of the European Parliament and of the Council, Directives 94/22/EC, 98/70/EC, 2009/31/EC, 2009/73/EC, 2010/31/EU, 2012/27/EU and 2013/30/EU of the European Parliament and of the Council, Council Directives 2009/119/EC and (EU) 2015/652 and repealing Regulation (EU) No 525/2013 of the European Parliament and of the Council (Text with EEA relevance.). PE/55/2018/REV/1. OJ L 328, 21.12.2018, p. 1–77
- Riahi et al., 2017. The Shared Socioeconomic Pathways and their energy, land use, and greenhouse gas emissions implications: An overview, *Global Environmental Change*, Volume 42, 2017, Pages 153-168, ISSN 0959-3780, <https://doi.org/10.1016/j.gloenvcha.2016.05.009>.

- Riesch, H. (2013). Levels of Uncertainty in Essentials of Risk Theory, S. Roeser, R. Hillerbrand, P. Sandin and M. Peterson, Eds., London, Springer, pp. 29-56.
- Sanderson, I. 2003. Is it 'what works' that matters? Evaluation and evidence-based policy-making. *Research Papers in Education*, 18 (4): 331 – 345.
- Sidney, M.S. 2007. Policy Formulation: Design and Tools. In: Fisher, F., Miller, G.J and Sidney, M.S. *Handbook of public policy analysis: theory, politics, and methods*. CRC Press: Boca Raton, FL, USA.
- Simmons, D.C., Dauwe, R., Gowland, R., Gyenes, Z., King, A.G., Riedstra, D., Schneiderbauer, S., 2017. Qualitative and quantitative approaches to risk assessment. In: Poljanšek, K., Marín Ferrer, M., De Groeve, T., Clark, I. (Eds.). *Science for disaster risk management 2017: knowing better and losing less*. EUR 28034 EN, Publications Office of the European Union, Luxembourg, Chapter 2.1, doi: 10.2788/688605.
- Slovic, P., Fischhoff, B., and Lichtenstein, S. 1982a. Facts versus fears: understanding perceived risk. In: Kahneman, D., Slovic, P., and Tversky, A. (eds). *Judgement under uncertainty: heuristics and biases*. Cambridge University Press, Cambridge. pp. 463-489.
- SWD/2013/0134 final. COMMISSION STAFF WORKING DOCUMENT Guidelines on developing adaptation strategies Accompanying the document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS An EU Strategy on adaptation to climate change.
- SWD/2018/461 final. COMMISSION STAFF WORKING DOCUMENT Evaluation of the EU Strategy on adaptation to climate change, Accompanying the document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of the EU Strategy on adaptation to climate change UN, 2015. Adoption of the Paris Agreement.
- UNDP, 2008a. Capacity Assessment Methodology, User's guide. Capacity Development Group, Bureau for Development Policy, November 2008
- UNDP, 2008b. Capacity Assessment, Practice note. United Nations Development Programme.
- UNDRR, 2015. Sendai Framework for Disaster Risk Reduction 2015-2030. United Nations Office for Disaster Risk Reduction.
- UNISDR, 2017. Words into Action Guidelines National Disaster Risk Assessment. United Nations Office for Disaster Risk Reduction.
- Vlek, C. A.J. (1996). A multi-level, multi-stage and multi-attribute perspective on risk assessment, decision-making and risk control. *Risk Decision and Policy*, 1(1), 9-31.
- Walker, W.E., Harremoes, P.E., Rotmans, J., Van der Sluijs, J.P., van Asselt, M.B., Janssen, P. and Kraymer von Krauss, M. P. (2003). Defining Uncertainty. A conceptual basis for Uncertainty Management in Model-Based Decision Support, *Integrated Assessment*, 4(1), pp. 5-17.
- Wistow J., Dominelli L., Oven K., Dunn C., Curtis S., 2015. The role of formal and informal networks in supporting older people's care during extreme weather events. *Policy Polit.*, 43 (1) (2015), pp. 119-135.
- Wouter Botzen W.J. et al. (2019) Integrated Disaster Risk Management and Adaptation. In: Mechler R., Bouwer L., Schinko T., Surminski S., Linnerooth-Bayer J. (eds) *Loss and Damage from Climate Change. Climate Risk Management, Policy and Governance*. Springer, Cham. [https://doi.org/10.1007/978-3-319-72026-5\\_12](https://doi.org/10.1007/978-3-319-72026-5_12).

## 10 Floods

FRANCESCO DOTTORI, PETER SALAMON.

### 10.1 Context

A flood can be defined as the temporary covering by water of land not normally covered by water [EU 2007]. While floods are natural phenomena that may occur everywhere, human activities (such as encroaching in floodplains and land use changes) and climate modifications may increase the likelihood and adverse impacts of flood events, creating a risk for people and assets. Specifically, “flood risk” means the combination of the probability of a flood event and of the potential adverse consequences for human health, the environment, cultural heritage and economic activity associated with a flood event [EU 2007].

Every year floods cause enormous losses to economies and societies worldwide. In Europe, direct economic losses from floods (e.g. economic losses due by physical damage) are estimated to be approximately EUR 6 billion per year, and 250 000 people per year are estimated to be exposed (Alfieri et al., 2016). These figures are comparable to estimates based on observed impacts (EEA 2010).

#### 10.1.1 Legal framework of flood risk assessment in the European Union

Flood risk assessment in the European Union is regulated by the Floods Directive of the 2007 [EU 2007; FD in the following text], which is now integrated in the national legislation of EU countries. The Directive describes the steps that each Member State should take to implement flood risk assessment:

- Preliminary Flood Risk Assessment: based on available information on past studies, evaluate impacts on human health and life, the environment, cultural heritage and economic activity.
- Risk Assessment: identify the areas at significant risk to produce flood hazard and risk maps, including detail on the flood extent, depth and velocity for three risk scenarios (high, medium and low probability).
- Flood Risk Management Plans to indicate to policy makers, developers, and the public the nature of the risk and the measures proposed to manage these risks

Moreover, the Floods Directive foresees regular updates and review of each part of risk assessment every 6 years, as indicated in **Table 6**. The following table summarizes the relevant steps identified by the Floods Directive and the milestones for implementation and review (EU, 2016a). The first round of implementation of the Floods Directive has been finalized in 2016 and the results have been described in a number of reports (EU 2016a,b; WGF 2017).

**Table 6.** List of steps identified by the Floods Directive and the milestones for implementation and review. WFD: Water Framework Directive.

Subject	Main Article	Other Articles	Responsibility	To	Report Due date	Frequency/ review
Transposition	17		MS	COM	26/11/2009	
Competent Authorities and Units of Management (if different from WFD)	3.2 (annex 1 WFD)		MS	COM	26/05/2010	3 months after any changes
Preliminary Flood Risk Assessment	4	13.1(a) and 13.1(b)	MS	COM	22/03/2012	22/12/2018, every 6 years thereafter

Flood Hazard Maps and Flood Risk Maps	6	13.2	MS	COM	22/03/2014	22/12/2019, every 6 years thereafter
Flood Risk Management Plans	7	13.3	MS	COM	22/03/2016	22/12/2021, every 6 years thereafter
Progress by MS in implementation	16		COM	COM	22/12/2018	Every 6 years thereafter

Source: EC 2000.

Given its relevance, the description of methods for flood risk assessment in the following sections will often refer to the prescriptions of the Floods Directive.

## 10.2 Risk identification

In the risk assessment framework outlined by the Directive, the first requirement is the identification of relevant flood processes than can produce significant consequences in the areas of interest. The identification of relevant processes is generally based on the analysis of past flood events in the area of interest, which had significant adverse impacts on human health, the environment, cultural heritage and economic activity.. Such analysis should also include significant floods which have occurred in the past, where significant adverse consequences of similar future events might be envisaged.

Several natural and man-made processes can give origin to flood events. In practical applications, flood events are classified according to the main drivers and the water bodies that cause the event itself. The following list is taken from Poljanšek et al. (2017).

- Fluvial floods (riverine floods) occur when river levels rise and burst or overflow their banks, inundating the surrounding land. This can occur in response to storms with higher than normal rainfall totals and/or intensities, to seasonal strong weather systems such as monsoons or winter stormtracks, or to sudden melting of snow in spring.
- Flash floods can develop when heavy rainfall occurs suddenly, particularly in mountainous river catchments, although they can occur anywhere. Strong localised rainfall, rapid flood formation and high water velocities can be particularly threatening to the population at risk and are highly destructive.
- Heavy rainfall may cause surface water flooding, also known as pluvial flooding, particularly in cities where the urban drainage systems become overwhelmed.
- Floods can also be generated by infrastructure failure (e.g. dam breaks), obstructions caused by avalanches, landslides or debris, glacial/ lake outbursts and groundwater rising under prolonged very wet conditions, which cause waterlogging
- Coastal flooding is caused by a combination of high tide, storm surge and wave conditions. Note that floods caused by tsunami events are generally considered as geophysical hazards, and therefore are analyzed with different techniques (Poljanšek et al., 2017).

In many cases, flooding occurs as a result of more than one of the generating mechanisms occurring concurrently, making the prediction of flood hazards and impacts more challenging. As such, the construction of a comprehensive database of past flood events is crucial for a correct identification of all possible sources of flood hazard, and for understanding how flood hazard and impacts have been developing in time.

Following the identification of relevant flood processes, it is indispensable to identify and collect any relevant data related to risk components, namely hazard, exposure, vulnerability and coping capacity. The process of data collection is closely linked to the selection of adequate methodologies to evaluate risk components (see Chapter 10.3), because different methodologies would require different types of data. At the same time, data availability is one of the main drivers in selecting risk assessment tools, because the quality of any model depend on the quality of data available for its setup.

The following subsections provide an overview of how the different risk components should be characterized in the case of flood risk.

### 10.2.1 Hazard

Flood hazard is defined as the combination of probability and magnitude of relevant flood events that may affect the area of interest. In practical applications, flood hazard is quantified providing a spatial and temporal evaluation of the following variables, as mentioned in the Floods Directive:

- Probability of occurrence
- Flood extent
- Water depth
- flow velocity
- sediment load
- pollutant load

The probability of occurrence of a specific flood event is usually expressed as a return period. For instance, a 100-year flood event means that the event is expected to have 1% probability of occurring every year (that is, the return period is the inverse of the frequency of occurrence). Flood extent, water depth and flow velocity define how and how much floodwaters can spread over usually dry areas. Sediment load (e.g. the amount of fine and coarse materials transported by flow) may be a crucial variable where floodwaters have a potential to transport relevant quantities of sediments at high velocity, as in the case of flash floods involving areas with steep slopes. Pollutants load is important in case of flood events affecting infrastructures such as chemical industries and wastewater treatment plants.

Evaluating hazardous floods requires to calculate the magnitude, frequency and spatial distribution of extreme floods events in the area of interest, which requires the knowledge of the meteorological and hydrological regime of the area (ECE 2003). Then, hazardous events have to be related with the potential extent, duration of the inundation they might cause.

Where observed datasets have adequate spatial and temporal coverage (i.e. measurements are continuously available for a period of several decades), the magnitude and frequency of extreme events can be directly estimated through extreme value analysis techniques (Mentaschi et al., 2017).

However, in standard practice the available observations are generally not sufficient to fully characterize the regime of the extreme events. Therefore, observed datasets are integrated with modelling tools (empirical methods or physically-based models), regionalization techniques (that allow the analysis of the spatial pattern of variations of meteorological and hydrological phenomena, see Gottschalk 1985), or a mix of both approaches.

Precipitation, water level and stream discharge are some of the crucial variables that need to be extensively measured to evaluate the hazard related to intense rainfall events and to overflowing from the river network (both flash floods and river floods). Data requirements include hydrological measurements for the water bodies in the area of interest, such as time series of water level and flow measured from gauge stations, as well as the characterization of the river reaches (cross section shape, bed slope, geometry and location of hydraulic structures...). In case of coastal floods, the variables to be measured include wind speed, tide and storm wave heights, duration and extent of storm surge events.

In case of small areas subject to inland flooding (e.g. a single river basin with limited extent), the hydrological regime can be defined using empirical methods or hydrological models. In both cases, the aim is to estimate the runoff regime and hence extreme values based on available meteorological data (e.g. precipitation, temperature, humidity) and characteristics of the river hydrographic basins (e.g. geological, soil and land use maps). There is a wide range of existing commercial and research hydrological models that can be used (see for instance Beven 2011), as well as a large variety of empirical methods for more rapid runoff estimation, such as the Curve Number method, developed by the Soil Conservation Service of the United States [USDA, 1986].

In case of complex river networks, a river hydraulics model is needed to simulate water flow in the river network, including man-made structures such as dams and retention basins. In standard practice, coupled hydrological-hydraulic models can be set up to derive river flow regime from observed meteorological data.

Moreover, hydrological and hydraulic models can be coupled with meteorological forecasts to create a flood early warning system, which can provide real-time indication of expected flood hazard. Notably, hydrological and hydraulic models are necessary for analyzing hypothetical flood scenarios, such as changes in flooding regime caused by climate change or the construction of protection structures, and are therefore recommended.

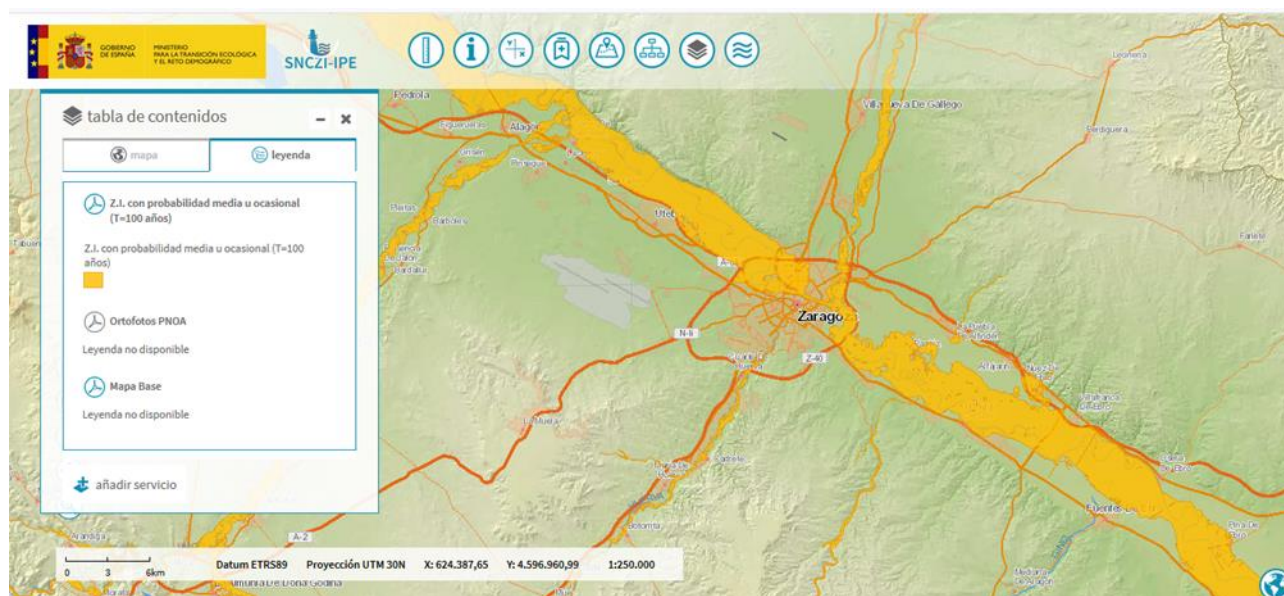
While the approach so far exposed made reference to inland flood processes, the general approach is also used to analyze coastal flood hazard. In this case, flood hazard is a consequence of the tidal, storm and wave regimes of the area of interest, which can be derived using storm surge and wave models in combination with observed data and regionalization techniques.

The meteorological and hydrological regime derived from modelling tools need to be statistically analysed to estimate frequency and magnitude of significant extreme events. Usually, the analysis is aimed at producing analytical curves relating extreme peaks to their probability of occurrence and consequently to their return period. A typical approach used in flood hazard modeling is the fit of maximum annual peaks (e.g. river flow, precipitation) with an extreme value distribution, such as the Gumbel distribution (see Hosking, 1990) or more advanced non-stationary analyses that can better reproduce changes varying in time due to changes in the dynamic system (Mentaschi et al., 2016).

The characterization of hazardous flood events must include the potential extent, magnitude and duration of the inundation they might cause, along with the quantification of the other variables of interest such as flow velocity and sediment transport. In standard practice, this is done by simulating relevant flooding processes through dedicated models, since inundation events are usually rare and difficult to measure in detail. Inundation models might be separate modeling tools (e.g. when used to derive flood scenarios such as dyke breaches or dyke overtopping at specific locations), or they can be integrated with the models used to simulate river flow regime or wave regime. Alternatively, methods based on topography and morphology can be applied to quickly evaluate flood prone areas, however these methods do not allow to estimate all the hazard variables requested for a complete risk evaluation. Researchers and practitioners nowadays can count on a wide variety of commercial and research models to model hydrodynamics processes (see for instance Teng et al., 2017). For instance, the HEC-RAS model developed by USACE (<http://www.hec.usace.army.mil/software/hec-ras>) and the DELFT-3D model developed by Deltares (<https://oss.deltares.nl/web/delft3d>) are two examples of freely available and well known models that are used worldwide, respectively for river hydrodynamics, and coastal hydrodynamics modelling.

The application of inundation modelling tools requires digital terrain models (DTMs) to describe the morphology of the study, together with information about past flood events, such as flood extent maps (nowadays often available as satellite-derived maps) and high water marks, to calibrate and validate model results. Detailed information about man-made structures (e.g. dykes and reservoirs for inland water bodies, coastal defences for coastal areas) is also necessary to simulate their influence on flooding processes.

**Figure 11.** 1-in-100-year flood hazard map for the Ebro River, Spain, near the city of Zaragoza,, published by Ministerio para la Transición Ecológica y el Reto Demográfico.



Source: Sistema Nacional de Cartografía de zonas Inundables, <https://sig.mapama.gob.es/snczi/>, accessed on 7/12/2020)

Alternatively, hazard models can be used to run probabilistic simulations of flood processes over long periods (usually hundreds or thousands of years), using synthetic input data (e.g. stochastic climate simulations consistent with historical observed climate). This so-called Monte Carlo simulation approach allows to derive robust probability distributions of significant extreme events, including low-probability events. Such methods are increasingly being applied for calculating hazard projections under climate change, for instance for future extreme sea levels (Vousdoukas et al., 2017).

The final product of flood hazard models is usually a set of flood hazard maps describing relevant variables (typically flood extent, water depth and flow velocity) for a number of reference flood scenarios. An example is shown in **Figure 11**. This approach is prescribed by the Floods Directive and constitutes one of the elements of risk evaluation (See Chapter 10.4).

### 10.2.2 Exposure

In the definition of flood risk maps, the Floods Directive indicates how flood exposure should be characterized in order to map potential adverse consequences associated with flood scenarios. Specifically, the following elements of exposure have to be considered (EU 2007):

- the indicative number of inhabitants potentially affected;
- type of economic activity of the area potentially affected;
- installations which might cause accidental pollution in case of flooding and potentially affected protected areas as by the Water Framework Directive (EU 2000);
- areas subject to floods with a high content of transported sediments, or with significant sources of pollution.

Other aspects of exposure that are mentioned by the FD are critical infrastructures (such as transport and energy networks, hospitals etc) and cultural heritage buildings.

As such, the requirements of the FD make necessary to characterize the spatial exposure of population, relevant assets (e.g. agricultural areas, industrial and commercial districts), critical infrastructures and protected natural areas. For population, the standard approach is to use population maps derived from national-scale census data. The exposure of economic activities and builtup areas is generally evaluated with land use maps, which describes the extent and location of built-up and natural areas with similar characteristics (e.g. residential areas, industrial districts, forests etc). These maps can be based on national-scale census data or derived from satellite images. For instance, the Corine Land Cover map is a satellite-



derived product available for all the EU Member states (Copernicus LMS, 2017). The location and characterization of critical infrastructures, cultural heritage buildings, protected natural areas and other points of exposure requires detailed information at local scale. A promising way to improve knowledge of these exposed assets is by leveraging global, open-access datasets such as Open Street Map. Finally, characterizing economic exposure requires data regarding building market values, values of building inventory and machinery (e.g. for industrial buildings) etc. Alternatively, proxy variables such as gross domestic product (GDP) at various administrative levels that can be used to infer the value of exposed assets.

In standard practice, exposure is often used as a proxy for flood risk, to provide a first evaluation of the impacts of hazardous flood events. This happens especially for population exposure, since quantifying the consequences of flood events on population is often complex and subject to relevant uncertainty (see Chapter 10.2.3).

The evaluation of exposure to flood events is usually carried out by combining the described exposure maps with hazard maps describing different flood scenarios. It is possible both to define exposure related to specific flood scenarios (e.g. total population exposed to the 1-in-100-year flood extent), or to elaborate statistical estimates that take into account a range of possible extreme flood events (e.g. expected annual population exposed to floods), as further described in Chapter 10.3.

### **10.2.3 Vulnerability**

The evaluation of the different facets of vulnerability (social, economic, environmental) requires both analytical studies of potential adverse effects of flood waters and the collection of loss and impact data from past flood events in the area(s) of interest.

Economic consequences of floods are usually evaluated distinguishing between direct and indirect damages. Direct damages (and consequent economic losses) are defined as physical, short term consequences such as physical damage to buildings, assets and consequent repair costs. These impacts are a function of different hazard variables (such as water depth and flood duration), as described in Merz et al. (2010). As such, vulnerability diagnoses should be carried out to assess the possible consequences of flooding, especially for critical buildings and infrastructures (ECE 2003). In addition, loss data collection should be carried out with the aim of quantifying all the mentioned aspects with an adequate spatial and temporal resolution (e.g. for several flood events, and including all relevant assets in the area of interest).

Indirect losses identify impacts that are not directly caused by floods, such as consequences of electricity cut-offs, roads closures, or loss of revenue due to closing of commercial activities (Merz et al., 2010). Similarly to direct damages, vulnerability diagnoses and loss data collection must be carried out to characterize all relevant consequences at different time periods.

Consequences of floods on population range from the risk of death and major injuries, to displacement and evacuation of people at danger, to short- and long-term physical and psychological consequences. Similarly to economic impacts, characterizing social vulnerability requires to analyse and record all relevant consequences on population at different time periods.

In standard practice, direct damages are usually evaluated using flood damage curves, which relate different hazard variables (such as water depth and flood duration) with physical consequences to different types of buildings and their related content (e.g. residential buildings and furniture, industrial buildings and machinery). The technical and scientific literature reports a wide range of methodologies to estimate damage functions, as well as established catalogues of functions (see for instance Huizinga et al., 2017). Indirect losses are generally evaluated using economic models that simulate the effect of floods on the economy of the affected areas, such as consequences of electricity cut-offs, or loss of revenue of commercial activities. A detailed review of the existing methods is reported in Merz et al. (2010). Similar approaches can be used to evaluate impacts on critical infrastructures, although in this case specific models might be necessary.

Consequences of floods on population are generally evaluated considering resident population in the flood prone areas and quantifying the number of people exposed to the flood events of interest, as described in Chapter 10.2. Even though flood risk for people includes the risk of death and major injuries, they are not usually addressed as it is more complex to evaluate. When performing risk assessment at municipality or limited scales, personal safety risk models based on precise hydro-dynamic analysis may be applied (e.g. Arrighi et al. 2016), although with a relevant uncertainty. Conversely, in larger scale applications probabilistic risk methods (e.g. de Bruijn et al., 2014) and the use of mortality rates calculated from previous flood events (e.g. Jongman et al., 2015; Tanoue et al., 2016) are more feasible.

### 10.2.4 Coping capacity

The consequences of hazardous flood events might be prevented or reduced when adequate prevention, protection and preparedness measures have been put in place to increase coping capacity, often in the form of flood risk management plans. The evaluation of existing measures, if available for the area of interest, is therefore of paramount importance for a correct evaluation of flood risk. Risk management plans are foreseen by the Floods Directive and ideally contain objectives for the reduction of the likelihood and potential adverse consequences of flooding for human health, the environment, cultural heritage and economic activity, including non-structural initiatives. In particular, these plans should consider all the prevention, protection and preparedness measures in place, such as protection measures (e.g. dyke systems, retention basins), flood forecasts and early warning systems, emergency plans, interventions to improve water retention and flood attenuation. All these measures should be listed and characterized, to understand how they influence flood hazard and vulnerability.

The mentioned methods described in Chapter 10.2.3 can be adapted to incorporate the effect of prevention, protection and preparedness measures in reducing flood vulnerability. For instance, flood forecasts, early warning systems and emergency plans can all increase the capacity to react and cope with flood consequences, and therefore reduce impacts (see for instance Molinari et al., 2014).

### 10.3 Risk analysis

As stated in the Flood Directive (EC 2007), risk assessment should aim at identifying people, economic activities and critical infrastructures potentially affected. In standard practice, risk evaluation can be undertaken with qualitative or semi-quantitative approaches (e.g. classifying the territory into risk classes) or quantitative methods (e.g. calculating risk in terms of possible economic, social and environmental impacts using probabilistic frameworks). It is important to note that the Floods Directive does not provide specific indications on the methodologies to be applied for evaluating flood hazard and flood risk, thus leaving to Member States the choice of the most suitable approach.

Risk analysis requires the selection of adequate models and methodologies. These include flood hazard modelling tools and methods, to define probability, magnitude and extent of flood-prone areas; flood impact models, relating hazard variables and exposure with consequences, such as physical damage to buildings; and flood risk assessment methods. We provide here a description of the methodologies commonly applied to evaluate risk components and quantify flood risk, together with recommendations.

Where deemed important, the links with other hazards and cascading effects need to be investigated with specific tools. Potential cascading effects of a flood event may include the loss of vital infrastructure, the outbreak of epidemic or epizootic events, damage to industrial facilities causing the release of chemical or radioactive substances (EC 2017).

Flood risk needs to be evaluated considering the range of possible impacts produced by relevant extreme events, taking into account their variable frequency and magnitude. This can be done with different semi-quantitative and quantitative approaches.

Semi-quantitative risk analysis seeks to categorise risks by comparative scores rather than by explicit probability and financial or other measurable consequences. It is thus more rigorous than a purely qualitative approach but falls short of a full comprehensive quantitative risk analysis (Poljansek et al 2017). Semi-quantitative methods can however be used to illustrate and compare quantitative risk estimates (see Chapter 10.4

A simple quantitative approach is to calculate risk separately in a number of representative flood scenarios, which can offer a comprehensive overview of the overall risk in the area of interest. For instance, the basic approach described in the Floods Directive (EC 2007) requires to quantify the population, type of economic activity and sources of pollutions (industrial installations) which can be potentially affected by the occurrence of at least three different scenarios (high, medium and low probability).

The risk scenario approach does not allow to consider the full range of possible relevant extreme events, nor the influence of analysed risk scenarios in determining overall risk. This can be done instead with the risk integral method. The integral method estimates the average annual impact of floods over the area of interest by computing the integral of the impact-probability curve, or risk curve (see Alfieri et al., 2016). In standard applications practice, the method requires to calculate the impact values for a selected range of return periods (e.g. overall economic damage, total population exposed) to construct a piece-wise risk function describing impacts according to the event frequency. Therefore, the expected annual impact values (e.g.

expected annual damage) is given by the integral of the risk curve across return periods. The integral method can account for existing flood protection structures (e.g. river dykes, retention areas) either by including them in the calculation of impacts, or by truncating the risk curve for return periods lower than or equal the local flood protection standard (see Alfieri et al., 2016).

An alternative method is probabilistic or stochastic risk modelling, which seeks to model all potential events with their associated probabilities and outcomes by running probabilistic simulations of flood processes over long periods, as described in Chapter 10.2. Stochastic risk modelling allows to derive robust risk probability distributions, including the effect of low-probability events. Traditionally, such methods form the basis of the risk models (catastrophe models) used by insurance and re-insurance companies, but they are increasingly being applied in research applications for evaluating future flood risk under varying climate and socioeconomic scenarios (Vousdoukas et al., 2017).

## 10.4 Risk evaluation

The use of flood risk models able to quantify risk components allow a wide range of risk analyses, including:

- define current flood risk at different geographical levels (e.g. to profile country risk, or risk for specific administrative regions)
- compare risk estimates across regions including comparison with other hazards
- reconstructing impacts of specific flood events (e.g. to be used as reference scenarios)
- analyze historical trends in flood risk (e.g. incorporating historical datasets of population, landuse, economic growth etc. into flood risk analysis of past flood events)
- how risk may change as a result of future climate, socio-economic and demographic changes.
- compare the outcome of different strategies to manage and mitigate risk. In particular, the cost and benefit of different solutions can be compared, and so an optimal strategy rationalised

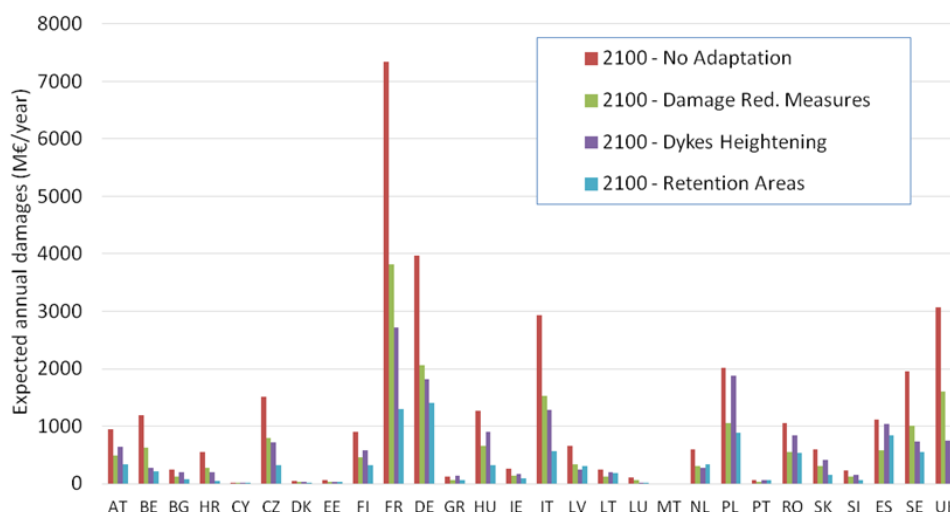
All the mentioned analyses should be considered in carrying out a comprehensive risk evaluation and communicate the results of the risk analysis.

In standard practice, including in the requirements of the Floods Directive, the outcomes of flood risk analysis are usually produced as risk maps, illustrating the spatial distribution of risk-prone population and assets. Usually, results are shown aggregated at different administrative levels, with the exception of specific risk hotspots (such as critical infrastructures, or installation with associated pollution risk).

Risk estimates in maps and tables can be provided using qualitative, semi-quantitative or quantitative approaches. Qualitative assessment categorise risk in classes, to provide a ranking of risk-prone areas within, say, the same country or region. An example is the traffic light rating systems (for example where red is severe risk, orange is medium risk, yellow is low risk and green is very low risk). While the outcomes are easy to communicate, it does not provide quantitative information and does not allow to understand differences between the same risk class. A more complete approach can be obtained with semi-quantitative approaches, where risk is categorised by comparative scores (e.g. normalized indices). Semi-quantitative methods can be used to illustrate comparative risk and consequences in an accessible way to users of the information. A risk matrix is a means to communicate a semi-quantitative risk assessment: a combination of two dimensions of risk, severity and likelihood, which allows a simple visual comparison of different risks. Indeed, some output from complex stochastic models may be presented in forms similar to that used in semi-quantitative risk analysis, e.g., risk matrices.

Finally, quantitative assessments (e.g. expected annual impacts) allow a great flexibility in presenting and comparing risk information across regions, time (e.g. comparing past and present risk scenarios, or future risk scenarios under climate change) and even across different hazards. Moreover, quantitative estimates can be easily applied to develop maps, graphs and risk matrices. For instance, the graph presented in **Figure 12**, compare expected annual economic damages for all EU countries under different scenarios. However, numerical results may be more difficult to interpret for a non-expert audience and need therefore to be carefully explained.

**Figure 12.** Comparison of expected annual damages in 2100 for all EU countries and United Kingdom, assuming no adaptation to future river flood risk conditions, and with the implementation of three different adaptation strategies. Results are calculated assuming a 2°C warming scenario.



Source: Dottori et al., 2020.

## 10.5 Gaps and challenges

The implementation of the Floods directive can be considered a success story in the field of natural hazards risk management. It allowed to establish a common ground in flood risk assessment in the European Union, introducing minimum requirements while leaving flexibility in its application. In particular, all EU Member states have now developed flood hazard and flood risk maps for at least three different flood scenarios, which are publicly available and are being used to inform flood risk management actions. Moreover, all Member States have completed and adopted flood risk management plans.

Despite this progress, there are a number of gaps and challenges that still need to be tackled in order to progress further flood risk management capacities (ECA 2018).

Regarding flood hazard maps, the surveys conducted among Member States (WGF 2017) highlighted a number of possible improvements. For instance, only 14 MS (out of 28) considered pluvial flooding among the possible drivers of flood hazard, even though pluvial flooding is a widespread problem. More in general, flash flood and pluvial floods are not always considered in flood risk management plans, as well as hazard deriving from multiple flood processes (e.g. combination of pluvial and river floods) or from multiple natural hazards (e.g. combination of landslides, debris flows and flash floods in mountain areas).

Regarding flood Risk Maps, all MS included the number of people potentially affected, adverse consequences on economic activity and on the environment. However, in many cases risk evaluation is still based on qualitative or semi-quantitative approaches (e.g. classifying the territory into risk classes) rather than quantitative methods (e.g. taking into account potential economic damage). Quantifying all aspects of risk is crucial to carry out reliable cost-benefit analyses as requested by the FD, and to allow comparisons across regions and scenarios. Currently, the application of impact models is hampered by relevant limitations in both modelling tools and loss data for model setup and validation. First, there is no agreement yet on methods to compare and quantify the variety of possible flood impacts, that is, economic losses, human impacts and consequences on cultural and natural heritage. This would require the development of common guidelines and methods for EU. Furthermore, flood loss data collection is still at the beginning in most of the EU Member States. Official estimates are still affected by the absence of clear standards for loss assessment and reporting, although progresses have been made in the last years (Corbane et al., 2015; IRDR, 2015). Loss reports are rarely complete and can strongly deviate from true extents and damages, thus complicating the validation and set up of impact models (Thielen et al. 2016). Indirect losses due to floods are rarely quantified in flood risk assessment works, due to the complex application and verification of the related economic models. Therefore, it is crucial to continue ongoing efforts in loss data collection and standardization.

Finally, the influence of climate change in modifying flood hazard and risk map has been taken into account by over half of the Member States (EC 2019). Also, 24 of the 26 Member States considered different aspects of climate change in their Flood Risk Management Plans, even though climate change impacts were considered only by ten Member states, while less than half refer to the national adaptation strategies prepared under the EU Climate Change Adaptation Strategy (EC 2019). Further efforts will be needed to better integrate the effects of future climate scenarios into flood risk management (ECA, 2018), and to measure progress in the adaptation to future climate change.

## 10.6 References

- Alfieri, L., Feyen L., Salamon P., Thielen J., Bianchi A., Dottori F., Burek P (2016) Modelling the socioeconomic impact of river floods in Europe. *Nat. Hazards Earth Syst. Sci.* 16, 1401–1411.
- Arrighi, C., Oumeraci, H., Castelli, F., 2017. Hydrodynamics of pedestrians' instability in floodwaters. *Hydrol. Earth Syst. Sci.*, 21, 515-531, 2017, doi:10.5194/hess-21-515-2017.
- Beven, K. J. (2011). *Rainfall-runoff modelling: the primer*. John Wiley & Sons
- Copernicus Land Monitoring Service. Corine Land Cover. <http://land.copernicus.eu/pan-european/corine-land-cover> (accessed 12-2-2017).
- De Bruijn, K. M., Diermanse, F. L. M., Beckers, J. V. L., 2014. An advanced method for flood risk analysis in river deltas, applied to societal flood fatality risk in the Netherlands. *Nat. Hazards Earth Syst. Sci.*, 14, 2767-2781, doi:10.5194/nhess-14-2767-2014.
- Dottori F, Mentaschi L, Bianchi A, Alfieri L and Feyen L, Adapting to rising river flood risk in the EU under climate change, EUR 29955 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-12946-2, doi:10.2760/14505, JRC118425
- Huizinga H. J., 2007. Flood damage functions for EU member states, HKV Consultants, Implemented in the framework of the contract #382442-F15C awarded by the European Commission - Joint Research Centre.
- Huizinga, J., de Moel, H., Szewczyk, W. (2017). Global flood damage functions. Methodology and the database with guidelines. EUR 28552 EN. doi: 10.2760/16510
- Jongman, B., Winsemius, H.C., Aerts, J.C.J.H., Coughlan de Perez, E., Van Aalst, M.K., Kron, W., Ward, P.J., 2015. Declining vulnerability to river floods and the global benefits of adaptation. *Proceedings of the National Academy of Sciences of the United States of America*, E2271-E2280, doi:10.1073/pnas.1414439112.
- European Court of Auditors (ECA), 2018. Floods Directive: progress in assessing risks, while planning and implementation need to improve. Luxembourg: Publications Office of the European Union, doi:10.2865/356339
- Economic Commission for Europe (ECE) 2003. Best Practices on Flood Prevention and Mitigation, presented at the meeting of the Water Directors in Athens in June 2003, prepared by The Netherlands and France (an update of the United Nations and Economic Commission for Europe (UN/ECE) Guidelines on Sustainable Flood Prevention of 2000) [http://ec.europa.eu/environment/water/flood\\_risk/pdf/flooding\\_bestpractice.pdf](http://ec.europa.eu/environment/water/flood_risk/pdf/flooding_bestpractice.pdf)
- European Commission (EC), 2000. Directive 2000/60/EC of the European Parliament and of the Council of 23 October 2000 establishing a framework for Community action in the field of water policy. *Official Journal of the European Communities*, Brussels.
- European Commission, 2007. Directive 2007/60/EC of the European Parliament and of the Council on the assessment and management of flood risks. *Official Journal of the European Communities*, Brussels.
- European Commission, 2015. Risk Management Capability Assessment Guidelines (2015/C 261/03), *Official Journal of the European Union*, Brussels.
- European Commission 2016(a). European Overview Assessment of Member States' reports on Preliminary Flood Risk Assessment and Identification of Areas of Potentially Significant Flood Risk. Luxembourg: Publications Office of the European Union, doi:10.2779/576456 ([http://ec.europa.eu/environment/water/flood\\_risk/overview.htm](http://ec.europa.eu/environment/water/flood_risk/overview.htm), accessed 23/4/2018)
- European Commission 2016(b). EU overview of methodologies used in preparation of Flood Hazard and Flood Risk Maps – final report. Luxembourg: Publications Office of the European Union, doi:10.2779/204606 ([http://ec.europa.eu/environment/water/flood\\_risk/overview.htm](http://ec.europa.eu/environment/water/flood_risk/overview.htm), accessed 23/4/2018)

European Commission, 2017. Overview of Natural and Man-made Disaster Risks the European Union may face. Commission Staff Working Document, Luxembourg: Publications Office of the European Union, doi:10.2795/861482

European Commission, 2019. Report from the Commission to the European Parliament and the Council on the implementation of the Water Framework Directive (2000/60/EC) and the Floods Directive (2007/60/EC) ([https://eur-lex.europa.eu/resource.html?uri=cellar:bee2c9d9-39d2-11e9-8d04-01aa75ed71a1.0005.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:bee2c9d9-39d2-11e9-8d04-01aa75ed71a1.0005.02/DOC_1&format=PDF), accessed on 7/12/2020)

European Environment Agency (EEA). Mapping the Impacts of Natural Hazards and Technological Accidents in Europe—An Overview of the Last Decade; European Environment Agency: Copenhagen, Denmark, 2010; p. 144.

Gottschalk, L. (1985). Hydrological regionalization of Sweden. *Hydrological Sciences Journal*, 30(1), 65-83.

Hosking, J. R. M., 1990. L-Moments: Analysis and Estimation of Distributions Using Linear Combinations of Order Statistics, *J. Roy. Stat. Soc. B*, 52, 105–124, 1990.

Huizinga, J., Moel, H. de, Szewczyk, W. (2017). Global flood depth-damage functions. Methodology and the database with guidelines. Publications Office of the European Union, Luxembourg, EUR 28552 EN. doi: 10.2760/16510

Merz, B., Kreibich, H., Schwarze, R., and Thieken, A., 2010: Review article “Assessment of economic flood damage”, *Nat. Hazards Earth Syst. Sci.*, 10, 1697–1724, doi:10.5194/nhess-10-1697-2010.

Mentaschi, L., Vousdoukas, M., Voukouvalas, E., Sartini, L., Feyen, L., Besio, G., and Alfieri, L.: The transformed-stationary approach: a generic and simplified methodology for non-stationary extreme value analysis, *Hydrol. Earth Syst. Sci.*, 20, 3527–3547, <https://doi.org/10.5194/hess-20-3527-2016>, 2016

Molinari, D., Ballio, F., Menoni, S. (2013). Modelling the benefits of flood emergency management measures in reducing damages: A case study on Sondrio, Italy. *Natural Hazards and Earth System Sciences*, 13, 1913–1927

Poljanšek, K., Marin Ferrer, M., De Groeve, T., Clark, I., (Eds.), 2017. Science for disaster risk management 2017: knowing better and losing less. EUR 28034 EN, Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-60679-3, doi:10.2788/842809, JRC102482.

Tanoue, M., Hirabayashi, Y., Ikeuchi, H., 2016. Global-scale river flood vulnerability in the last 50 years. *Scientific Reports*, 6, 36021.

Teng, J., Jakeman, A. J., Vaze, J., Croke, B. F., Dutta, D., & Kim, S. (2017). Flood inundation modelling: A review of methods, recent advances and uncertainty analysis. *Environmental Modelling & Software*, 90, 201-216.

United States Department of Agriculture (1986). Urban hydrology for small watersheds (PDF). Technical Release 55 (TR-55) (Second ed.). Natural Resources Conservation Service, Conservation Engineering Division.

Vousdoukas, M.I., L Mentaschi, E Voukouvalas, M Verlaan, S Jevrejeva, Jackson, L.P., Feyen, L., 2017. Global probabilistic projections of extreme sea levels show intensification of coastal flood hazard- *Nature communications* 9 (1), 1-12

Working group on Floods (WGF), 2017. Flood Risk Management in the EU and the Floods Directive's 1st Cycle of Implementation (2009-15). A questionnaire based report. [https://circabc.europa.eu/sd/a/c9abb873-6476-4cb6-bb7a-1ec296d28846/Review%20of%20the%20FD%27s%20first%20cycle%20WGF%20workshops%20w%20recommendation\\_FINAL.pdf](https://circabc.europa.eu/sd/a/c9abb873-6476-4cb6-bb7a-1ec296d28846/Review%20of%20the%20FD%27s%20first%20cycle%20WGF%20workshops%20w%20recommendation_FINAL.pdf), accessed on 17/6/2020

## 11 Droughts

ALFRED DE JAGER, GUSTAVO NAUMANN, PAULO BARBOSA, JÜRGEN V. VOGT

### 11.1 Context of drought risk assessment

Drought is for many countries among the most damaging and costly weather- and climate-related disasters. This affirmation is true for both, the world and for Europe. Estimations of annual losses due to drought in the U.S. are in the order of 5.6 billion € (NOAA, 2020) and in EU28 the recent annual losses were estimated to be around 9.4 billion € (EC, 2020). This situation is emphasized by the recent prolonged heat and dryness, resulting in unprecedented drought impacts for farmers, private households and wildlife in Europe. During the 2018 and 2019 summers, raging wildfires in the South as well as the North, severe restrictions for shipping on major rivers and irrigation, as well as reduced power supply have heightened European concerns about a possible rise in the severity and frequency of drought events as a manifestation of climate change (Cammalleri et al. 2020).

In this section, recommendations for the development of national drought risk assessments and for reporting on drought disasters are presented. The recommendations are mainly based on the methodologies presented in a recently published JRC Technical Report on drought risk assessment and management (Vogt et al. 2018) and the guidelines developed by the Global Water Partnership for Central and Eastern Europe in 2015 (GWP-CEE, 2015). Recommendations from the reporting obligations under the EU Water Framework Directive and from the scientific literature are also presented.

The Member States of the European Union report on the national risk assessment every three years for various disasters that occur on their respective territories. In order to assess priorities at European level an initiative was started aiming to make the reporting between the various Member States comparable. This first version of recommendations aims to help different assessments to converge over time, allowing the Member States to learn from experiences of neighbouring countries with similar issues and problems.

### 11.2 Risk Identification

According to the main characteristics of the water deficit and the related impacts, droughts are often divided in four main types: Meteorological Drought, which is related to a lack of precipitation and/or high evaporative demand, lasting from weeks to months or even years; Agricultural Drought, which is a period with reduced soil moisture resulting in a deficit in plant water supply which impacts on agricultural crops and/or natural vegetation; Hydrological Drought, which is characterised by reduced river and groundwater flows (can reduce accessibility of waterways and access to cooling water for industrial and energy generating processes); Socioeconomic Drought is a condition in which important services such as energy and drinking water supply are reduced.

The effect of a drought disaster can be exacerbated if it coincides with a heatwave. Warmer conditions increase evapotranspiration, depleting surface and soil water resources quicker. Moreover, a heat wave constitutes a disaster in itself in which access to clean water becomes essential both for humans as well as (wild) animals.

Since droughts are a recurring feature of all climates and can occur almost everywhere (excluding deserts and very cold regions) every Member State should have a drought management plan to cope with possible impacts. However, in Europe there are areas more prone to recurrent droughts such as the Mediterranean or parts of central Europe, in which Member States are more susceptible to suffer the negative effects of severe droughts.

Unlike other natural hazards such as earthquakes, floods, or wind storms that result in immediately noticeable and structural damage, droughts develop slowly and can last for long periods of time from some months up to several years. Frequently, drought conditions remain unnoticed until water shortages become severe and adverse impacts on environment and society become evident. Drought impacts may be minimized by adaptive buffers (e.g. water storage, purchase of livestock feed) and can continue long after precipitation has returned to normal conditions.

The slowly developing nature and long duration of droughts, together with a large variety of impacts beyond commonly noticed agricultural losses, hinders the task of quantifying drought impacts.

Impacts of droughts can be classified as direct or indirect. Vogt et al., (2018) provide a detailed characterization of the many different sectors that might be adversely affected by droughts. Examples of

direct impacts are a reduction of water levels, reduced crop and forest productivity, increased wild fire occurrence, increased livestock mortality, damage to ecosystems, and decreasing tourism among many others.

Similarly, many economic sectors and livelihoods are indirectly affected by droughts since they rely in different ways on water availability. These indirect effects can propagate or cascade quickly through the economic system, affecting also regions far from where the drought originates. Indirect impacts relate to secondary consequences on natural and economic resources. They may affect ecosystems and biodiversity, human health, commercial shipping and forestry. In extreme cases drought may result in temporary or permanent unemployment or even business interruption, increased prices of food, and can lead to malnutrition and disease in more vulnerable countries (Vogt et al. 2018).

The main sectors potentially affected by droughts might be identified by consultation with the main stakeholders as a first step of the risk assessment. Once the main sectors are recognised the assessment should be tailored to these specific needs and several complementary information layers could be drafted for the different users. For instance, the information relevant for a farmer is not necessarily relevant for a water manager working in an inter-basin water transfer system and vice versa.

Some extended drought events took place in the last years in areas not used to cope with drought. Parts of Germany, Belgium, the Netherlands, Poland, Czechia and Sweden were all affected by droughts especially accentuated in springtime of 2017, 2018<sup>48,49,50</sup>, 2019<sup>51</sup> and 2020<sup>52</sup> (see EDO analytical reports [footnotes]). Among the many sectors and systems affected, the forests of northern Europe were particularly hit. Germany, Czechia, Sweden, Finland, Poland and the Baltic countries have an important timber industry that got affected by these droughts leading to beetle outbreaks, caterpillar pests, wildfires and worries (e.g. Buras et al., 2020). The worries are especially related to the knowledge that the production forests in the Atlantic and Nordic areas of Europe are dominated by species being genetically mal-adapted to a hotter and drier climate (Ciais, et al., 2003; Isaac-Renton, et al., 2018), often monocultures planted 150 years ago on non-fertile soils but anyhow important for timber production, recreation and ecosystem services.

Knowledge on how to manage these forests is lacking and at political level there is a low interest in funding sector tailored research. Such research would need to answer questions like what tree types can replace the existing coniferous types, can non monocultures provide a profitable timber economy, can large grazing species and their ferocious predators assist in enhancing the ecosystem services and be accepted to live with by the local population and how to transfer from the existing forest stands to a forest better adapted to the expected new climatic conditions. Ecosystem services sciences, landscape ecology are however disciplines that originate in the sixties of the previous century, therefore a direction can already be given, but hard figures, like how much water a forest extracts, retains and gives back, alike we can do with irrigation schemes are missing and will require more fundamental research and setting aside large areas for such a purpose. Peatlands are another domain of ecosystem service that are suffering from compound pressures including climatic drying, warming and direct human impacts and particularly can suffer from large not reversible damage caused by drought in usual humid areas (Swindles, et al., 2019). The restoration of the forest biome in Europe should be integrated with the restoration of peatlands, both landscapes that provides essential ecosystem services, like their ability to retain water longer in an uphill area, thus alleviating drought risk considerably.

### **11.3 Drought risk analysis and characterization**

There are several ways to approach drought risk. However, the most commonly applied ones are the so-called outcome and contextual approaches (Van Lanen et al. 2017). The outcome or impact approach is based on the interactions between stressor and response. In this case, the endpoint of the analysis is the vulnerability (the more damage a society suffers, the more vulnerable it is). This approach relies on the use of quantitative measures of historical impacts as proxies for the vulnerability estimation (e.g. Blauhut et al. 2015; Naumann et al., 2015). However, relying on historical impacts has several limitations, mainly because impact data are often unavailable and frequently are not directly comparable between different regions.

---

<sup>48</sup> [https://edo.jrc.ec.europa.eu/documents/news/EDODroughtNews201809\\_Central\\_North\\_Europe.pdf](https://edo.jrc.ec.europa.eu/documents/news/EDODroughtNews201809_Central_North_Europe.pdf)

<sup>49</sup> [https://edo.jrc.ec.europa.eu/documents/news/EDODroughtNews201808\\_Central\\_North\\_Europe.pdf](https://edo.jrc.ec.europa.eu/documents/news/EDODroughtNews201808_Central_North_Europe.pdf)

<sup>50</sup> [https://edo.jrc.ec.europa.eu/documents/news/EDODroughtNews201807\\_Central\\_North\\_Europe.pdf](https://edo.jrc.ec.europa.eu/documents/news/EDODroughtNews201807_Central_North_Europe.pdf)

<sup>51</sup> [https://edo.jrc.ec.europa.eu/documents/news/EDODroughtNews201908\\_Europe.pdf](https://edo.jrc.ec.europa.eu/documents/news/EDODroughtNews201908_Europe.pdf)

<sup>52</sup> [https://edo.jrc.ec.europa.eu/documents/news/EDODroughtNews202006\\_Europe.pdf](https://edo.jrc.ec.europa.eu/documents/news/EDODroughtNews202006_Europe.pdf)



The contextual approach is based on intrinsic social or economic factors that define the vulnerability. Here the vulnerability is the starting point, allowing understanding why the exposed population or assets are susceptible to the damaging effects of a drought (e.g. Carrão et al. 2016; Meza et al. 2020). It is more suitable for setting targets for disaster risk reduction. This approach generally relies on combined indicators, which are mathematical combinations of risk determinants that have no common unit of measurement.

Agriculture (crop and livestock production) is often the first sector affected by droughts. A reduction in water availability and increases in solar radiation and temperature during a drought event can be directly translated into a significant reduction of crop productivity. In Europe, the share of drought losses in the agricultural sector is around 44%, with an estimate annual damage of around 4 billion € (Cammalleri et al. 2020).

End users, water managers, and policy makers rely on drought risk assessments that are usually developed with emphasis on agricultural and primary sector impacts. The conceptual framework presented here as an example of drought risk assessment was tested and applied in an operational global risk assessment. This system is mainly oriented to agriculture. However, the described methodology can be adapted to different sectors and applied at different scales (regional to local).

According to this framework, drought risk can be conceptualized as a combination of the natural hazard, the exposed assets and their inherent vulnerability (susceptibility to drought and adaptive capacity). Following this definition, the risk to be subject to damages and economic losses from a drought event depends on the combination of the severity and probability of occurrence of a certain event, the exposed assets (crops, livestock, critical infrastructure) and/or people, and their intrinsic vulnerability (susceptibility and adaptive capacity) to cope with a disaster (Carrão et al. 2016).

### **11.3.1 Hazard characterization**

Droughts affect different economic sectors and hence sector-specific risk assessments need to be developed. The characterization of the drought hazard should identify the most suitable drought indicator to represent the water resources necessary to meet the specific needs and uses of each sector. For instance, precipitation and/or soil moisture anomalies are key for rainfed agriculture, while river low flows, groundwater and reservoir storage are important for water supply systems (UNISDR, 2019).

### **11.3.2 Exposure identification**

Drought exposure is linked to the location of assets and persons that could potentially be affected by droughts. This information has to be represented through spatially explicit geographic variables. For instance, Carrão et al. 2016, proposed an approach taking into account different proxy indicators characterizing agriculture, namely crop areas and livestock distribution (agricultural drought), industrial domestic water stress (hydrological drought) and human population (socioeconomic drought).

### **11.3.3 Vulnerability identification**

Drought vulnerability is a key risk component as it allows identifying the policy relevant variables to be targeted (Naumann et al. 2018a). Since it is not possible to reduce drought frequency and severity, interventions to reduce drought impacts have to focus on reducing the vulnerability of human and natural systems.

As illustrated in Carrão et al., 2016, a multidimensional model composed by social, economic and infrastructural factors can represent vulnerability. Social vulnerability is linked to the level of well-being of individuals, communities and society; economic vulnerability is highly dependent upon the economic status of individuals, communities and nations; and infrastructural vulnerability comprises the basic infrastructures needed to support the production of goods and sustainability of livelihoods. During the Conference of the Parties in New Delhi in 2019 (COP-14), this theoretical framework to assess drought vulnerability was identified as a strategic objective for drought by UNCCD (ICCD/COP(14)/CST/7, 2019).

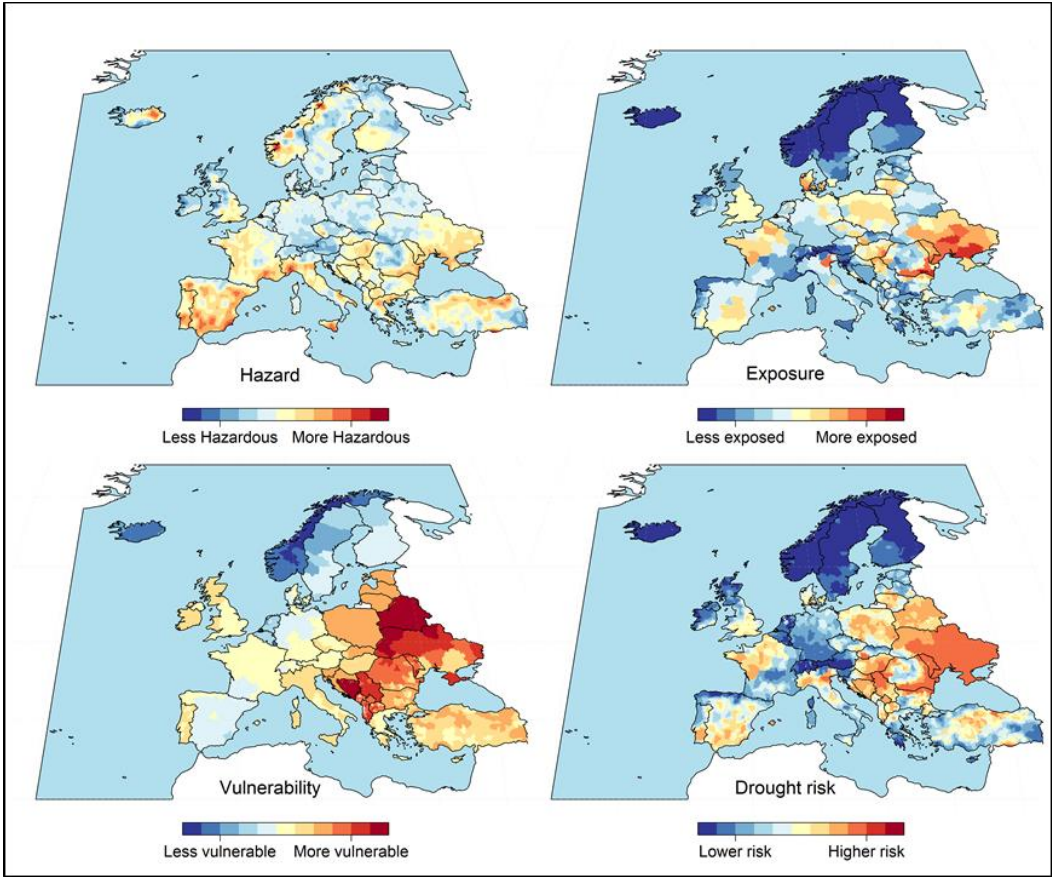
According to this approach, each dimension is represented by generic proxies that reflect the level of development of different constituents of civil society and its economy. In that sense, individuals require a range of independent factors or capacities to achieve positive resilience to drought impacts while no single factor on its own is sufficient to yield the varied livelihood outcomes that a society needs in order to cope with droughts. Appropriate social-ecological drought vulnerability indicators can be identified and weighted by consulting relevant experts and stakeholders (Meza et al., 2019; 2020).

Some variables that can be included into the vulnerability assessments are listed below as an example:

- Dependency on agriculture for livelihoods,
- Energy use,
- Farmers with crop/livestock insurance,
- Market fragility,
- Adult literacy rate,
- Availability of functioning drought early warning systems,
- Volume of water storage in a safe reservoir,
- Population without access to improved water,
- Institutional capacity and government effectiveness,
- Fertiliser consumption,
- Availability of water infrastructure, like reservoirs and irrigation systems.

As an example, **Figure 13** shows the three determining factors of drought risk (hazard, exposure and vulnerability) that result in the drought risk map for agricultural production in Europe. In this case, the scores for each component are not an absolute measure, but a relative statistic that provides a regional ranking of hotspots where to target and prioritise actions to reinforce adaptation plans and mitigation activities. This kind of analysis could be refined at higher resolution to obtain meaningful results at different scales of analysis. These can range from the farm level to the continent allowing an assessment of the spatial distribution of the drought risk within a given area of interest (e.g. farm, province, river basin or country). This framework is data driven and to obtain reliable estimates the main limitation is the availability and accuracy of relevant information at the different administrative levels.

**Figure 13.** Drought hazard, exposure, vulnerability and risk for the agricultural sector in Europe according to the conceptual approach



## 11.4 Risk identification in the context of climate change

Global warming is expected to modify the hydrological cycle across Europe through variations in the spatial and temporal distribution of precipitation, including more frequent and persistent dry spells, and increased atmospheric evaporative demand (Naumann et al., 2018b). As an immediate consequence of global warming, droughts will become more frequent, severe, and longer-lasting in many parts of Europe (Spinoni et al., 2019).

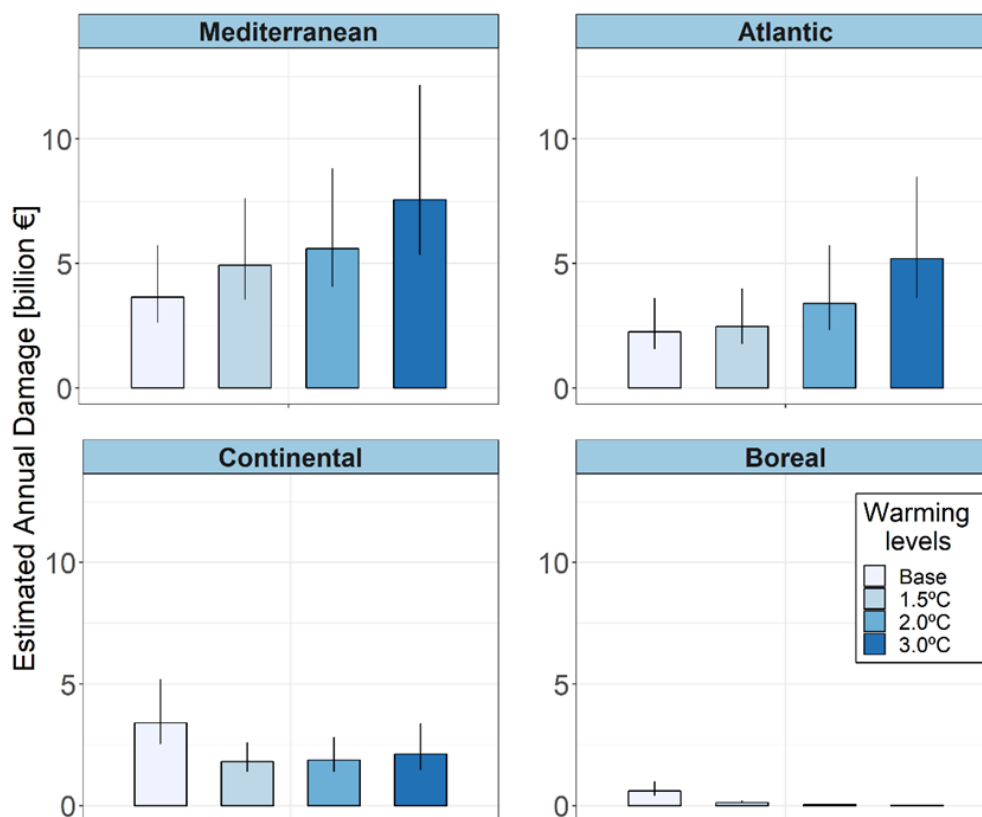
Assessments of future drought losses in the context of climate change are rare in literature, and to date only the recent PESETA IV task on droughts (Cammalleri et al. 2020) provides one of the first quantitative assessments on how drought impacts across Europe are expected to evolve with global warming.

When accounting only for the effects of climate change, aggregated European drought losses do not present significant changes up to 1.5°C warming, but increase to more than 11 billion €/year at 2°C warming and reach 15 billion €/year at 3°C warming. Therefore, a 3°C warmer climate applied on today's economy would result in a 50% increase of drought losses in Europe compared to present climate (Cammalleri et al. 2020).

There are, however, strong regional differences in Europe. PESETA IV projections show that the Mediterranean and Atlantic sub-regions of Europe could see a two-fold rise in drought impacts without mitigation if no additional adaptation measures are implemented (Figure 14). The spread in drought loss estimates increases with the magnitude of absolute losses but also grows relatively to the magnitude with the level of warming. This suggests that with warming there will be increasing uncertainty in drought conditions, even in regions where droughts will become less severe in general.

The above-mentioned results on projected impacts depend on present sectorial drought vulnerability estimates and hence assume no adaptation. There is a wide variety of drought risk mitigation and adaptation measures. Rather than supply-side measures, which can lead to a higher dependence on water resources that will increase drought vulnerability, adaptation should be targeted at strengthening drought resilience of society and sectors. This includes specific measures in drought-sensitive sectors, such as improved cooling techniques, drought-resistant crops, silvopasture and agroforestry practices, lighter river navigation vessels, but also institutional transformations, livelihood and economic diversification, insurance and other market tools, social safety nets, monitoring and data collection, and early warning and alert systems. Evaluating the costs and benefits of investments and policy actions taken to mitigate drought impacts remains a huge challenge. A recent study by the Integrated Drought Management Programme (IDMP) found that the cost of drought-related impacts without doing nothing to stop them, are much higher than the expense of financing proper public policy responses (WMO and GWP, 2017). In the same direction, the returns from investing in ex ante risk management actions are higher than those of investing in ex post crisis management. The actual costs and benefits of adaptation measures will vary substantially depending on the local geographical, climate, and socio-economic conditions.

**Figure 14.** Current and projected annual losses (in € billion, 2015 values) under different global warming levels relative to pre-industrial conditions (1.5°C; 2.0°C and 3.0°C) for EU-28 countries by region, for all economic sectors considered and assuming that current socio-economic conditions continue into the future. The top of each bar shows the average estimate and the vertical lines indicate climate uncertainty.



Source: Cammalleri et al. 2020.

## 11.5 Risk Treatment

To reduce the drought risk Member States need to present an inventory of the legal and institutional tools available in their country to perform the actions (Iglesias et al. 2009) briefly presented in the following chapters. After this short introduction for every action, a quantification method will be proposed, allowing comparing the readiness between the Member States.

Drought policies are needed to cope with drought disasters. Each Member State policy, however, needs to be adapted to represent particular local conditions. Drought policies should not simply be a post facto response to disaster, but should be a permanent concern of governments and society. In that sense, as proposed by HDMNDP (2013), Pischke and Stefanski (2018) and Vogt et al. (2018), any drought policy should be based on three pillars: 1) drought monitoring, forecast, and early warning systems; 2) vulnerability, and impact assessment and 3) drought preparedness, mitigation and response.

The preparation of Drought Management Plans should be linked to an agreed conceptual framework for drought management and based on clear drought definitions (Vogt et al. 2018). A good example can be found in the National Drought Management Policy Guidelines published by the Integrated Drought Management Programme (IDMP) (WMO and GWP 2014) and adapted to regional circumstances by the Global Water Partnership for Central and Eastern Europe (GWP-CEE 2015).

As presented in EC (2007); FAO (2019); UNCCD (2019) and UNISDR (2019) two basic approaches for drought risk management are currently applied. Their related legal and institutional tools can be divided into reactive and proactive actions. The proactive approach is linked with plans to prevent or minimize drought impacts in advance; these are mainly long-term actions, aimed to make the territory and the economy more robust to cope with droughts. The reactive approach includes actions after a drought event has started and is linked to short-term actions that can be executed during an emergency.

### 11.5.1 Organizational issues

It is recommended that the Member State establish a Drought Scientific and Advisory Committee. This Committee consists of scientific and practical experts in Land and Water Management and must be able to advise the various government bodies freely and openly. Care must be taken that the Committee is not representing specific stakeholders. Stakeholders should be represented using the normal political decision process.

The Committee should set out rules on when to gather during an emerging catastrophe and have the power to advise the government on declaring the state of emergency. The committee can also set out the relevance of the various actions mentioned in this document considering the local climatological, geographical and economical context of the Member State. In Member States with differing climates or federalization, more than one of these committees can co-exist.

Following UNCCD, 2019 recommendations, it is advised that national policymakers follow some of the following actions:

- Take a pro-active approach to assess vulnerability before a drought crisis escalates
- Foster inclusive, cross-sectoral and multi-scale approaches to risk and vulnerability assessments
- Integrate assessments of impacts on livelihoods, ecosystem service production and water balance accounting
- Assess both predictable and emerging economic implications of ongoing vulnerability to drought
- Learn by trial and review which methods are best-suited to encourage participation in risk and vulnerability assessments by different groups and sectors
- Document assessment successes and failures – including cases where anticipated drought impacts do not occur and vice-versa (some of these may indicate effective management)
- Share best practices and lessons learned with decision makers at different levels
- Learn from others' mistakes and successes by taking part in coordinated international knowledge exchange
- Where best practices or lessons learned are relevant to experiences for more than one country, seek out and validate generalizable lessons and document them to provide training materials for future decision makers
- Promote the improvement of regional databases on drought impact and vulnerability

### 11.5.2 Short Term Actions, during and immediately after the emergency

Depending on local conditions, short and long-term actions to tackle drought emergencies might be oriented to the supply-side (find additional supply to increased demands) or demand-side (measures to regulate water use and encourage efficiency). From the supply-side approach, policy measures often encourage renovation and improvement of existing water infrastructures or continued usage and expansion of natural catchments and aquifers. The demand-side approach, on the other hand, promotes policy measures that encourage subsidies and water efficiency strategies (EEA, 2009). In order to mitigate the effects of an emerging drought disaster the Member State needs to be able and have legislation in place, to perform the following actions (**Table 7**).

**Table 7.** Short term actions to be implemented during and after a drought emergency

<b>Water Demand Reduction</b>	<b>Water Supply Increase</b>	<b>Impact minimization</b>
<ul style="list-style-type: none"> <li>- Information campaigns for water saving</li> <li>- Domestic water use restrictions (e.g. car washing, gardening etc.)</li> </ul>	<ul style="list-style-type: none"> <li>- Temporary use of additional sources (river, seawater)</li> <li>- Temporary exploitation of groundwater reserves</li> </ul>	<ul style="list-style-type: none"> <li>- Temporary reallocation of water resources</li> <li>- Public aids to compensate income losses</li> </ul>

<ul style="list-style-type: none"> <li>- Irrigation restrictions</li> <li>- Mandatory Rationing</li> </ul>		<ul style="list-style-type: none"> <li>- Tax reduction or delay of payment deadlines</li> <li>- Public aids for crop insurance</li> </ul>
--	--	---

Source: Authors

### 11.5.3 Long-term actions, National Strategy

In order to make the territory and the economy less prone to drought disasters the Member State can develop a policy using a Drought Management Plan. Such a plan can focus on the long-term actions illustrated in **Table 8**.

**Table 8.** Long-term actions to be implemented before, during and after a drought emergency

Water Demand Reduction	Water Supply Increase	Impact minimization
<ul style="list-style-type: none"> <li>- Economic incentives for water saving</li> <li>- Pricing policy</li> <li>- Agronomic techniques for reducing water consumption</li> <li>- Drought resistant crops replacing more water demanding crops in irrigated areas</li> <li>- Measures to reduce the water required for irrigation in orchards (e.g. net shading)</li> <li>- Dual distribution network for urban use</li> <li>- Water recycling in industries</li> </ul>	<ul style="list-style-type: none"> <li>- Reuse of treated waste water</li> <li>- Leak detection programs</li> <li>- Construction of farm ponds</li> <li>- Control of seepage and evaporation losses</li> <li>- Keeping water longer in the ecosystem by naturalization of channeled rivers and creation of ponds</li> <li>- Counter actions on cementation (surface sealing), increasing soil water storage capacity</li> <li>- (Re)Forestation policy and closer-to-nature forest management</li> </ul>	<ul style="list-style-type: none"> <li>- Education / awareness campaigns</li> <li>- Reallocation of water resources based on water quality requirements</li> <li>-Development and/or improvement of early warning systems</li> <li>- Implementation of Drought Management Plans</li> <li>- Programs for areas with soils subjective to additional hazards during droughts: <ul style="list-style-type: none"> <li>- <i>Peatlands, leaking/ drainage problems</i></li> <li>- <i>Clayey soils, cracking/ construction problems</i></li> <li>- <i>Sandy soils, lack of moisture holding capacity/ quick dryness of soils</i></li> <li>- <i>Percolation of salty sea water in groundwater resources in coastal areas</i></li> </ul> </li> <li>- Insurance programs</li> </ul>

Source: Authors

### 11.5.4 Quantification of the actions

A short overview of the actions previously presented is illustrated in **Table 9** accompanied by a quantification method allowing them to be comparable between the Member States. The list is not exhaustive, and some measures are not relevant in very wet climates and/or in areas with a low population density.

Besides the quantification, it is recommended to notice the source on which the quantification is based as well as a judgement on the quality of the quantification (poor, good, excellent).

**Table 9.** Overview of actions accompanied by a quantification method allowing them to be comparable between Member States.

Action	Impact	Quantification	Remark
Information/Education Campaigns	Change of behaviour in quantity of water use	€ / per citizen / per year	Measure effect, divide state and private sector campaigns
Restrictions in water use	Prioritizing the available resource	Effort in enforcing the law in €	Description of the law
Restrictions in irrigation	Prioritizing the available resource	Loss of crops in € per year	Description of the law
Mandatory rationing	Prioritizing the available resource	Effort in enforcing the law in €	Description of the law
Temporary use of additional water sources	Increasing resource of lower quality	Realization price of the effort	m <sup>3</sup> potential available
Temporary use of groundwater	Increasing resource	m <sup>3</sup> potential available in emergency	Description of installations
Temporary reallocation of water resources	Prioritizing the available resource	m <sup>3</sup> potential available in emergency	Description of installations
Public aids to compensate income losses	Preservation of the economic structure of the food production sector	In €, total available funds, total used fund in year	Reference to the law
Tax reduction or delay of payment deadlines	Preservation of the economic structure of the food production sector	In € and time for year	Reference to the law
Public aids for crop insurance	Preservation of the economic structure of the food production sector	In € and for year	Reference to the law
Economic incentives for water saving	Gradually spilling less water	In € per year	Potential of water saving should be quantified
Agronomic techniques for reducing water consumption	Gradually spilling less water	# of researchers working on the topic	Peer reviewed articles on the subject produced by researchers of the Member State
Dry crops in place of irrigated crops	Reducing vulnerability	Percent decrease in irrigated area per year	Mark if official policy objectives
Dual distribution network for urban use	Optimizing use of resource	€ invested per citizen per year, # of citizens connected to a dual system	Mark if official policy objective
Water recycling in industries	Optimizing resource, avoiding pollution	€ invested per year, m <sup>3</sup> water extracted per year, per major river	Reference to River basin plan of the WFD
Reuse of treated waste water	Increasing quantity of resource	m <sup>3</sup> water reused per year	
Leak detection programs	Avoiding loss, also economic	Length of water piping system, m <sup>3</sup> water loss through leaks, K€ investment per year. Maintenance investment per year in national water pipe and sewage system.	
Inter-basin and within-basin water transfers	Flexibility increase	Description of the possibilities in m <sup>3</sup> water per basin (from to)	Reference to River basin plan of the WFD
Reservoir construction or amplification of existing reservoirs	Flexibility increase	Storage capacity in the existing reservoirs (m <sup>3</sup> ), m <sup>3</sup> storage capacity in planned reservoirs. K€ planned investment for next 3 years	

Action	Impact	Quantification	Remark
Construction of farm ponds	Increasing coping capacity	# of existing ponds, # of planned ponds for next 3 years	Reference to River Basin Management Plan of the WFD
Desalination	Straight increase of availability resource	Capacity in m <sup>3</sup> and percentage reliance on renewable energy of Desalinization.	Provide planning for the next 3 years both public and private (guess)
Control of seepage and evaporation losses	Improving agricultural practices	Investment in K€ per year	
Keeping water longer in the ecosystem, naturalization of channelled rivers and creation of ponds	Adaptation of the hydro geographical system, correction of past errors	Investment in K€ and capacity potential	
Counter actions on cementation, enhancing Soil Water Storage capacity increase	Increasing the storage capacity of water in the landscape	Investment in K€ in projects regarding the subject	
Reallocation of water resources based on water quality requirements	Enhancing flexibility during hazard	m <sup>3</sup> of potential water resources	
Stimulation of silvo-pasture and agroforestry	Connecting vegetation with groundwater	Km <sup>2</sup> increase of area under silvo-pasture or agroforestry	Provide government measurements to enhance change
Development/improvement of early warning systems	Timely information flow	Qualitative description	Reference to the systems, relation to setting state of emergency
Implementation of a Drought Management Plan	Coordination between various agents	Qualitative description	Relation to upstream and downstream plans in neighbouring countries
Programs for areas with soils subjective to additional hazards during droughts	Minimize impact	Mapping of the areas with sensitive soils for example with cracking	Description of the programs, soils with changing properties if drought lasts long.
Insurance programs	Enabling restart after the hazard	M€ of harvest insured against drought	Also M€ claimed and reimbursed to be marked.
Drought Scientific Advisory Board	Counteracting focus on short term interests	Members of the Board and their affiliations	Did the board create an advice in the last 3 years?

Source: Authors

## 11.6 Gaps and challenges

Assessing the risk for drought-related impacts to society and environment is a complex task, complicated by the very nature of the phenomenon, its often large spatial extent and temporal duration, leading to cascading impacts that may affect areas far distant from the actual drought and may last long after the actual drought has ceased. Lack of standardized data on historical impacts (both damage and loss) are a further difficulty.

The interlinkages with other hazards such as wildfires, heatwaves and even floods, and the combined risks arising from different hazards need to be explored. These risk assessments need to be sector specific, requiring an adequate set of environmental and socio-economic data related to the respective sectors.

However, together with more efforts in the collection and standardisation of impact data, the development of conceptual models that rely on policy relevant variables or proxies of socio-economic vulnerability can help stakeholders and policy makers to spot the most vulnerable and exposed sectors and define the goals to be achieved in the risk prone areas.



## 11.7 References

- Blauhut, V., Gudmundsson, L. and Stahl, K., 2015. Towards pan-European drought risk maps: quantifying the link between drought indices and reported drought impacts. *Environmental Research Letters*, 10(1), p.014008.
- Buras, A., Rammig, A., & Zang, C. S. (2020). Quantifying impacts of the 2018 drought on European ecosystems in comparison to 2003. *Biogeosciences*, 17(6), 1655-1672.
- Cammalleri C., Naumann G., Mentaschi L., Formetta G., Forzieri G., Gosling S., Bisselink B., De Roo A., and Feyen L., 2020. Global warming and drought impacts in the EU, European Commission, JRC Ispra, 2020.
- Carrão H., G. Naumann, P. Barbosa, 2016. Mapping global patterns of drought risk: an empirical framework based on sub-national estimates of hazard, exposure and vulnerability. *Glob Environ Change*, 39, 108-124.
- Ciais, P., Reichstein, M., Viovy, N., Granier, A., Ogee, J., Allard, V., ... & Valentini, R. (2005). Europe-wide reduction in primary productivity caused by the heat and drought in 2003. *Nature*, 437(7058), 529-533.
- EC, European Commission, 2007. Drought Management Plan Report, Including Agricultural, Drought Indicators and Climate Change Aspects. Technical Report 2008–023, Water Scarcity and Droughts Expert Network, DG Environment.
- EC, European Commission, 2020: Climate change impacts and adaptation in Europe. JRC PESETA IV final report. Science for Policy report. Publication Office of the European Union, Luxembourg, 2020.
- EEA, European Environmental Agency, 2009. Water resources across Europe-confronting water scarcity and drought. <https://www.eea.europa.eu/publications/water-resources-across-europe>. Accessed 10 Feb 2020
- FAO, Food and Agriculture Organization, 2015. The Impact of Natural Hazards and Disasters on Agriculture and Food Security and Nutrition: A Call For Action To Build Resilient Livelihoods, Rome.
- FAO, Food and Agriculture Organization, 2019. Proactive approaches to drought preparedness – Where are we now and where do we go from here? Rome.
- GWP-CEE, Global Water Partnership Central and Eastern Europe, 2015. Guidelines for the preparation of drought management plans. Development and implementation in the context of the EU Water Framework Directive. GWP, Stockholm, Sweden.
- HMNDP – High Level Meeting on National Drought Policies, 2013. Towards More Drought Resilient Societies. Geneva, 11 – 15 March 2013.
- ICCD/COP(14)/CST/7, 2019. Outcomes of the work of the Committee on Science and Technology on a monitoring framework for the strategic objective on drought. CST 14, New Delhi, India, 2019. <https://www.unccd.int/official-documents/cst-14-new-delhi-india-2019/iccdcop14cst7>
- Iglesias A., Garrote L., Cancelliere A., 2009. Guidelines to Develop Drought Management Plans. In: Iglesias A., Cancelliere A., Wilhite D.A., Garrote L., Cubillo F. (eds) *Coping with Drought Risk in Agriculture and Water Supply Systems*. Advances in Natural and Technological Hazards Research, vol. 26. Springer, Dordrecht.
- Isaac-Renton, M., Montwé, D., Hamann, A., Spiecker, H., Cherubini, P., & Treydte, K. (2018). Northern forest tree populations are physiologically maladapted to drought. *Nature communications*, 9(1), 1-9.
- Meza, I., Hagenlocher, M., Naumann, G., Vogt, J., Frischen, J., 2019. Drought vulnerability indicators for global-scale drought risk assessments. EUR 29824 EN, Publications Office of the European Union, Luxembourg. doi:10.2760/73844
- Meza, I., Siebert, S., Döll, P., Kusche, J., Herbert, C., Eyshi Rezaei, E., Nouri, H., Gerdener, H., Popat, E., Frischen, J., Naumann, G., Vogt, J. V., Walz, Y., Sebesvari, Z., and Hagenlocher, M., 2019: Global-scale drought risk assessment for agricultural systems, *Nat. Hazards Earth Syst. Sci.*
- Naumann G, Carrão H, and Barbosa P, 2018a. Indicators of social vulnerability to drought. Chapter 6 In *Wiley Book on Drought: Science and Policy, Part II: Vulnerability, risk and policy*. Wiley-Blackwell.
- Naumann G., Spinoni J., Vogt, J.V. and Barbosa, P., 2015. Assessment of drought damages and their uncertainties in Europe. *Environmental Research Letters*, 10 124013.
- Naumann, G., Alfieri, L., Wyser, K., Mentaschi, L., Betts, R. A., Carrao, H., Spinoni J., Vogt, J., Feyen, L., 2018b. Global changes in drought conditions under different levels of warming. *Geophysical Research Letters*, 45(7), 3285-3296.

NOAA National Center for Environmental Information (NCEI) U.S. Billion-Dollar Weather and Climate Disasters, 2020. <https://www.ncdc.noaa.gov/billions/> accessed 10 February 2020

Pischke F. and Stefanski, R, 2018. Integrated Drought Management Initiatives, Chapter 3 in D. Wilhite and R. Pulwarty Drought and Water Crises: Integrating Science, Management and Policy, Second Edition; CRC Press, Taylor & Francis Group.

Spinoni, J., Vogt, J. V., Naumann, G., Barbosa, P., & Dosio, A., 2018. Will drought events become more frequent and severe in Europe? *International Journal of Climatology*, 38(4), 1718-1736.

Swindles, G.T., Morris, P.J., Mullan, D.J., Payne, R.J., Roland, T.P., Amesbury, M.J., Lamentowicz, M., Turner, T.E., Gallego-Sala, A., Sim, T. and Barr, I.D., 2019. Widespread drying of European peatlands in recent centuries. *Nature Geoscience*, 12(11), pp.922-928.

UNCCD, 2019. Drought Impact and Vulnerability Assessment: a Rapid Review of Practices and Policy Recommendations. United Nations Convention to Combat Desertification (UNCCD), Bonn, Germany.

UNISDR, 2019. Global Assessment Report on Disaster Risk Reduction 2019, UN, New York, <https://doi.org/10.18356/f4ae4888-en>.

Van Lanen, H., Vogt, J.V, Andreu, J., Carrao, H., De Stefano, L., Dutra, E., Feyen, L., Forzieri, G., Hayes, M., Iglesias, A., Lavaysse, C., Naumann, G., Pulwarty, R., Spinoni, J., Stahl, K., Stefanski, R., Stilianakis, N., Svoboda, M., Tallaksen, L., 2017. Climatological risk: droughts. In: Poljanšek, K., Marín Ferrer, M., De Groeve, T., Clark, I. (Eds.). *Science for disaster risk management 2017 knowing better and losing less*. EUR 28034 EN, Publications Office of the European Union, Luxembourg, Chapter 3.9.

Vogt, J., Naumann, G., Masante, D., Spinoni, J., Cammalleri, C., Erian, W., Pischke, F., Pulwarty, R., Barbosa, P., 2018. Drought Risk Assessment. A conceptual Framework. EUR 29464 EN, Publications Office of the European Union, Luxembourg, 2018. ISBN 978-92-79- 97469-4, doi:10.2760/057223, JRC113937

WMO and GWP, World Meteorological Organization and Global Water Partnership, 2014. National Drought Policy Guidelines: A template for action (D.A. Wilhite). *Integrated Drought Management Programme (IDMP) Tools and Guidelines Series 1*. WMO, Geneva, Switzerland and GWP, Stockholm, Sweden.

## 12 Wildfires

DUARTE OOM, DANIELE DE RIGO, JESUS SAN-MIGUEL-AYANZ, TOMAS ARTES-VIVANCOS, ROBERTO BOCA, ALFREDO BRANCO, WESLEY CAMPANHARO, ROSANA GRECCHI, TRACY DURRANT HOUSTON, DAVIDE FERRARI, GIORGIO LIBERTA, PIERALBERTO MIANTI, HANS PFIEFFER

### 12.1 Context of Risk Assessment. Introduction

Wildfire risk assessment is fundamental for developing prevention, mitigation and preparedness plans. Many countries have customized approaches to assess wildfire risk and these vary widely among them (San-Miguel-Ayanz et al. 2003). The level of elaboration of these assessments is often related to the impact of fires in these regions and countries. Normally, those countries more often confronted with wildfires are more prepared and have elaborated detailed wildfire risk maps at country/regional level. However, this process has led to different regional/national approaches that are not comparable, although wildfires are often transborder events and may affect several countries simultaneously.

Harmonized procedures for wildfire risk assessment are needed in the context of the pan-European region to enhance planning and coordination of prevention, preparedness and firefighting actions to mitigate the damaging effects of wildfires. The impact of fires across the EU and neighbor countries requires a pan-European assessment of wildfire risk, which is described in the sections that follow. This approach is currently under development in close cooperation with between the Joint Research Center (JRC) of the European Commission, other Commission services and the Commission Expert Group on Forest Fires, which is now composed of fire management representatives from 42 countries in the region. A harmonized approach would improve cooperation among different regions of Europe and support a more efficient response in case of critical wildfire events, which are becoming more frequent under a changing climate.

The main goal of this chapter is to describe the development of a pan-European wildfire risk assessment based on a standardized approach described in JRC Science for Disaster Risk Management report published in 2017 (San-Miguel-Ayanz et al. 2017). This approach was further elaborated in the JRC Technical Report on Basic Criteria to assess Wildfire Risk at the pan-European level (San-Miguel-Ayanz et al. 2018) by presenting a first set of data that would enable the implementation of proposed assessment. The development of this pan-European approach follows from a series of EU regulations that require the European Commission to have a wide overview of the wildfire risk in the European region, to support the actions of its Member States and to ensure compliance in the implementation of EU regulations related to wildfires. The assessment will allow the inter-comparison of wildfire risk assessment among countries and be complementary to existing national wildfire risk assessments. Additionally, it can serve as a first approach to assess wildfire risk in those countries that have not yet performed a national wildfire risk assessment.

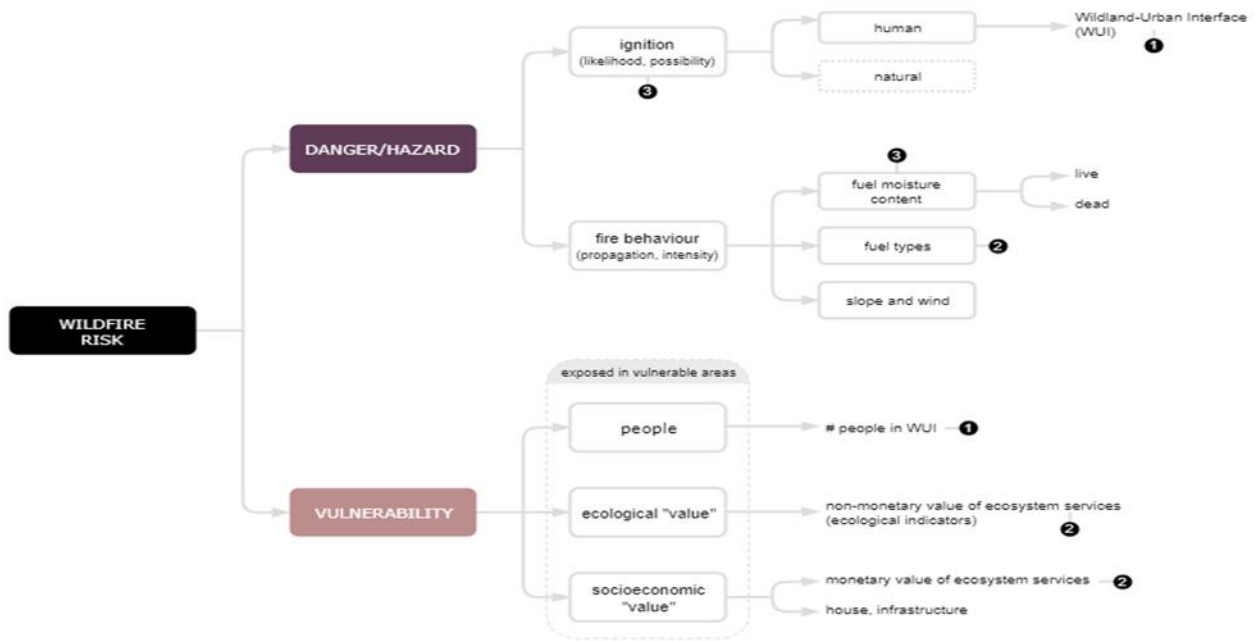
### 12.2 Risk identification

Wildfire risk can be identified as the joint effect of:

- wildfire danger (also known as fire hazard) and
- wildfire vulnerability of people, ecosystems and goods exposed to wildfires.

These two main components of wildfire risk, danger and vulnerability, are influenced by several factors that are described in detail in the following sections. Figure 15 summarizes the scheme proposed in terms components of wildfire danger/hazard and vulnerability.

**Figure 15.** A summary workflow highlighting the key components of the wildfire risk.



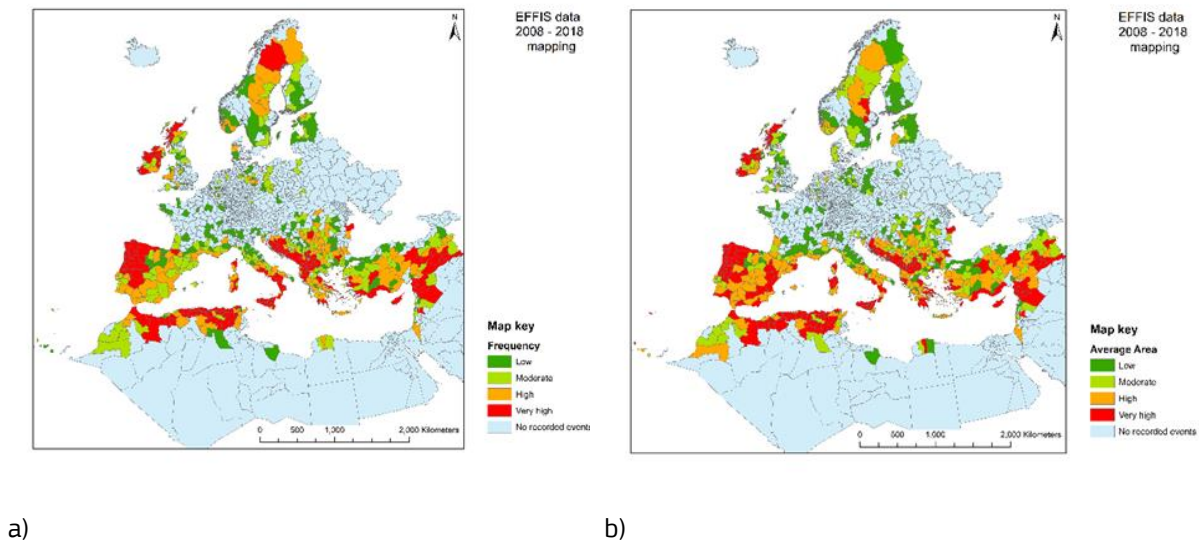
Source: Authors

Two main groups of components are defined by considering the fire danger (or hazard), and the vulnerability on three categories: people, ecological and socioeconomic value exposed in vulnerable areas. The following sections describe the different datasets that could be used for each component in the assessment of wildfire risk at the pan-European level.

### 12.2.1 Wildfire Danger

Wildfire danger. Wildfire danger is influenced by the factors related to the probability of ignition and those affecting fire behavior. It is therefore composed by the likelihood of having a fire ignition, and the behavior (propagation and intensity) of a fire once it is ignited. The upper branch of the scheme presented above in **Figure 15** represents all these factors.

**Figure 16.** (a) Annual fire frequency (number of fires per province (NUTS3)/years) and (b) average burned area (total burned area per province (NUTS3)/years) mapped in EFFIS, classified in four categories for the period 2008 - 2018.



Source: European Forest Fire Information System (EFFIS)

Historical records on the number of fires and burnt areas could be used to assess the contribution of fire ignition and extent to fire danger. An example of annual fire frequency per province (NUTS3) and annual average burned area per province in European Forest Fire Information System (EFFIS) for the period 2008-2018 s presented in Figure 16 at NUTS3 levels.

### 12.2.2 Wildfire ignitions

In Europe, the vast majority of ignitions is due to human causes (either deliberate or accidental), highlighting the critical role of the human factor in fire occurrence. The available information on fire causes reported by 19 countries, which follows a harmonized scheme at the European level (Camia et al. 2013), is included in the Fire Database of the European Forest Fire Information System (EFFIS). This shows that only 4% of the fires are not linked with human causes, being the rest of them linked to human actions, either deliberate or due to negligence or accident (Gantaume et al. 2013; de Rigo et al. 2017).

### 12.2.3 Fire behavior

The fire behavior is influenced by the fuel moisture content of both dead and live fuels, the different fuel types, slopes, and wind patterns that will determine the propagation (rate of spread and spread direction) of a wildfire and eventually its extent.

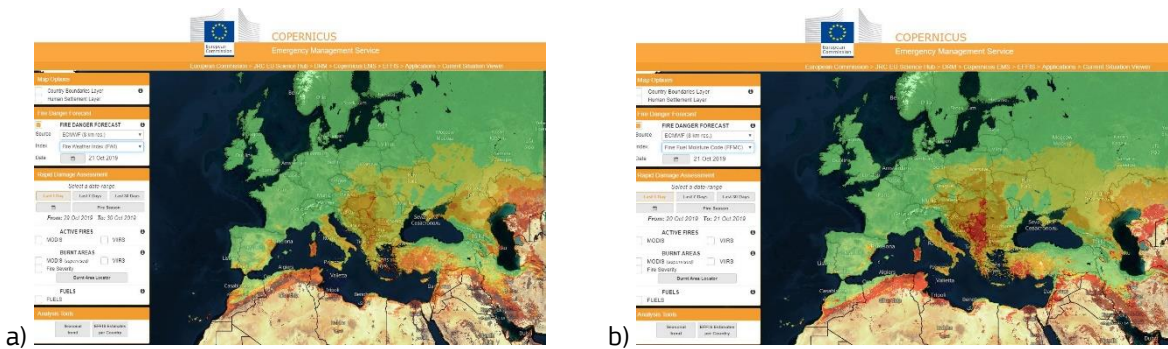
### 12.2.4 Fuel moisture

In the wildfire terminology, the term “fire danger” is often used for indices that are derived from meteorological variables, only. One of these indices, which is widely used in the world and is the standard in EFFIS, is the Canadian Fire Weather Index (FWI - **Figure 17a**). The FWI is based on three codes that assess the moisture content of dead fuels: the Fine Fuel Moisture Code (FFMC - **Figure 17b**), the Duff Moisture Code (DMC - Source: European Forest Fire Information System (EFFIS)

Figure **18a**) and the Drought Code (DC - **Source:** European Forest Fire Information System (EFFIS)

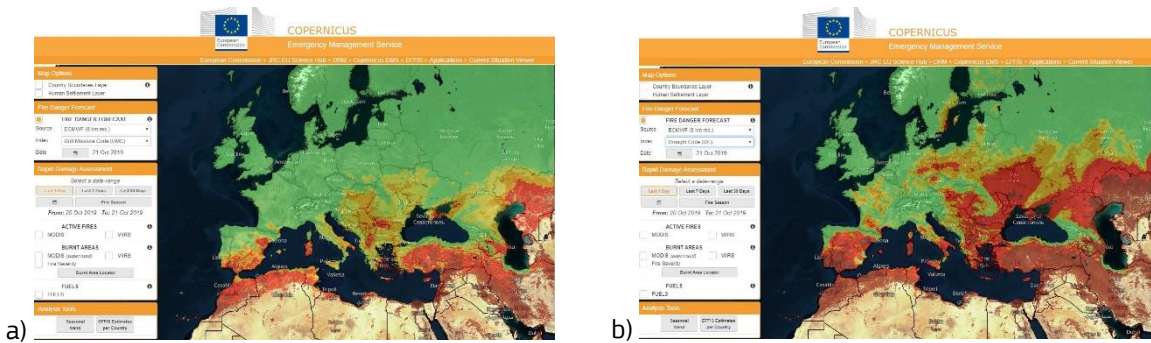
Figure **18b**). They refer, respectively, to the moisture content of litter and fine fuels, medium-size fuels, and thicker fuel components, with a longer drying rate (De Groot 1987).

**Figure 17.** Examples depicted from EFFIS for the (a) Canadian Forest Fire Weather Index (FWI), (b) Fine Fuel Moisture Content (conditions on October 21 2019).



Source: European Forest Fire Information System (EFFIS)

**Figure 18.** Examples depicted from EFFIS for (a) Duff Moisture Code, and (d) Drought Code (conditions on October 21 2019).



Source: European Forest Fire Information System (EFFIS)

When Wind is combined with the FFMC mentioned above, an intermediate index referred to as the Initial Spread Index (**Figure 19**) is obtained. This index considers the combined effects of wind and the Fine Fuel Moisture Code (**Figure 17a**) and represents the expected rate of fire spread.

**Figure 19.** Example of the Initial Spread Index in EFFIS (conditions on October 21 2019).



Source: European Forest Fire Information System (EFFIS)

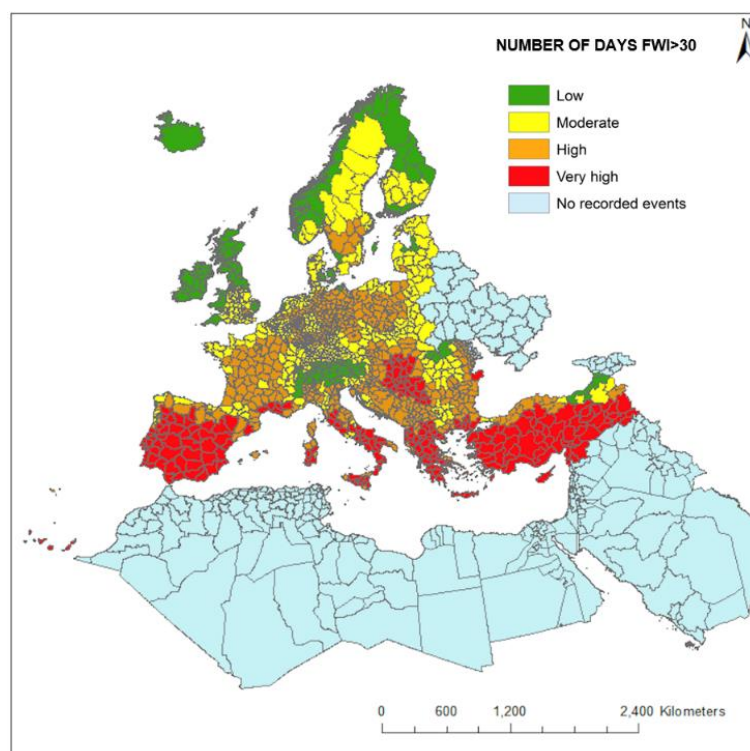


The FWI uses information on the moisture content of dead fuels, as estimated from meteorological variables, and wind speed to determine the level of “fire danger” in different areas (Van Wagner 1987). Each fuel moisture code relates to a specific size of fuels that can provide information on the probability of fire ignition, spread or fire intensity.

Long-term series of FWI data can be used as an explanatory variable in the assessment of wildfire danger at the pan-European level. As an example, Figure 20 shows areas in which high FWI higher than 30 (i.e. denoting high-to-extreme conditions of fire danger by weather) are frequent in the region.

In addition to the moisture content of dead fuels, the live fuel moisture content is important in determining fire spread and intensity. Existing approaches for the estimation of moisture content of live fuels rely on empirical methods or simulations, as those based on radiative transfer models (RTM) (Chuvienco et al. 2010; Yebra et al. 2013). However, estimation of live fuel moisture content is difficult and has so far only proven successful for grasslands and shrubs (Chuvienco et al. 2009). This layer of information is not yet included in the pan-European assessment of wildfire risk presented here.

**Figure 20.** Frequency of days with high fire danger (Fire Weather Index greater than 30).



Source: European Forest Fire Information System (EFFIS)

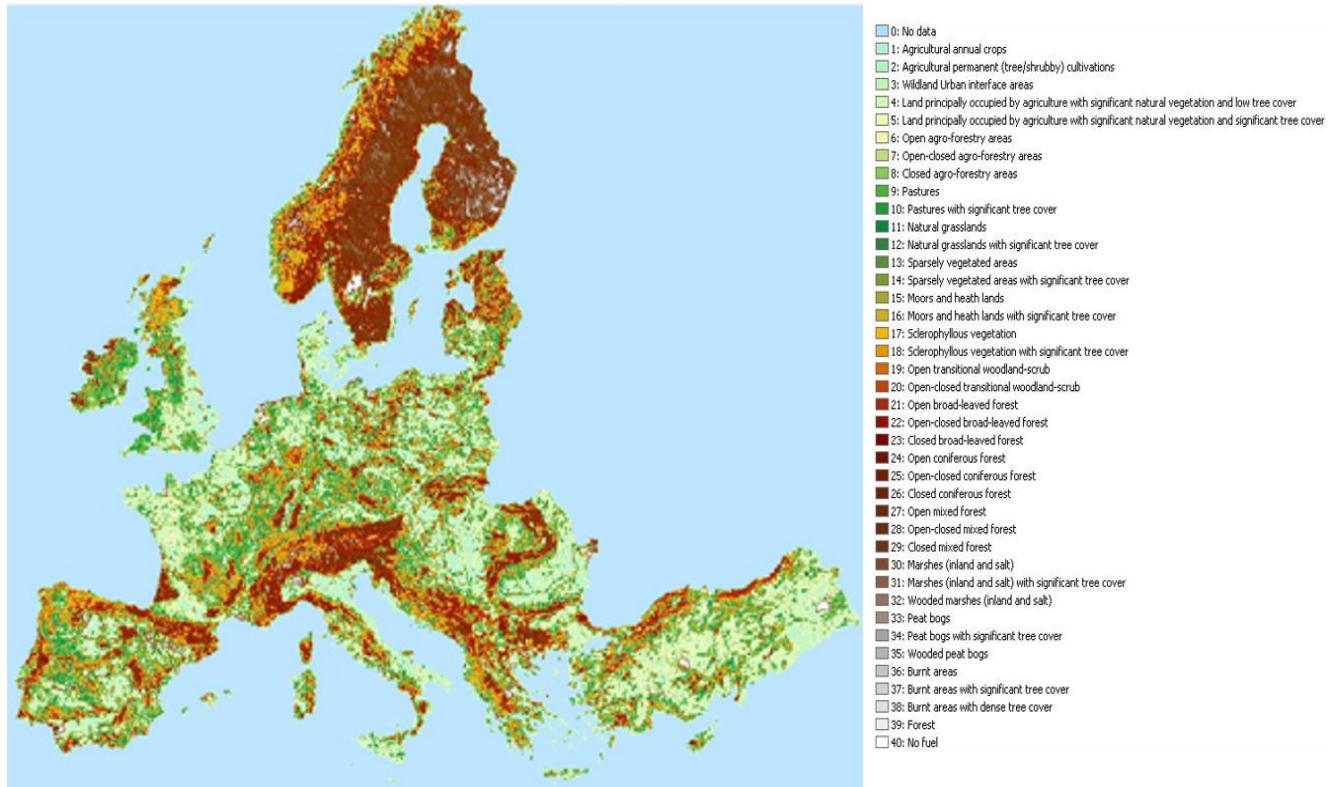
### 12.2.5 Fuel Types

The characteristics of the fuels available to burn, which may include trees, shrubs, grasslands, etc., influences directly the wildfire propagation. Each type of vegetation, with its physical and chemical specific attributes and its phenology, affects wildfire behaviour (rate of spread, fire intensity, and propagation) and the impacts of wildfires. Moreover, wildfire behaviour is highly dependent on the horizontal and vertical structure of the fuels and the inter-connection among them, which may determine the horizontal and vertical progression of the fire front (Scott and Burgan 2005).

The determination of fuel properties and their combinations in practice is a very complex process, and so they are usually grouped in fuel types. These follow classification schemes or typologies and are a necessary input for assessing risk management and fire effects. Fuel type maps are often developed through a combination of ground measurements such as forest and vegetation inventories and remote sensing techniques. A data set that is already available and useful to address fuel types as a criterion to assess wildfire danger at the European scale is the Fuel Map of Europe (EFFIS 2017). This data set (**Figure 21**), which initially maps 42 fuel types that are organized in 9 groups (Grassland, Shrubland, transitional shrubland/forest, conifer forest,

broadleaved forest, mixed forest, aquatic vegetation, agro-forestry areas and peat bogs), is further converted into the 13 fuel models of the National Fire Danger Rating System (NFDRS) to assess wildfire behaviour (Anderson 1982).

**Figure 21.** Fuel map of Europe.



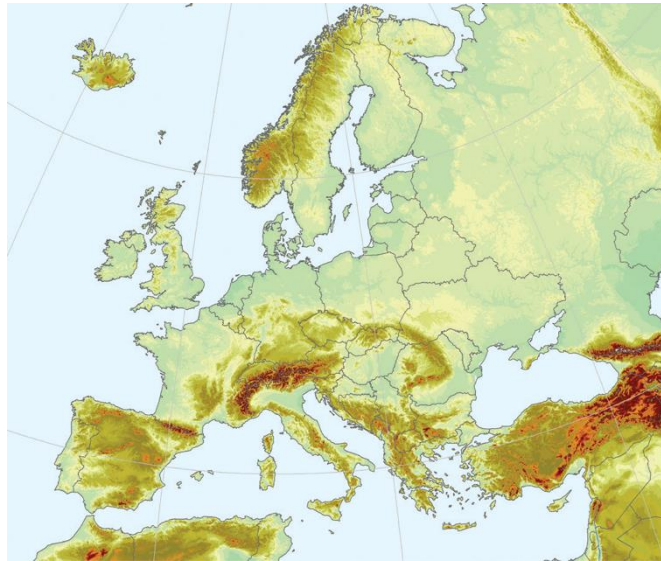
Source: EFFIS, 2017.

### 12.2.6 Slope

Slope is related to local conditions with relevance for fire behavior and wildfire propagation. For example, steep slopes may affect wind direction and speed facilitating fire spread. The orientation (aspect) of the slope may also have an influence on fire danger, e.g. southern facing slopes are likely to be hotter and drier, and hence can effectively dry fuels that may become prone to fire ignition and propagation. Terrain slope and wind (direction, speed) are the main local conditions affecting wildfire propagation and intensity. **Figure 22** shows the topography for the pan-European region.



**Figure 22.** Topography of the pan-European region derived from the European Atlas of Forest Tree Species



Source: de Rigo *et al.*, 2016

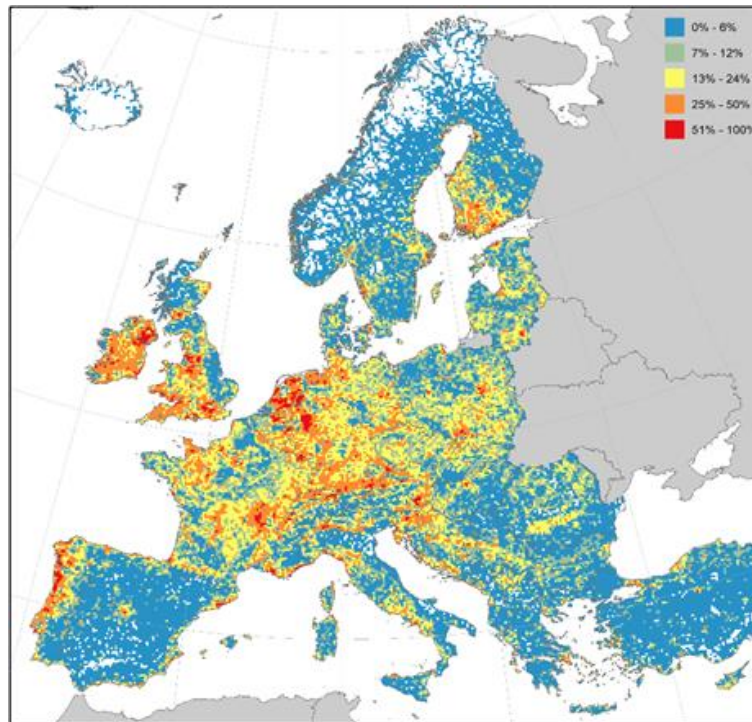
### 12.2.7 Vulnerability

Vulnerability is associated with the term exposure, which represents the presence of assets in hazard zones UNISDR (2015). Vulnerability can be defined as “the conditions determined by physical, social, economic and environmental factors or processes, which increase the susceptibility of an individual, a community, assets or systems to the impacts of hazards” (UNISDR 2009). Vulnerability refers to the condition of assets subject to being damaged by wildfires. These assets must be then exposed to suffer damage by wildfires. We consider three types of vulnerable assets: (1) people, (2) natural assets that have an intrinsic ecological value that is difficult to quantify, i.e. ecological value, and (3) human and natural assets whose value may be quantified, i.e. socioeconomic value.

### 12.2.8 People

Populated areas are often close to natural areas (wildland), generating a human-nature interface. In particular, this may be observed where natural vegetation expands into abandoned agricultural areas close to inhabited areas or conversely where settlements expand over areas previously dominated by wildland. This interface is referred to as the wildland-urban-interface (WUI). The WUI contributes to wildfire risk as wildfires are often started in this interface. Additionally, once wildfires are ignited, they pose a major threat to the population living in the WUI (Oliveira *et al.* 2018). In the proposed wildfire risk assessment approach, a WUI layer (Costa *et al.* 2020) is considered as component to determine human vulnerability to wildfires (Figure 23). In terms of assets that could be exposed to wildfires, a layer of information that is available is Global Human Settlement Layer (GHSL, Pesaresi *et al.* 2016), which is derived from remote sensing imagery and provides information on human houses/structures at a spatial resolution of 30 meters.

**Figure 23.** Percentage of land area which lies in the WUI.



Source: Costa et al. 2020

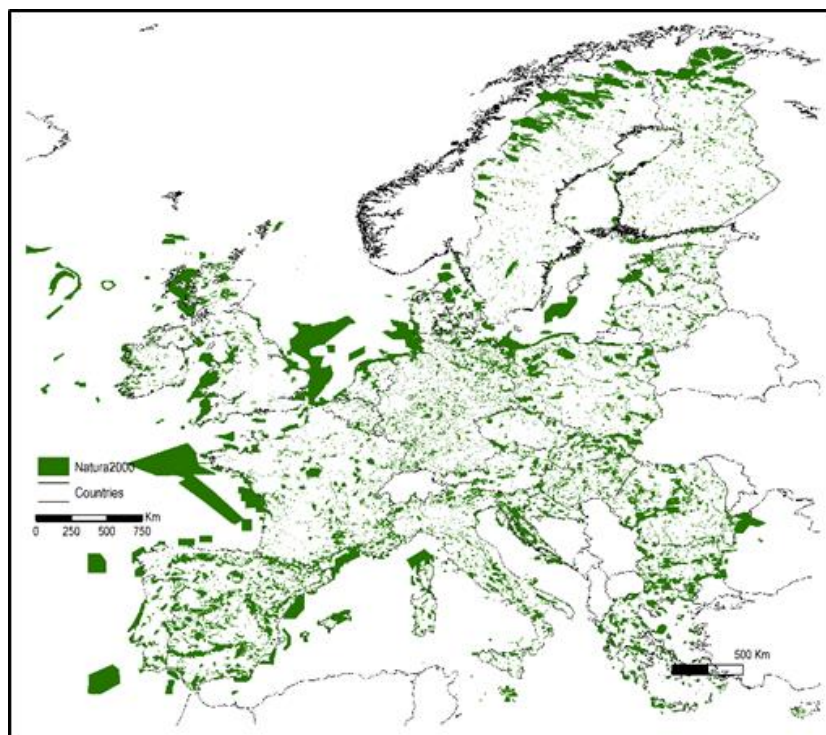
### 12.2.9 Ecological value

The value of ecological areas may be characterized by ecological indicators to account for the non-monetary value of the ecosystem services provided by them. Examples of ecological indicators may include the presence of protected natural areas, and of areas of those ecosystems in which the recovery after wildfires may be compromised by weather conditions. According to Chuvieco et al. (2014), this value is related with the ecosystem capacity to provide biodiversity richness/uniqueness, its conservation status and its habitat fragmentation.

Taking into account that ecological values are difficult to measure as they are often intangible, we suggest a qualitative approach to assess the ecological value within the wildfire risk assessment framework. Therefore, to emphasize the special ecological values of a territory we use the Natura 2000 network (**Figure 24**). This network was created using harmonized criteria for defining protected areas in the European context, to ensure the long-term survival of Europe's most valuable and threatened species and habitats. In 2017, they included over 1.5 million km<sup>2</sup> across 39 European countries (covering almost 26% of Europe's terrestrial territory) ranging from national parks to forest reserves and from strict nature reserves to resource reserves with more than 100 000 sites (<https://www.eea.europa.eu/data-and-maps/indicators/nationally-designated-protected-areas-10/assessment>). Natura 2000 is a key instrument to protect biodiversity in the European Union and identifies the most valuable and threatened species and habitats in Europe, whose damage from wildfires would represent a great loss.

Member States are encouraged to use their national or regional maps for Natura 2000 areas, which will probably provide more granularity of the various types of ecosystems protected, and thus also better inform their risk analysis. Moreover, an increase in the protected areas up to 30% of the EU territory has been promoted in the 2020 EU Biodiversity Strategy, and therefore, the most updated plans and mapping for protected areas should be used at national or regional level.

**Figure 24.** Natura 2000 network sites.



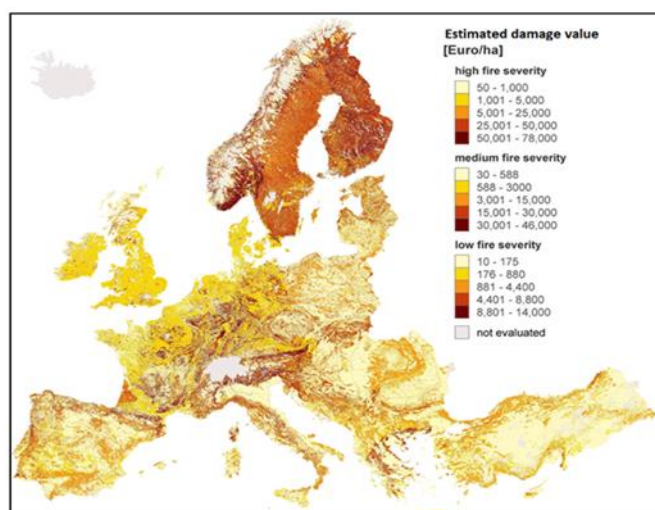
Source: European Environment Agency

### **12.2.10 Socioeconomic value**

Socio-economic damages caused by wildfires affect people's livelihood, safety, health, etc. Socioeconomic values may be quantified considering the presence and value of houses and infrastructure, the monetary value of the vegetation and wildlife that may burn as well as the value of ecosystem services that would be lost after wildfires. Properties, infrastructures, economic services provided by the vegetation (wood, non-wood products, hunting revenues, fungi, etc.), agricultural products, carbon stocks or recreational and tourist services can be associated to economic and social factors and be a part of the "tangible" values at stake (vulnerability) in the wildfire risk assessment.

A practical approach to address this criterion is to estimate the damage of wildfires in terms of costs of restoring land cover to its state, previous to a potential wildfire. Wildfire damage costs have been estimated for Europe based on the restoration cost of CORINE Land Cover classes (Oehler et al. 2012; Camia et al. 2017). These authors established a restoration cost for each land cover class at country level, and an average restoration time was defined according to the recovery capacity of the land cover. The damage caused by wildfire was estimated by discounting the cost of restoring the land cover over a restoration period. Different estimates were produced for three different vulnerability scenarios in which different levels of damage could be caused by low, medium and high wildfire severity (Figure 25).

**Figure 25.** Socio-economic value (reconstruction cost of different land cover types).



Source: Oehler et al. 2012.

### 12.3 Risk analysis

Wildfire risk in Europe may be assessed through a semi-quantitative approach by using the available quantitative data presented in Section 12.2, above, as proxy information for the wildfire danger and vulnerability components, along with a qualitative aggregation of them in classes of importance according to expert knowledge (from low to high importance). For instance, areas could be assigned a category of wildfire risk in three levels, low, medium or high, on the basis of the values of the different components.

Areas at wildfire risk may be assessed by considering the vulnerable areas where people ecological and socioeconomic values are exposed to fire danger. An aggregated wildfire risk index is proposed, which prioritizes the risk for human lives, while also considering ecological and socioeconomic aspects. This would be done by ranking as high-risk areas those where people may be exposed to wildfires, and secondarily other areas where ecological and socioeconomic aspects are at stake.

#### **Box 9: European fire risk: simple, consistent maps to support policy**

Wildfire risk is defined combining wildfire danger and vulnerability (people, ecosystems, goods exposed in vulnerable areas). Ecosystems are assessed by their ecological value. Goods are assessed by their socioeconomic value.

A wildfire risk map is then generated as an index to summarize the combined effect of wildfire danger and vulnerability. High risk may be expected where high wildfire danger affects the most critical areas for people, and secondarily for the other ecological and socioeconomic aspects.

The format of the risk map allows risk classes (from low to high risk) to be identified, with a simple score ranging from 0 % to 100 %, which could then be aggregated in three levels of risk: low, medium and high.

### 12.4 Wildfire risk and climate change

The effects of climate change are already noticeable in the expansion of the fire seasons in many regions of the world as well as in the increase of the intensity and frequency of critical fire episodes in the last years (Bowman et al. 2017; Nature Climate Change, 2017). Climate change has a direct effect on fire danger by increasing the parameters that contribute to it, such temperature, precipitation, relative humidity, etc., as well as to the vulnerability of ecosystems, which are weakened as the conditions for survival of existing plant and animal species are modified.

The results of the PESETA<sup>53</sup> studies carried out by JRC (Camia et al. 2017; de Rigo et al. 2017) show the confirmed tendency to an increase fire danger in the next years, leading to the increase in the number of days under high to extreme fire danger. According to these scenarios, the amount of burnt area, which is highly correlated with high danger values, would increase as the fire danger increases. Furthermore, the changes in

<sup>53</sup> Projection of Economic impacts of climate change in Sectors of the European Union based on bottom-up Analysis (PESETA), see <https://ec.europa.eu/jrc/en/peseta-iii>

climatic conditions will affect vegetation, which will in turn become more vulnerable to wildfires (Costa et al. 2020).

## 12.5 Gaps and challenges/Conclusions

A semi-quantitative methodology is proposed to assess wildfire risk at pan-European level on the basis of available information for the different components of wildfire danger and vulnerability to wildfires, in agreement with the UNDRR standards. Nevertheless, research is ongoing on both deriving enhanced datasets and methods. For instance:

- Fuel classification – an accurate mapping of fuel types would include detailed information on composition and structure of the fuels. Furthermore, fuels types are made of vegetation complexes, which change dynamically with time and management. Accordingly, having up to date information on fuel types is very challenging.
- Socio economic components – The adequate estimate of socio-economic value requires updated information on the value at assets that may be exposed to wildfires, such as human housing and infrastructures, condition and value of ecosystem services and the lapse of time for their recovery after fires. Often, this information is not available and has to be estimated through proxy datasets.
- Terminology – A major issue in scientific literature is the heterogeneity (and sometimes inaccuracy) of the terminology. In the existing literature wildfire risk and wildfire danger are often used as inter-changeable concepts, which leads to confusion among potential users of wildfire risk maps.
- Validation of wildfire risk – Wildfires are a complex phenomenon in which many factors have an important role for both the initiation (ignition) of the event and its development. Different from other phenomena, wildfires do not have a probabilistic cycle or time of return, because of their intrinsic linkage with human factors which are far beyond the current modelling capabilities. Thus, the validation of wildfire risk is as complex as its computation.

## 12.6 References

- Anderson, H.E., 1982. Aids to determining fuel models for estimating fire behavior. U.S. Department of Agriculture, Forest Service, Intermountain Forest and Range Experiment Station, General Technical Report INT-122, <https://doi.org/10.2737/INT-GTR-122>
- Bowman, D.M.J.S., Williamson, G.J., Abatzoglou, J.T., Kolden, C.A., Cochrane, M.A., Smith, A.M.S., 2017. Human exposure and sensitivity to globally extreme wildfire events. *Nature Ecology & Evolution* 1, 0058+. <https://doi.org/10.1038/s41559-016-0058>
- Camia, A., Houston Durrant, T., San-Miguel-Ayanz, J., 2013. Harmonized classification scheme of fire causes in the EU adopted for the European Fire Database of EFFIS. Publications Office of the European Union, Luxembourg. ISBN:978-92-79-29385-6, <https://doi.org/10.2788/86859> INRMM-MiD:14167573
- Camia, A., Libertà, G., San-Miguel-Ayanz, J., 2017. Modeling the impacts of climate change on forest fire danger in Europe: sectorial results of the PESETA II Project. Publications Office of the European Union, Luxembourg. ISBN: 978-92-79-66259-1, <https://doi.org/10.2760/768481>
- Chuvieco, E., Gonzalez, I., Verdu, F., Aguado, I., Yebra, M., 2009. Prediction of fire occurrence from live fuel moisture content measurements in a Mediterranean ecosystem. *International Journal of Wildland Fire* 18(4) 430-441 <https://doi.org/WF08020>
- Chuvieco, E., Aguado, I., Yebra, M., Nieto, H., Salas, J., Martín, M. P., De La Riva, J., 2010. Development of a framework for fire risk assessment using remote sensing and geographic information system technologies. *Ecological Modelling*, 221(1), 46-58. <https://doi.org/10.1016/j.ecolmodel.2008.11.017>
- Chuvieco, E., Martínez, S., Román, M. V., Hantson, S., Pettinari, M. L., 2014. Integration of ecological and socio-economic factors to assess global vulnerability to wildfire. *Global Ecology and Biogeography* 23(2), 245-258. <https://doi.org/10.1111/geb.12095>
- Corbane, C., Florczyk, A., Pesaresi, M., Politis, P. Syrris, V., 2018. GHS built-up grid, derived from Landsat, multi-temporal (1975-1990-2000-2014), R2018A. European Commission, Joint Research Centre (JRC) <https://doi.org/10.2905/jrc-ghsl-10007> PID: <http://data.europa.eu/89h/jrc-ghsl-10007>



- Costa H., de Rigo, D., Liberta, G., Houston Durrant, T., San-Miguel-Ayanz, J., 2020. European wildfire danger and vulnerability in a changing climate: towards integrating risk dimensions. Publications Office of the European Union, Luxembourg, ISBN: 978-92-76-16898-0, <https://doi.org/10.2760/4695>
- Costa, H., de Rigo, D., San-Miguel-Ayanz, J., 2020. Wildland-urban interface in Europe: a fuzzy approach. (in prep.)
- De Groot, W. J., 1987. Interpreting the Canadian Forest Fire Weather Index (FWI) System. In: Fourth Central Regional Fire Weather Committee Scientific and Technical Seminar, Proceedings. pp. 3-14. <http://cfs.nrcan.gc.ca/publications/?id=23688> INRMM-MiD:14176512
- de Rigo, D., Caudullo, G., Houston Durrant, T., San-Miguel-Ayanz, J., 2016. The European Atlas of Forest Tree Species: modelling, data and information on forest tree species. In: San-Miguel-Ayanz, J., de Rigo, D., Caudullo, G., Houston Durrant, T., Mauri, A. (Eds.), European Atlas of Forest Tree Species. Publications Office of the European Union, Luxembourg, pp. e01aa69+. <https://w3id.org/mntv/FISE-Comm/v01/e01aa69>
- de Rigo, D., Libertà, G., Houston Durrant, T., Artés Vivancos, T., San-Miguel-Ayanz, J., 2017. Forest fire danger extremes in Europe under climate change: variability and uncertainty. Publications Office of the European Union, Luxembourg, 71 pp. ISBN:978-92-79-77046-3 , <https://doi.org/10.2760/13180> INRMM-MiD:14519341
- European Forest Fire Information System (EFFIS), <https://effis.jrc.ec.europa.eu>
- European Environment Agency, Natura 2000 Network Viewer, <https://natura2000.eea.europa.eu/>
- European Forest Fire Information System (EFFIS) - European Fuel Map, 2017, based on JRC Contract Number 384347 on the "Development of a European Fuel Map", European Commission.
- Ganteaume, A, Camia, A. Jappiot, M., San-Miguel-Ayanz, J., Long-Fournel, M., Lampin, C., 2012. A review of the main driving factors of forest fire ignition over Europe. Environmental management. doi:10.1007/s00267-012-9961-z.
- Nature Climate Change, 2017. Spreading like wildfire. Nature Climate Change 7, 755. <https://doi.org/10.1038/nclimate3432>
- Oehler, F., Oliveira, S., Barredo, J. I., Camia, A., Ayanz, J., Pettenella, D., Mavsar, R., 2012. Assessing European wildfire vulnerability. In EGU General Assembly Conference Abstracts (Vol. 14, p. 9452).
- Oliveira, S., Félix, F., Nunes, A., Lourenço, L., Laneve, G., Sebastián-López, A., 2018. Mapping wildfire vulnerability in Mediterranean Europe. Testing a stepwise approach for operational purposes. Journal of environmental management, 206, 158-169. <https://doi.org/10.1016/j.jenvman.2017.10.003>
- Pastor, E., Muñoz, J.A., Caballero, D., Àgueda, A., Dalmau, F., Planas, E., 2019. Wildland-urban interface fires in Spain: summary of the policy framework and recommendations for improvement. Fire Technology. <https://doi.org/10.1007/s10694-019-00883-z> INRMM-MiD:z-2JBBFPHW
- Pesaresi M., Ehrlich, D., Ferri, S., Florczyk, A.J., Freire, S., Halkia, S., Julea, A.M., Kemper, T., Soille, P., Syrris, V., 2016. Operating procedure for the production of the Global Human Settlement Layer from Landsat data of the epochs 1975, 1990, 2000, and 2014. Publications Office of the European Union, Luxembourg. ISBN: 978-92-79-55012-6 , <https://doi.org/10.2788/253582>
- Pettinari, M. L., Chuvieco, E., 2016. Generation of a global fuel data set using the Fuel Characteristic Classification System. Biogeosciences 13(7), 2061-2076. <https://doi.org/10.5194/bg-13-2061-2016>
- San-Miguel-Ayanz, J., Carlson, J. D., Alexander, M., Tolhurst, K., Morgan, G., Sneeuwjagt, R., Dudley, M., 2003. Current methods to assess fire danger potential. In: Wildland Fire Danger Estimation and Mapping. Vol. 4 of Series in Remote Sensing, World Scientific, pp. 21-61. [https://doi.org/10.1142/9789812791177\\_0002](https://doi.org/10.1142/9789812791177_0002)
- San-Miguel-Ayanz, J., Costa, H., de Rigo, D., Libertà, G., Artés Vivancos, T., Houston Durrant, T., Nuijten, D., Löffler, P., Moore, P., et al., 2018. Basic criteria to assess wildfire risk at the Pan-European level. Publications Office of the European Union, Luxembourg. ISBN 978-92-79-98200-2, <https://doi.org/10.2760/052345>
- Scott, J. H., Burgan, R. E., 2005. Standard fire behavior fuel models: a comprehensive set for use with Rothermel's surface fire spread model. General Technical Report RMRS-GTR-153. Fort Collins, CO: U.S. Department of Agriculture, Forest Service, Rocky Mountain Research Station, General Technical Report RMRS-GTR-153, <https://doi.org/10.2737/RMRS-GTR-153>
- UNISDR, 2009. Terminology on disaster risk reduction. United Nations International Strategy for Disaster Reduction (UNISDR). <https://doi.org/978-600-6937-11-3>

UNISDR, 2015. Sendai Framework for Disaster Risk Reduction 2015-2030.  
<https://sustainabledevelopment.un.org/frameworks/sendaiframework>

Van Wagner, C.E., 1987. Development and structure of the Canadian Forest Fire Weather Index System. Vol. 35 of Forestry Technical Report. Canadian Forestry Service, Ottawa, Canada.

<https://cfs.nrcan.gc.ca/publications?id=19927> Yebra, M., Dennison, P. E., Chuvieco, E., Riano, D., Zylstra, P., Hunt Jr, E. R., Danson F. M., Jurdao, S., 2013. A global review of remote sensing of live fuel moisture content for fire danger assessment: moving towards operational products. *Remote Sensing of Environment* 136, 455-468.  
<https://doi.org/10.1016/j.rse.2013.05.029>

## 13 Biodiversity loss

MARINE ROBUCHON, CHRISTINE ESTREGUIL, ALEXANDRA MARQUES

### 13.1 Context of Risk Assessment/Introduction

Biodiversity corresponds to the variety among all living organisms on Earth and the ecological complexes of which they are part of: this includes diversity within species, between species and of ecosystems. Besides having an intrinsic value, **biodiversity is a vital asset for human societies** as it provides essential services for human existence and well-being (Millennium Ecosystem Assessment, 2005). This includes provisional services (e.g. provision of food, medicine, and energy), regulation services (e.g. regulation of climate, air quality, and water quality) and cultural services (e.g. spiritual, recreational and educational). Currently, unsustainable use of natural resources is **driving biodiversity to decline worldwide faster than at any time in human history, putting at risk current and future well-being** (IPBES, 2019).

The prevention of biodiversity loss has been at the core of multiple international and European policies since the 1990's. Biodiversity policies are also intertwined with other sectoral policies on agriculture, forests, fisheries, climate, environment, trade, transport and regional development. Even though we focus here on EU biodiversity policies, these EU policies comply with international targets on biodiversity loss<sup>54</sup> and sustainable development<sup>55</sup>. The EU Biodiversity Strategy to 2020<sup>56</sup> aims at halting biodiversity loss in the EU and helping stop global biodiversity loss by 2020. It comprises six targets: protect species and habitats, maintain and restore ecosystems, achieve more sustainable agriculture and forestry, make fishing more sustainable and seas healthier, combat invasive alien species and help stop the loss of global biodiversity.

The legal instruments to reach these objectives are:

- the Birds and Habitats Directives (Directive 2009/147/EC<sup>57</sup> and Habitats Directive 92/43/EEC<sup>58</sup>); the protected areas designed under these directives form the Natura 2000 network<sup>59</sup>, which is the largest coordinated network of protected areas in the world
- the Zoos Directive (Directive 1999/22/EC<sup>60</sup>), seeking to promote the protection and conservation of wild animal species by strengthening the role of zoos in the conservation of biodiversity
- the Invasive Species Regulation (Regulation No 1143/2014<sup>61</sup>), providing a set of measures to be taken across the EU in relation to invasive alien species included on the list of Invasive Alien Species of Union concern<sup>62</sup>
- the Wildlife Trade Legislation with two regulations and one directive (Regulation No 1007/2009<sup>63</sup>, Regulation No 3254/91<sup>64</sup>, Directive 83/129/EEC<sup>65</sup>) which derive from the Convention on International Trade in Endangered Species (CITES)<sup>66</sup>
- the Water Framework Directive (Directive 2000/60/EC<sup>67</sup>), providing a framework for the protection of inland surface waters, transitional waters, coastal waters and groundwater
- the Marine Strategy Framework Directive (Directive 2008/56/EC<sup>68</sup>), aiming to protect more effectively the marine environment across Europe.

Non-binding commitments have also been taken to reach the objectives of the EU Biodiversity Strategy to 2020:

---

<sup>54</sup> <https://www.cbd.int>

<sup>55</sup> <https://www.un.org/sustainabledevelopment/sustainable-development-goals/>

<sup>56</sup> [https://ec.europa.eu/environment/nature/biodiversity/strategy/index\\_en.htm](https://ec.europa.eu/environment/nature/biodiversity/strategy/index_en.htm)

<sup>57</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0147>

<sup>58</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31992L0043>

<sup>59</sup> [https://ec.europa.eu/environment/nature/natura2000/index\\_en.htm](https://ec.europa.eu/environment/nature/natura2000/index_en.htm)

<sup>60</sup> [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.1999.094.01.0024.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.1999.094.01.0024.01.ENG)

<sup>61</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1417443504720&uri=CELEX:32014R1143>

<sup>62</sup> [https://ec.europa.eu/environment/nature/invasivealien/list/index\\_en.htm](https://ec.europa.eu/environment/nature/invasivealien/list/index_en.htm)

<sup>63</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009R1007>

<sup>64</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31991R3254>

<sup>65</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31983L0129>

<sup>66</sup> <https://www.cites.org/>

<sup>67</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32000L0060>

<sup>68</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0056>

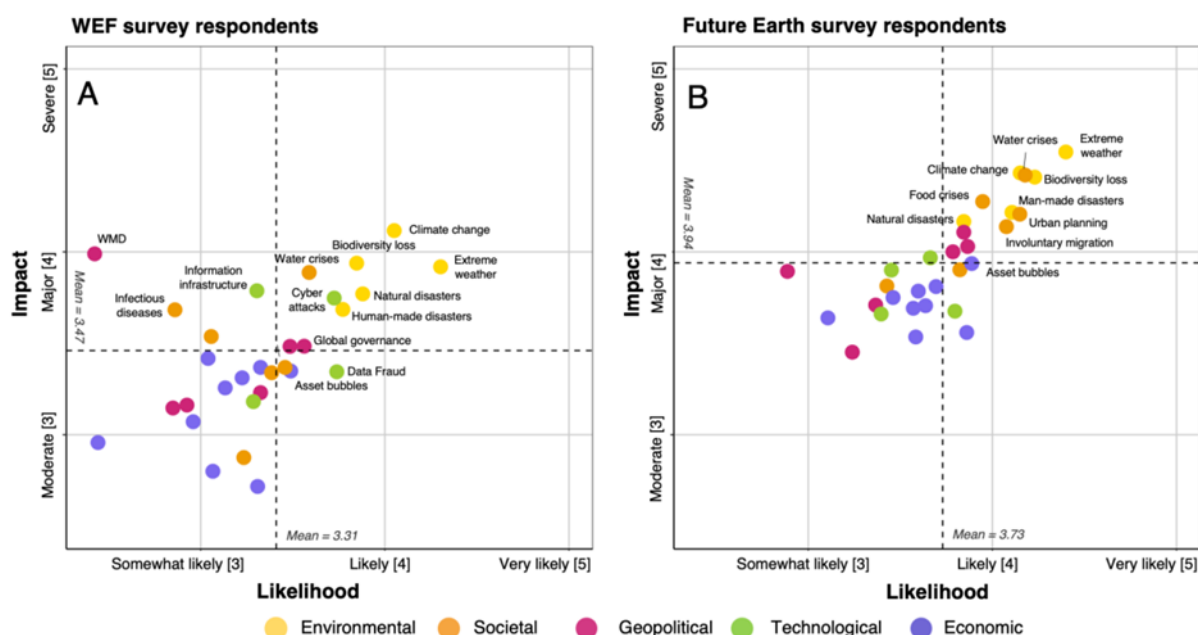


- the Green Infrastructure (GI) Strategy<sup>69</sup>, aiming at encouraging the deployment of green (and blue) infrastructure at European and Member States level, as a strategically planned network of natural and semi-natural areas in both urban and rural context, to help biodiversity to recover and strengthen the delivery of multiple ecosystem services
- the EU pollinators initiative<sup>70</sup>, which sets strategic objectives and a set of actions to be taken by the EU and its Member States to address the decline of pollinators in the EU and contribute to global conservation efforts.

The new, recently-adopted EU Biodiversity Strategy to 2030<sup>71</sup> builds on these legal instruments and non-binding commitments and proposes new ones - such as legally-binding restoration targets to be adopted in 2021 - to take action into four areas: protect nature, restore ecosystems, enhance transformative change, and ensure a high level of EU ambition and mobilize all efforts for the good of the world's biodiversity. As all these new instruments are not in place yet at the time of writing, the reader is encouraged to follow them up, notably via consulting the Knowledge Centre for Biodiversity<sup>72</sup>.

Recent major reports have highlighted **the risk that biodiversity loss represents for human well-being by altering the services biodiversity provides**: (1) the global and regional assessment reports on biodiversity and ecosystem services of the Intergovernmental Science-Policy Platform on Biodiversity and Ecosystem Services (IPBES; Brondizio et al., 2019; IPBES, 2018) providing independent, interdisciplinary and extensive reviews on the status, trends, and future of the links between people and nature (Díaz et al., 2019), (2) the global risks assessment report of the World Economic Forum (WEF; World Economic Forum, 2020), based on a survey of business leaders on their perception of global risks, and (3) the risk perceptions report of the global network of scientists Future Earth (FE; Future Earth, 2020), based on a survey of scientists on their perception of global risks.

**Figure 26.** The Global Risks Landscape 2020 perceived by business leaders (A) and by scientists (B).



Source: Garschagen et al., 2020

The scientific, political, and economic contexts all converge in identifying biodiversity loss as a major global risk that needs urgent consideration. The WEF and FE surveys respectively ranked it at the top 3<sup>rd</sup> and 4<sup>th</sup> risk in terms of impact and at the top 4<sup>th</sup> and 2<sup>nd</sup> risk in terms of likelihood (**Figure 26**). Business leaders tended

<sup>69</sup> [https://ec.europa.eu/environment/nature/ecosystems/strategy/index\\_en.htm](https://ec.europa.eu/environment/nature/ecosystems/strategy/index_en.htm)

<sup>70</sup> [https://ec.europa.eu/environment/nature/conservation/species/pollinators/index\\_en.htm](https://ec.europa.eu/environment/nature/conservation/species/pollinators/index_en.htm)

<sup>71</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590574123338&uri=CELEX:52020DC0380;>

[https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal/actions-being-taken-eu/eu-biodiversity-strategy-2030\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal/actions-being-taken-eu/eu-biodiversity-strategy-2030_en)

<sup>72</sup> [https://knowledge4policy.ec.europa.eu/biodiversity\\_en](https://knowledge4policy.ec.europa.eu/biodiversity_en)

to underestimate the urgency compared to scientists (Garschagen et al., 2020). Both surveys further highlighted that biodiversity loss was connected to four other global risks: climate change, extreme weather, food crises and water crises. These results justify to now and for the first time addressing explicitly the risk of biodiversity loss within the Recommendations for National Risk Assessment.

This chapter is mainly built upon the findings and recommendations from the IPBES global and regional reports (IPBES, 2018; Brondízio et al., 2019), and **the reader is strongly encouraged to read the IPBES reports** for further insight.

## 13.2 Risk identification

The IPBES global and regional assessment reports (Brondízio et al., 2019; IPBES, 2018) provide the **most extensive and up-to-date information** (more than 15.000 scientific publications) **on past biodiversity loss, the direct and indirect drivers of biodiversity decline, and risk of biodiversity loss under different future scenarios**. Importantly, each main finding of the IPBES assessments – including the figures reproduced in this chapter – is **associated with a level of uncertainty** (see Appendix 2 in IPBES, 2019; Figure 27 and Figure 28). The uncertainty level is low for findings with a confidence level finding “well-established”, intermediate findings “established but incomplete” or “unresolved”, and high for findings “inconclusive”. For the later, major knowledge gaps in biodiversity inventories, status, variables, and scenarios are further detailed in chapter 13.6. The IPBES reports consider the services that biodiversity provides to humans through the lens of **nature’s contributions to people** (NCPs), referring to all the contributions that humanity obtains from nature, which conveniently coincide with the SDGs (see Chapter 3 in Brondízio et al., 2019).

### 13.2.1 Past trends in biodiversity and NCPs

Globally, most of the >50 indicators used to assess past trends in biodiversity since 1970 show a **net deterioration** (see Chapter 2 in Brondízio et al., 2019). This holds true for indicators documenting **ecosystem structure** (the distribution of natural ecosystems on Earth), **community composition** (assemblage of plant, animal and other species that are interacting in a unique habitat), **species populations** (abundance and distribution of a species’ population), **organismal traits** (characteristics of plant and animal species describing how they uptake, use and allocate resources), and **genetic composition** (diversity in genes within and between species). For instance, **natural ecosystems have declined by 47%** on average, relative to their earliest estimated states; **the abundance of naturally-present species has declined by 23%** on average in terrestrial communities; and **the global biomass of mammals has fallen by 82%**.

The observed declines in biodiversity have resulted in declining NCPs for 14 out of the 18 categories: while more food, energy and materials than ever before are now being supplied to people in most places, this frequently undermines nature’s many other contributions such as pollination and regulation of air and freshwater quality.

In Europe and Central Asia, including the sub-regions of Western and Central Europe that encompass all EU countries, trends in biodiversity between 1950 and 2016 are quite similar to global ones: **biodiversity is deteriorating in all ecosystems** (IPBES, 2018; **Figure 27**). The mid-term review assessing progress under the EU biodiversity strategy<sup>73</sup> and the state and outlook reports from the European Environment Agency (EEA, 2019, 2015) indicate that, as compared with the EU 2010 biodiversity baseline, **EU continues to lose biodiversity at an alarming rate**. In marine ecosystems, **the abundance, range and habitat size of many species is shrinking** under human pressures. Nonetheless, some **positive trends** have been detected recently, such as increases in some fish stocks in the North Sea and in plankton diversity in the Black Sea. Such positive trends, due to improved fishing practices, the establishment of marine protected areas and a reduction in eutrophication, show that **conservation policies work when they are implemented**. In freshwater ecosystems, **lakes, ponds and streams are altered and disappearing**. The extent of wetlands in Western, Central and Eastern Europe has declined by 50 per cent from 1970, while **71 per cent of fish and 60 per cent of amphibians with known population trends have been declining** over the last decade. In terrestrial ecosystems, species and habitats have long-term declining trends in population size,

<sup>73</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015DC0478>

range, habitat intactness and functioning. However, the conservation status of some species and habitats that benefited from targeted conservation measures (e.g. large felids or bird species listed on the EU Birds Directive) has improved, providing further evidence that conservation policies can work.

Similarly to the global trends, biodiversity declines in Europe and Central Asia has resulted in the alteration of NCPs (**Figure 28**). There are **negative trends for the majority of nature's regulating, and some non-material, contributions to people**. Importantly, the population of Europe and Central Asia uses more natural resources than are produced within the region, and depends on net imports of natural resources. Some of these imports **negatively affect biodiversity and NCPs in other parts of the world**. This is why **the assessment of biodiversity loss at the EU level and within EU countries should not only consider the EU territories but encompass the entire globe**.

**Figure 27.** Assessment of past (~1950–2000) and current (~2001–2017) trends in biodiversity status of marine, inland surface water and terrestrial ecosystems for the four sub-regions and the whole of Europe and Central Asia.

WE = Western Europe, CE = Central Europe, EE = Eastern Europe, CA = Central Asia, ECA = Europe and Central Asia (EU countries belong to either WE or CE). These trends are based on the expert assessment of available indicators of habitat intactness, species richness and the status of endangered species, and are categorised into 3 confidence levels: “well-established” when the finding is based on many converging studies, “established but incomplete” when the finding is based on a limited number of studies, and “unresolved” when multiple independent studies exist but their conclusions do not agree, and “inconclusive” when there is limited evidence and a recognition of major knowledge gaps.

		PAST					PRESENT				
		WE	CE	EE	CA	ECA	WE	CE	EE	CA	ECA
TERRESTRIAL	Agroecosystems	↘	↘	↘	↘	↘	↘	↘	↕	↕	↘
	Alpine and subalpine systems	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘
	Boreal peatlands	↘	•	↘	•	↘	↘	•	↘	•	↘
	Deserts	↘	•	↘	↘	↘	↘	•	↘	↘	↘
	Forest-steppe, steppe and other southern peatlands	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘
	Mediterranean forests and scrubs	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘
	Pernafrost peatlands	→	•	→	•	→	↘	•	↘	•	↘
	Snow and ice-dominated systems	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘
	Subterranean habitats	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘
	Temperate and boreal forests and woodlands	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘
	Temperate grasslands	↘	↘	↘	↘	↘	↘	↘	↕	↕	↕
	Temperate peatlands	↘	↘	↘	•	↘	→	→	→	•	→
	Tropical and subtropical dry and humid forests	↘	↘	↘	↘	↘	↕	↕	↕	↕	↕
	Tundra	↘	•	↘	•	↘	↘	•	↘	•	↘
	Urban ecosystems	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘
INLAND SURFACE WATER	Aral Sea	•	•	•	↘	↘	•	•	•	↘	↘
	Caspian Sea	•	•	↘	↘	↘	•	•	↘	↘	↘
	Inland surface water	↘	↘	↘	↘	↘	↘	↕	↘	↘	↘
	Saline lakes	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘
MARINE	North East Atlantic	Baltic Sea		Mediterranean Sea	Black and Azov Seas	Arctic Ocean	North West Pacific Ocean		ECA deep-sea		
	PAST	↘	↘	↘	↘	↕	↘	↕			
PRESENT	↘	↘	↘	↘	↘	↘	↘	↘			

Strong and consistent increase in indicator	Strong and consistent decrease in indicator	Stable indicator	Confidence level	Well established
Moderate and consistent increase in indicator	Moderate and consistent decrease in indicator	Variable trend in indicator		Established but incomplete/unresolved
		Not applicable		Inconclusive

Source: IPBES, 2018

**Figure 28.** Trends in nature's contributions to people (1960–2016) for Europe and Central Asia and the sub-regions

WE = Western Europe, CE = Central Europe, EE = Eastern Europe, CA = Central Asia, ECA = Europe and Central Asia (EU countries belong to either WE or CE). These trends reveal a decrease in 6 out of the 14 assessed NCPs in WE, and 7 out of the 14 assessed NCPs in CE.

		WE	CE	EE	CA	ECA
REGULATING NATURE'S CONTRIBUTIONS TO PEOPLE	Habitat maintenance	↘	↘	↘		↘
	Pollination	↘	↘	↘		↘
	Regulation of air quality	↕	↗	↗	↕	↗
	Regulation of climate	↗	↕	↗	↕	↕
	Regulation of ocean acidification					↕
	Regulation of freshwater quantity	↘	↕	↘	↘	↘
	Regulation of freshwater quality	↘	↘	↘		↘
	Formation and protection of soils	↘	↘	↘	↘	↘
	Regulation of coastal and fluvial floods	↕	↘	↘	↕	↘
	Regulation of organisms (removal of carcasses)	↗	↕	↗	↗	↗
MATERIAL NATURE'S CONTRIBUTIONS TO PEOPLE	Food	↗	↗	↗	↗	↗
	Biomass-based fuels	↗	→	→		↗
	Materials (wood and cotton)	→	→	→	→	→
NON-MATERIAL NATURE'S CONTRIBUTIONS TO PEOPLE	Learning derived from indigenous and local knowledge	↘	↘	↘	↘	↘
	Physical and psychological experiences	↕	↘	↘		↕
	Supporting identities					↕

↗ Increase

↘ Decrease

→ Stable

↕ Variable

Lack of evidence

Confidence level

↗ Well established

→ Established but incomplete/unresolved

→ Inconclusive

Source: IPBES, 2018

### 13.2.2 Risk drivers, exposure and capacities

Global declines in biodiversity and NCPs are due to **5 main direct drivers**, which are (by order of importance):

1. **Land/sea use change** and its consequences, including an increasing fragmentation and thus decreasing connectivity of natural and semi-natural areas
2. **Direct exploitation** (first driver of biodiversity decline for the marine realm) and its consequences, including land degradation
3. **Climate change** associated with global warming and changes in weather patterns
4. **Pollution** (e.g. plastics, nutrients) and its consequences, including eutrophication (i.e. the enrichment of water by nutrients resulting in degraded water quality)
5. **Invasive alien species** (plants, animals, pathogens and other organisms that are non-native to an ecosystem and which may cause economic or environmental harm or adversely affect human health).

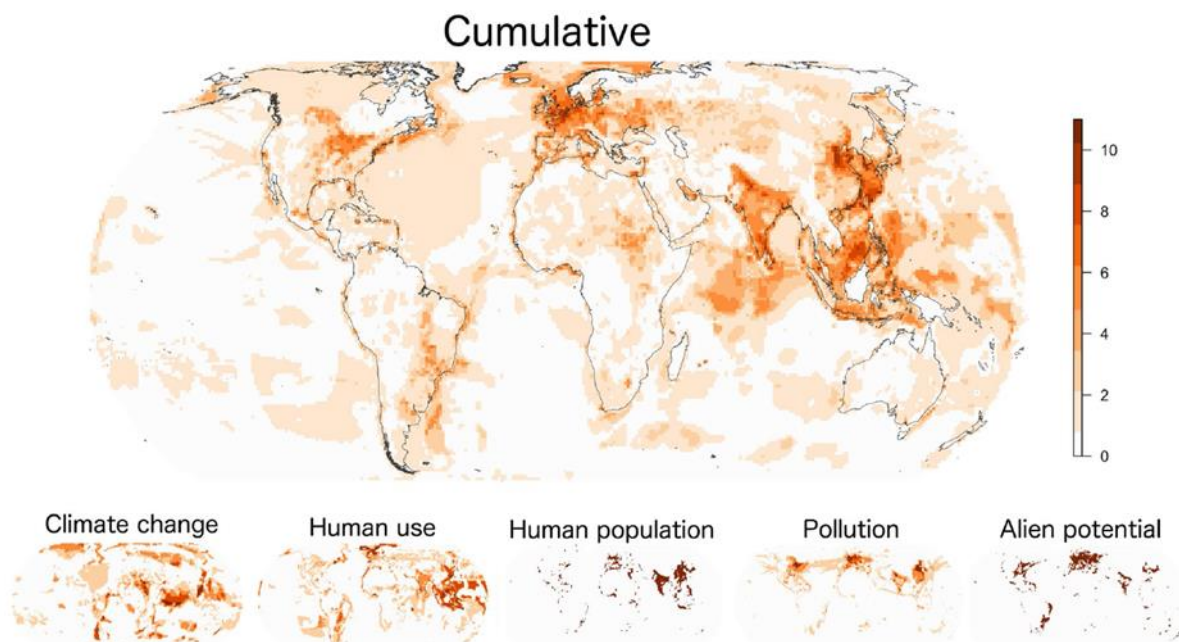
Such direct drivers result from an array of underlying societal causes (e.g. human population dynamics, land demand, consumption patterns, trade) which are called **indirect drivers**.

The direct drivers of decline in biodiversity and NCPs in Europe and Central Asia are the same than at the global scale, although their relative importance is not as clear. **Land-use change** is one of the major direct

drivers of biodiversity and NCPs declines, and, although protected areas have expanded, this alone cannot prevent biodiversity loss. The impact of **climate change** on biodiversity and NCPs is increasing rapidly and is likely to be among the most important drivers in the future, in particular **in combination with other drivers. Natural resource extraction, pollution and invasive alien species** continue to negatively impact biodiversity and NCPs.

The **drivers (direct and indirect) of biodiversity decline can be interpreted as the hazards biodiversity is facing**. Bowler et al. (2020) used the best available knowledge to comprehensively map these hazards across the planet, first individually and then cumulatively (**Figure 29**). This study is very relevant to **identify where biodiversity is highly exposed to one or several hazards** at large-scale. For instance, marine and terrestrial biodiversity in EU countries is highly exposed to multiple hazards, especially non-climatic hazards such as human use (combining land/sea use change and direct exploitation), pollution and alien potential (a proxy for invasive alien species). This study provides a methodological framework that can be replicated at finer scale - such as the national scale - when finer-scale spatially explicit data about hazards are available.

**Figure 29.** Regions of the world exposed to high intensities of multiple drivers. The main map shows the number of the 16 driver variables for which each grid cell was in the highest 10% of values within each realm. Regions in the darkest orange are exposed to high intensities of multiple variables, whereas those in off-white are exposed to lower intensities (i.e. within the 90% quantile of values) of all variables. The smaller plots below show the same for each of the separate drivers.



Source: Bowler et al., 2020

Within and among the EU Member States, the currently available **capacities** to strengthen biodiversity resilience and decrease the risk of biodiversity loss mainly target direct drivers of biodiversity loss and include (non-exhaustive list):

1. the establishment of a network of **protected areas** well connected and well managed to prevent further land/sea use change; this has been initiated under the impulsions of the Birds and Habitats Directives and the GI Strategy, and the Natura 2000 protected sites network now form the backbone of GI for Europe
2. the **maintenance or restoration of natural or semi-natural areas** outside protected areas to prevent further land/sea use change or mitigate it; this has been initiated by mainstreaming the EU Biodiversity Strategy and the GI Strategy within national sectoral policies of agriculture and forestry, water management and disaster risk reduction, spatial planning and territorial development including rural, urban and transport; together with protected areas, natural areas



form a multifunctional and connected GI network that provides multiple benefits<sup>74</sup>, help prioritising conservation and restoration actions and can be implemented at European, national<sup>75</sup> and regional scale (Estreguil et al., 2019).

3. the **regulation of natural resource extraction** to limit direct exploitation via the Common Fisheries Policy<sup>76</sup> and national forest policies<sup>77</sup>
4. the **regulation on wildlife trade** after the EU Wildlife trade legislation and the CITES to limit direct exploitation
5. the **regulation restricting the use of three neonicotinoids**<sup>78</sup> to limit the harmful effects of these pollutants on pollinators
6. the implementation of **carbon taxes** as a mean to incite reducing carbon emissions; the EU emissions trading system<sup>79</sup> operates in all EU countries to limit emissions from heavy energy-using installations and airlines, and 15 Member States have additionally implemented a national carbon tax to date<sup>80</sup>
7. the use of **pollution taxes** as a mean to incite limiting emissions to air or effluents to water (such as EU Nitrates Directive<sup>81</sup>), reducing and better recycling waste (EEA, 2016)
8. the **reward of biodiversity-friendly agricultural practices** through agri-environment schemes and other rural development measures from the **Common Agriculture Policy**<sup>82</sup> (e.g. sources of funding enabling farmers to protect wildlife habitats on agricultural land<sup>83</sup>), and the application of **penalties for non-compliance to EU standards** on good agricultural and environment condition on land and to sustainable management requirements
9. nature-based solutions promoting biodiversity, and sustainable use of land<sup>84</sup> within the urban context, e.g. “re-naturing” cities and “innovating with nature” for more sustainable and resilient societies
10. preventive, eradication and management measures to avoid limit and mitigate the effects of invasive alien species through the EU Regulation on Invasive Alien Species.

### 13.3 Risk analysis

There are several **qualitative and quantitative** methodologies to analyse the risk of biodiversity loss, which differ in regarding **the drivers they address** and the **biodiversity indicator(s)** they use to characterize the impact. To best picture of risk, the methodology should be **quantitative, address all the drivers** of biodiversity loss and document the impacts using a **set of indicators** that comprehensively represent biodiversity and the services it provides under **multiple scenarios** (UNISDR, 2017). However, such methodology does not exist yet. Best methodologies currently available are quantitative but they address a limited number of drivers.

For example, the IPBES global assessment report (IPBES, 2019) used multiple models to forecast the combined **impacts of land use and climate change on biodiversity and NCPs** in the different regions of the world. Three scenarios archetypes are proposed (**Figure 30**) and can be described as follows (see chapter 4 in Brondízio et al., 2019):

1. **global sustainability** combines proactive environmental policy and sustainable production and consumption with low greenhouse gas emissions

<sup>74</sup> [https://ec.europa.eu/environment/nature/ecosystems/benefits/index\\_en.htm](https://ec.europa.eu/environment/nature/ecosystems/benefits/index_en.htm)

<sup>75</sup> <https://biodiversity.europa.eu/countries/#overview>

<sup>76</sup> [https://ec.europa.eu/fisheries/cfp\\_en](https://ec.europa.eu/fisheries/cfp_en)

<sup>77</sup> <https://ec.europa.eu/environment/forests/fpolicies.htm>

<sup>78</sup> [https://ec.europa.eu/food/plant/pesticides/approval\\_active\\_substances/approval\\_renewal/neonicotinoids\\_en](https://ec.europa.eu/food/plant/pesticides/approval_active_substances/approval_renewal/neonicotinoids_en)

<sup>79</sup> [https://ec.europa.eu/clima/policies/ets\\_en](https://ec.europa.eu/clima/policies/ets_en)

<sup>80</sup> <https://taxfoundation.org/carbon-taxes-in-europe-2019/>

<sup>81</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561542776070&uri=CELEX:01991L0676-20081211>

<sup>82</sup> [https://ec.europa.eu/environment/nature/rbaps/index\\_en.htm](https://ec.europa.eu/environment/nature/rbaps/index_en.htm) and <https://ec.europa.eu/info/food-farming-fisheries/sustainability-and-natural-resources/agriculture-and-environment/cap-and-environment>

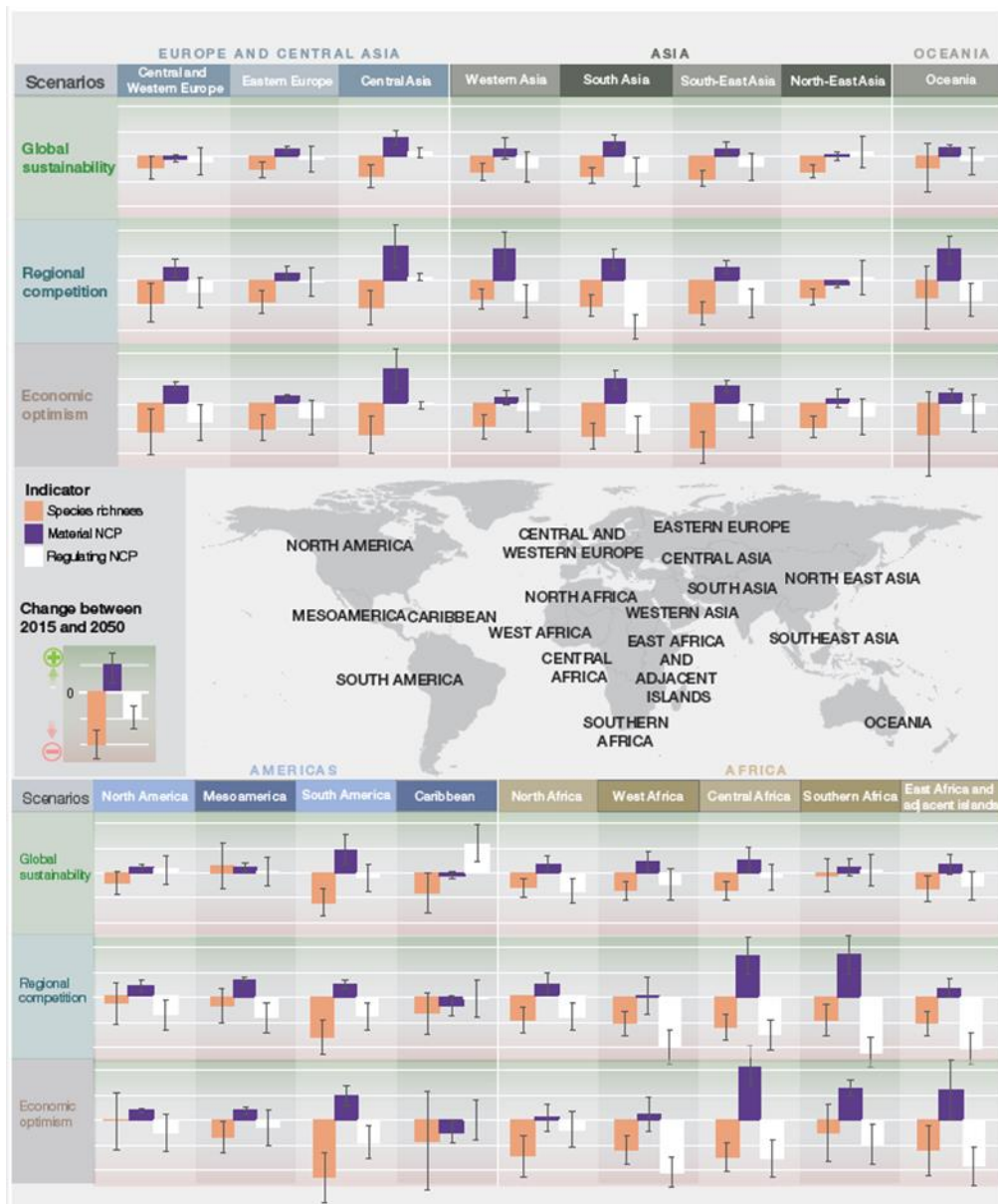
<sup>83</sup> [https://ec.europa.eu/environment/nature/rbaps/index\\_en.htm](https://ec.europa.eu/environment/nature/rbaps/index_en.htm)

<sup>84</sup> [https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/priority-themes-eu-cities/sustainable-use-land-and-nature-based-solutions-cities\\_en#eu-legislation](https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/priority-themes-eu-cities/sustainable-use-land-and-nature-based-solutions-cities_en#eu-legislation)

2. **regional competition** combines strong trade and other barriers and a growing gap between rich and poor with high emissions.
3. **economic optimism** combines rapid economic growth and low environmental regulation with very high greenhouse emissions.

They can be interpreted qualitatively or quantitatively in terms of possible futures for drivers of biodiversity loss (e.g. Kim et al., 2018). The results show that **biodiversity and nature’s regulating contributions to people are projected to decline further in most scenarios** of global change over the coming decades, while the supply and demand for nature’s material contributions to people that have current market value (food, feed, timber and bioenergy) are projected to increase. However, **the magnitude of the impacts on biodiversity and NCPs is expected to be smaller in the scenario of global sustainability**.

**Figure 30.** Projections of the impacts of land use and climate change on biodiversity (measured as change in species richness across a wide range of terrestrial plant and animal species at regional scales) and nature’s material (food, feed, timber and bioenergy) and regulating (nitrogen retention, soil protection, crop pollination, crop pest control and ecosystem carbon storage and sequestration) contributions to people between 2015 and 2050.



Source: IPBES, 2019



Quantitative forecast modelling can also be conducted at **smaller spatial scales**. For instance, Princé et al. (2015) modelled the combined impacts of land-use and climate change on bird population sizes in France, and found that land-use scenarios based on **the extensification of agricultural systems had the potential to mitigate the negative impacts due to climate change**.

Quantitative approaches can be **complemented by more qualitative ones using evidence based literature** like for instance, in the IPBES regional assessment for Europe and Central Asia (IPBES, 2018) where results showed trade-offs between the different biodiversity indicators and related NCPs. The scenarios for Western and Central Europe, which prioritized an increase in food provision through agricultural expansion or intensification, led to trade-offs with regulating contributions to people and biodiversity. The scenarios assuming pro-active environmental decision-making and cooperation between countries or regions were the most effective in mitigating these negative trade-offs and could even lead to mostly positive impacts on biodiversity and NCPs.

Importantly, the three above mentioned examples and most scientific studies **only consider a few drivers** in scenarios of biodiversity loss (mostly climate change and land-use) so they likely **underestimate the projected (negative) impacts**.

The most appropriate method to carry out risk analysis at the national scale would be to:

1. identify available risk analyses at global (e.g. IPBES, 2019), regional (e.g. IPBES, 2018) and national (e.g. Princé et al., 2015) scales, check the predictions of these existing analyses for the country and assess the knowledge gaps (see chapter 13.6); if knowledge gaps are important, pursue efforts to fill these gaps with a new risk analysis by following steps 2 to 6
2. gather existing future scenarios (or create new ones) for the national drivers of biodiversity loss (see chapter 13.2.2 for a check-list), including indirect drivers that may impact biodiversity outside the country (e.g. trade and consumption patterns)
3. gather existing biodiversity data on the current distribution of species and ecosystems in the country and in countries involved for trade and consumption
4. assess knowledge gaps in existing biodiversity inventories, status and variables, notably by groups (e.g. mammals, birds, invertebrates, plants, microorganisms) and by realms (marine, freshwater, terrestrial)
5. combine drivers for which quantitative future trends are available (gathered in step 2) with biodiversity data (gathered in step 3) to model and forecast the combined effect of drivers following and adapting the protocol proposed by Kim et al. (2018)
6. for drivers for which quantitative future trends are not available (gathered in step 2), and for groups and realms not comprehensively known (identified in step 4), conduct an expert based qualitative assessment of future trends in drivers and biodiversity.

Risk analysis of biodiversity loss, especially quantitative modelling of projected impacts, is very demanding in terms of technical and analytical skills. It is recommended to **include experts in biodiversity conservation**.

Two additional aspects are worth consideration when conducting risk analysis. The first one is related to **thematic interlinkages of risks**. Biodiversity loss is **strongly related to other major risks**, either because these other major risks are also drivers of biodiversity loss, or because biodiversity loss and these other major risks share the same underlying drivers. As such, climate change is one of the main drivers of biodiversity loss, while biodiversity can mitigate negative effects of climate change (e.g. healthy forests that reduce atmospheric carbon by fixing it, urban trees helping cities to adapt to higher temperature). **Assessing multiple risks together might therefore yield different results than assessing risk one by one**. Further, as the year 2020 has been profoundly marked by the covid-19 pandemic, it is important to recall that the same human activities that drive biodiversity loss and climate change also drive pandemic risk through their impact on the environment (IPBES, 2020). This implies that **solutions to halt biodiversity loss and fight climate change would also help preventing further pandemics**.

The second one is about **geospatial interlinkages**. Between-country trade linkages should be considered when assessing the drivers of biodiversity loss and gain across countries. For example, EU countries acknowledging forest transition, thus likely leading to reducing the risk of biodiversity loss, displace their land demand outside their borders particularly in tropical countries (e.g. tropical deforestation, thus biodiversity

loss, is embodied in the goods and services they consumed in the EU). There is thus a need to **incorporate a land-balance model** (Pendrill et al., 2019).

### 13.4 Risk Evaluation

Existing risk analyses of biodiversity loss at the global and regional level (see previous section, IPBES 2018, 2019) predict **important losses in biodiversity and regulatory services in most scenarios**. They highlight that **only pro-active environmental policies and strong cooperation between countries and/or regions are able to mitigate those losses**. Such outcomes would probably be similar for any new national risk analysis. This fact further emphasizes **the need to evaluate risk of biodiversity loss within the country itself and also outside its border**.

The outcomes of risk analysis of biodiversity loss should be analysed according to the following risk criteria:

- monetary: how much money will be lost if biodiversity loss is not mitigated? One attempt to put a monetary value on goods and services provided by ecosystems estimates the worth of biodiversity at US\$125 trillion per year (Costanza et al., 2014), i.e. around two-thirds higher than the global Gross Domestic Product. Such exercise has also been carried out at the EU scale for different ecosystem services (Vallecillo et al., 2019, 2018).
- legislation: which policy targets will be missed if biodiversity loss is not mitigated? The IPBES global report (IPBES, 2019) highlights that most international societal and environmental goals, such as the Aichi Targets and the SDGs, will not be achieved based on current trajectories. The last European environment state and outlook (EEA, 2019) reveals that this holds true for most targets of the EU Biodiversity Strategy to 2020 as well.
- effects on services: which services will deteriorate if biodiversity loss is not mitigated? The IPBES reports (IPBES, 2018, 2019) predict important losses in regulatory and cultural services unless pro-active environmental policies and strong cooperation between countries are urgently undertaken.
- societal perception: how do the different actors perceive biodiversity loss? Figure 26 shows that both business leaders and scientists perceive it as very impacting and very likely, and an overwhelming majority of Europeans are concerned about the loss of biodiversity and support stronger EU action to protect nature<sup>85</sup>.

To raise awareness of and buy-in from citizen, industry and political stakeholders, several formats can be used to communicate about the risk of biodiversity loss, such as risk mapping (e.g. **Figure 30**) and tables to represent the expected future trends in different risk indices. Furthermore, risk matrix is a good representation to compare different risks in terms of impact and likelihood (e.g. **Figure 26**).

### 13.5 Risk treatment

#### 13.5.1 Policy responses to biodiversity loss

The broad framework of EU biodiversity policy, including the capacities listed in Chapter 13.2.2, **remains highly relevant** to tackle the direct drivers of biodiversity loss. However, these policies need to be considerably **more widely and effectively implemented** to ensure that the principles included in the policy frameworks are reflected on the ground (EEA, 2019). According to the mid-term review of the Biodiversity Strategy to 2020, this could be achieved by **completing the Natura 2000 network for the marine environment**, ensuring **effective management of Natura 2000 sites** and **implementing the Invasive Alien Species Regulation**, and considering the most suitable approach for **recognizing our natural capital throughout** the EU. The upcoming final review should highlight which policies have been effective and which ones should have been better implemented to halt biodiversity loss.

In addition, and because indirect drivers of biodiversity loss (e.g. the ways we consume, produce and trade natural resources) are linked to a range of economic sectors and sectoral policies, halting biodiversity loss can only be achieved by a more effective **integration of biodiversity concerns across sectors**. This would require a transformation in policies and tax reforms in the region to set **coherent priorities** underpinned by

---

<sup>85</sup> [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_19\\_2360](https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2360)

**adequate funding** (IPBES, 2018). In that line, both EU and Member States could promote developing incentives and widespread capacity for environmental responsibility while eliminating perverse incentives. Mainstreaming biodiversity concerns and including them in sectoral policies is therefore crucial, especially for the post-2020 biodiversity agenda (Whitehorn et al., 2019). These include trade, agriculture, forestry, fisheries, spatial planning, energy, transport, health, tourism and the financial sector, including insurance (EEA, 2019). Such transformation is in line with the new Green Deal for Europe: “All EU policies should contribute to preserving and restoring Europe’s natural capital”<sup>86</sup>, which implies that all actions within and between sectoral policies should be aligned towards that goal. This is reflected in the new EU Biodiversity Strategy to 2030<sup>87</sup>, but also in the Climate Action<sup>88</sup>, the Farm to Fork Strategy<sup>89</sup>, and in the revised circular economy action plan<sup>90</sup>.

### 13.5.2 Socio-economic responses to biodiversity loss

In addition to policy, societal responses to biodiversity loss also play an important role, notably regarding **changes in the patterns of consumption** (e.g. Crenna et al., 2019; Marques et al., 2019). Further efforts are needed to **increase public awareness** of the importance of biodiversity and the services it provides for the well-being of Europeans, so that they may be more prepared to make personal efforts. Beyond individual changes in consumption patterns, this includes **influencing decision-making** with the aims of redefining priorities, achieving more coherent development of policies and stronger policy implementation, to contribute to sustainability transitions accepted by society (EEA, 2019). Implementing **horizon scanning on biodiversity conservation** (e.g. Sutherland et al., 2020) and foresight processes including participatory approaches can also contribute actionable knowledge to support decision-making towards anticipatory governance to mitigate risk of biodiversity loss more efficiently. Finally, by encouraging green jobs and innovation in green technologies, **economic investment in social and human capital for biodiversity** may also provide win-win responses to biodiversity loss.

## 13.6 Gaps and Challenges/Conclusion

The IPBES global and regional assessments (IPBES, 2018, 2019) also provide a detailed list of knowledge gaps that need to be filled to improve quantitative risk analysis of biodiversity loss. They include (among others):

1. Gaps in **biodiversity inventories**. Basic data on many taxa are still lacking: 86 per cent of existing species on Earth and 91 per cent of species in the ocean still await description. Inventories are particularly lacking for the marine, freshwater and soil ecosystems.
2. Gaps in **biodiversity status**. Data on extinction risks and population trends are missing, especially for insects, parasites and fungal and microbial species. Data from monitoring of ecosystem condition are also less well represented than ecosystem extent.
3. Gaps in **biodiversity variables**. Most data collected allow describing species populations and community composition while other essential biodiversity variables – such as genetic composition and ecosystem function – are poorly represented.
4. Gaps in **integrated scenarios**. There is a need to develop quantitative studies about future biodiversity scenarios accounting for multiple drivers of biodiversity loss and their interaction (currently only climate change and/or land use are considered), which integrate the knowledge of indigenous peoples and local communities, and which assess NCPs.
5. Gaps in the **understanding and assessment of diverse biodiversity values**. Biodiversity is difficult to value economically and there is still a lack of awareness of biodiversity potential benefits and its links to economic growth. Beyond the sole economic value, there is a need for better understanding, quantification and integrated monitoring of alternative values of biodiversity and NCPs. There is limited understanding of how these diverse values are endorsed by different

<sup>86</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0640>.

<sup>87</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590574123338&uri=CELEX:52020DC0380>;

[https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal/actions-being-taken-eu/eu-biodiversity-strategy-2030\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal/actions-being-taken-eu/eu-biodiversity-strategy-2030_en)

<sup>88</sup> [https://ec.europa.eu/clima/policies/eu-climate-action\\_en](https://ec.europa.eu/clima/policies/eu-climate-action_en)

<sup>89</sup> [https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal/actions-being-taken-eu/farm-fork\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal/actions-being-taken-eu/farm-fork_en)

<sup>90</sup> [https://ec.europa.eu/commission/presscorner/detail/en/fs\\_20\\_437](https://ec.europa.eu/commission/presscorner/detail/en/fs_20_437)

social groups and genders, which prevents further understanding about people behaviour regarding biodiversity conservation.

Further funding is necessary to fill those gaps, both in terms of research (in taxonomy, ecology and sociology) and monitoring infrastructures. In the meantime, qualitative risk analyses can complement quantitative ones on the gaps identified. Importantly, although these gaps identified at the global and the regional level constitute a good starting point to inventory gaps at the national scale, they do not replace the recommended gap analysis at the national scale (Chapter 13.3). Indeed, a global gap may not be a national gap (if there is comprehensive information at the national scale but not at the global scale) and vice-versa (if there is comprehensive information at the global scale but not at a fine-enough spatial resolution to be used at the national scale).

European cross-sectoral projects and national initiatives encompassing the risk of biodiversity loss are expected in the short term. They should closely be monitored to improve knowledge and assessment tools, and stimulate innovation at EU and national levels.

### 13.7 References

- Bowler, D.E., Bjorkman, A.D., Dornelas, M., Myers-Smith, I.H., Navarro, L.M., Niamir, A., Supp, S.R., Waldock, C., Vellend, M., Blowes, S.A., Böhning-Gaese, K., Bruelheide, H., Elahi, R., Antão, L.H., Hines, J., Isbell, F., Jones, H.P., Magurran, A.E., Cabral, J.S., Winter, M., Bates, A.E., 2020. Mapping human pressures across the planet uncovers anthropogenic threat complexes. *People Nat.* 00, 1–15. <https://doi.org/10.1101/432880>
- Brondízio, E.S., Settele, J., Diaz, S., Ngo, H.T., 2019. Global assessment report on biodiversity and ecosystem services of the Intergovernmental Science-Policy Platform on Biodiversity and Ecosystem Services. IPBES Secretariat.
- Costanza, R., de Groot, R., Sutton, P., van der Ploeg, S., Anderson, S.J., Kubiszewski, I., Farber, S., Turner, R.K., 2014. Changes in the global value of ecosystem services. *Glob. Environ. Chang.* 26, 152–158. <https://doi.org/10.1016/j.gloenvcha.2014.04.002>
- Crenna, E., Sinkko, T., Sala, S., 2019. Biodiversity impacts due to food consumption in Europe. *J. Clean. Prod.* 227, 378–391. <https://doi.org/10.1016/j.jclepro.2019.04.054>
- Díaz, S., Settele, J., Brondízio, E.S., Ngo, H.T., Agard, J., Arneeth, A., Balvanera, P., Brauman, K.A., Butchart, S.H.M., Chan, K.M.A., Lucas, A.G., Ichii, K., Liu, J., Subramanian, S.M., Midgley, G.F., Miloslavich, P., Molnár, Z., Obura, D., Pfaff, A., Polasky, S., Purvis, A., Razzaque, J., Reyers, B., Chowdhury, R.R., Shin, Y.J., Visseren-Hamakers, I., Willis, K.J., Zayas, C.N., 2019. Pervasive human-driven decline of life on Earth points to the need for transformative change. *Science.* 366. <https://doi.org/10.1126/science.aax3100>
- EEA, 2019. The European environment - state and outlook 2020: knowledge for transition to a sustainable Europe. European Environment Agency, Copenhagen. <https://doi.org/10.2800/45773>
- EEA, 2016. Environmental taxation and EU environmental policies, EEA Report No 17/2016. <https://doi.org/10.2800/296823>
- EEA, 2015. The European environment - state and outlook 2015: synthesis report. European Environment Agency, Copenhagen. <https://doi.org/10.2800/944899>
- Estreguil, C., Dige, G., Kleeschulte, S., Carrao, H., Raynal, J., Teller, A., 2019. Strategic Green Infrastructure and Ecosystem Restoration: geospatial methods, data and tools. Publications Office of the European Union, Luxembourg. <https://doi.org/10.2760/36800>
- Future Earth, 2020. Future Earth Risks Perceptions Report 2020 1st Edition.
- Garschagen, M., Wood, S., Garard, J., Ivanova, M., Luers, A., 2020. Too big to ignore: Global risk perception gaps between scientists and business-leaders. *Earth's Futur.* 8, 1–5. <https://doi.org/10.1029/2020ef001498>.
- IPBES, 2020. Workshop Report on Biodiversity and Pandemics of the Intergovernmental Platform on Biodiversity and Ecosystem Services. Daszak, P., das Neves, C., Amuasi, J., Hayman, D., Kuiken, T., Roche, B., Zambrana-Torrelío, C., Buss, P., Dundarova, H., Feferholtz, Y., Foldvari, G., Igbínosa, E., Junglen, S., Liu, Q., Suzan, G., Uhart, M., Wannous, C., Woolaston, K., Mosig Reidl, P., O'Brien, K., Pascual, U., Stoett, P., Li, H., Ngo, H. T., IPBES secretariat, Bonn, Germany, DOI:10.5281/zenodo.4147317

IPBES, 2019. Summary for policymakers of the global assessment report on biodiversity and ecosystem services of the Intergovernmental Science-Policy Platform on Biodiversity and Ecosystem Services. IPBES secretariat, Bonn, Germany.

IPBES, 2018. The IPBES regional assessment report on biodiversity and ecosystem services for Europe and Central Asia. Secretariat of the Intergovernmental Science-Policy Platform on Biodiversity and Ecosystem Services, Bonn, Germany.

Kim, H., Rosa, I.M.D., Alkemade, R., Leadley, P., Hurtt, G., Popp, A., Van Vuuren, D.P., Anthoni, P., Arneth, A., Baisero, D., Caton, E., Chaplin-Kramer, R., Chini, L., De Palma, A., Di Fulvio, F., Di Marco, M., Espinoza, F., Ferrier, S., Fujimori, S., Gonzalez, R.E., Gueguen, M., Guerra, C., Harfoot, M., Harwood, T.D., Hasegawa, T., Haverd, V., Havlik, P., Hellweg, S., Hill, S.L.L., Hirata, A., Hoskins, A.J., Janse, J.H., Jetz, W., Johnson, J.A., Krause, A., Leclère, D., Martins, I.S., Matsui, T., Merow, C., Obersteiner, M., Ohashi, H., Poulter, B., Purvis, A., Quesada, B., Rondinini, C., Schipper, A.M., Sharp, R., Takahashi, K., Thuiller, W., Titeux, N., Visconti, P., Ware, C., Wolf, F., Pereira, H.M., 2018. A protocol for an intercomparison of biodiversity and ecosystem services models using harmonized land-use and climate scenarios. *Geosci. Model Dev.* <https://doi.org/10.5194/gmd-11-4537-2018>

Marques, A., Martins, I.S., Kastner, T., Plutzer, C., Theurl, M.C., Eisenmenger, N., Huijbregts, M.A.J., Wood, R., Stadler, K., Bruckner, M., Canelas, J., Hilbers, J.P., Tukker, A., Erb, K., Pereira, H.M., 2019. Increasing impacts of land use on biodiversity and carbon sequestration driven by population and economic growth. *Nat. Ecol. Evol.* 3, 628–637. <https://doi.org/10.1038/s41559-019-0824-3>

Millennium Ecosystem Assessment, 2005. *Ecosystems and Human Well-being: Synthesis*. Island Press, Washington, DC.

Pendrill, F., Persson, U.M., Godar, J., Kastner, T., Moran, D., Schmidt, S., Wood, R., 2019. Agricultural and forestry trade drives large share of tropical deforestation emissions. *Glob. Environ. Chang.* 56, 1–10. <https://doi.org/10.1016/j.gloenvcha.2019.03.002>

Princé, K., Lorrillière, R., Barbet-Massin, M., Léger, F., Jiguet, F., 2015. Forecasting the effects of land use scenarios on farmland birds reveal a potential mitigation of climate change impacts. *PLoS One* 10, 1–25. <https://doi.org/10.1371/journal.pone.0117850>

Sutherland, W.J., Dias, M.P., Dicks, L. V., Doran, H., Entwistle, A.C., Fleishman, E., Gibbons, D.W., Hails, R., Hughes, A.C., Hughes, J., Kelman, R., Le Roux, X., LeAnstey, B., Lickorish, F.A., Maggs, L., Pearce-Higgins, J.W., Peck, L.S., Pettorelli, N., Pretty, J., Spalding, M.D., Tonneijck, F.H., Wentworth, J., Thornton, A., 2020. A Horizon Scan of Emerging Global Biological Conservation Issues for 2020. *Trends Ecol. Evol.* <https://doi.org/10.1016/j.tree.2019.10.010>

UNISDR, 2017. *Words into Action Guidelines National Disaster Risk Assessment*.

Vallecillo, S., La Notte, A., Kakoulaki, G., Kamberaj, J., Robert, N., Dottori, F., Feyen, L., Rega, C., Maes, J., 2019. Ecosystem services accounting: Part II - Pilot accounts for crop and timber provision, global climate regulation and flood control. Publications Office of the European Union, Luxembourg. <https://doi.org/10.2760/631588>

Vallecillo, S., La Notte, A., Polce, C., Zulian, G., Alexandris, N., Ferrini, S., Maes, J., 2018. Ecosystem services accounting: Part I - Outdoor recreation and crop pollination. Publications Office of the European Union, Luxembourg. <https://doi.org/10.2760/619793>

Whitehorn, P.R., Navarro, L.M., Schröter, M., Fernandez, M., Rotllan-Puig, X., Marques, A., 2019. Mainstreaming biodiversity: A review of national strategies. *Biol. Conserv.* 235, 157–163. <https://doi.org/10.1016/j.biocon.2019.04.016>

World Economic Forum, 2020. *The Global Risks Report 2020*, 15th ed.

## 14 Earthquakes

MARIA LUÍSA SOUSA, GEORGIOS TSIONIS

### 14.1 Context of National Risk Assessment

Earthquake is among the most common hazards assessed in the national risk assessments prepared in 2015<sup>91</sup> and 2018<sup>92</sup> by the countries participating in the Union Civil Protection Mechanism. Indeed, in 2015 19 countries (Austria, Bulgaria, Croatia, Cyprus, France, Germany, Greece, Hungary, Iceland, Italy, Malta, Norway, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, and Sweden) performed a risk assessment for earthquake phenomena and more four countries (Belgium, Netherlands, North Macedonia and United Kingdom) in 2018.

Considering the impact of a single event, earthquakes are among the most devastating natural hazards in history, posing the greatest threat to human life. The effects of earthquakes can vary from localised impacts to dramatic consequences on communities, the economy and the environment, across large regions. In some cases, they can cause cross-border impacts and cascading events, namely tsunamis, landslides, liquefaction phenomena, fire, industrial accidents, business interruption, etc.

Earthquakes may have long-lasting, and in certain cases multi-generational, effects depending on the severity of the event, vulnerability and accumulation of assets in seismic prone areas, individual and societal resilience to disruptive events.

Besides population exposed to seismic risk, the assets that may be impacted by earthquakes include the built environment, for instance, buildings, infrastructures (transportation, water, sewage, energy, communication, etc.), daily life facilities (health facilities, emergency services, educational facilities, etc.), cultural heritage, economic activities, and natural environment.

Earthquake risk analysis has perhaps reached the highest level of maturity among risk analyses for all-natural hazards, in part from the early efforts made by the nuclear industry for taking into account seismic hazard in power plant design (Hills et al., 2013).

Currently, earthquake risk is usually assessed in a fully probabilistic way, though most seismic risk studies do not go further than the determination of the levels of risk for a region, i.e., do not go beyond the risk analysis stage of the risk management process. In practice, the results of seismic risk analysis are sporadically compared with risk criteria to determine whether seismic risks levels are deemed acceptable or tolerable. Chapter 14.4 presents a few examples of seismic risk evaluation criteria useful to assist decisions about risk treatment.

### 14.2 Risk identification

#### 14.2.1 Potential impact of earthquakes and its cause

Ground shaking is the most damaging effect of earthquakes. It results from the passage of seismic waves through the ground, affecting built and natural environments. Ground shaking triggers other hazards, for example, liquefaction and subsidence, which can disrupt lifelines, harbours and originate bridge and building foundation failures. Examples of earthquake-induced environmental effects are rockfalls and landslides. Those were observed to cause significant soil erosion or to block river streams creating quake lakes of major concern to neighbouring urban regions. Severe shallow earthquakes causing vertical displacements on the ocean floor may generate tsunami waves able to produce destruction over large areas. Surface faulting and ground failure can cause the disruption of tunnels, railroads, powerlines, water supply networks and other lifelines. Fires following earthquakes, linked for instance to the rupture of gas mains, are important secondary effects of earthquakes, eventually aggravated by the disruption of water supply systems. Potential disastrous secondary damage caused by earthquakes can also result in Natech events, i.e., natural hazard triggering technological disasters, such as the release of hazardous materials and the destruction of vital transport and technical infrastructure, industrial buildings and facilities. Other examples of earthquake secondary effects are air pollution due to the burning of chemicals, demolition of damaged buildings and traffic congestion after a major earthquake (Gotoh et al., 2002; Lin et al., 2008). In the reconstruction phase, the increased

<sup>91</sup> Commission Staff Working Document on Overview of Natural and Man-made Disaster Risks the European Union may face, SWD(2017) 176 final, Brussels, 23.5.2017.

<sup>92</sup> Commission Staff Working Document on Overview of natural and man-made disaster risks the European Union may face, SWD(2020) 330 final, Brussels, 30.11.2020

demand for construction materials in a very short time may lead to a shortage of natural building materials and subsequently to environmental impacts like coastal erosion, saline intrusion, and illegal mining (Khazai et al., 2006).

The occurrence of a major seismic event in an urban area can have a particularly severe impact, resulting in the complete disruption of economic and social functions in the community. **Table 10** lists important earthquakes that occurred in Europe during the last two decades affecting whole regions and causing significant losses reaching billions of euros.

**Table 10.** Earthquakes in Europe since 2002, for which the EU Solidarity Fund intervened

Occurrence	Country	Category	Damage (million €)
October 2002, Molise	Italy	Regional	1558
April 2009, Abruzzo	Italy	Regional	10212
May 2011, Lorca	Spain	Regional	843
May 2012, Emilia Romagna	Italy	Regional	13274
January 2014, Kefalonia	Greece	Regional	147
November 2015, Lefkada	Greece	Regional	66
August 2016 – January 2017, Central Italy	Italy	Major	21879
June 2017, Lesbos	Greece	Regional	54
July 2017, Kos	Greece	Regional	101

Source: EU Solidarity Fund, 2020 ([http://ec.europa.eu/regional\\_policy/index.cfm/en/funding/solidarity-fund](http://ec.europa.eu/regional_policy/index.cfm/en/funding/solidarity-fund)).

Seismic risk is often expressed in terms of a combination of the magnitude of the consequences of an earthquake and the likelihood of these consequences to occur. It is normally obtained considering the seismic hazard of the site or region, the exposed assets that may be impacted by an earthquake and the vulnerability of those elements at risk, i.e. the vulnerability of different types of buildings or constructions.

This section discusses the main drivers of earthquake risk, i.e. hazard, exposure, and vulnerability.

### 14.2.2 Seismic hazard

Many countries in Europe are exposed to earthquakes, particularly in the South-Eastern part, which is consistent with the main fault lines in Europe located where the Eurasian plate meets the African plate and runs through the Mediterranean Sea.

Earthquake hazard may be assessed using scenario studies (e.g. Coburn and Spence, 2002), or using probabilistic methods for seismic hazard analysis (called PSHA). The latter have evolved significantly in the last decades and are widely used nowadays. Depending on the available data, they make use of historical and instrumental seismic records, seismogenic models, geological and geodetic data, time-dependent trends in earthquake recurrence, and ground motion prediction equations. Uncertainties in seismic hazard assessment originate from the models for the seismogenic source and ground motion, from the parameters used in those models, and from the random nature of seismic events (Silva et al., 2017).

The European Plate Observing System (EPOS)<sup>93</sup>, facilitates integrated use of data, data products, and facilities from distributed research infrastructures for solid Earth science in Europe. EPOS comprises Thematic Core Services that are relevant to seismic hazard assessment, namely on seismology, near-fault observatories, geological data, and modelling. One of the pillars of the EPOS seismology Thematic Core Service is the

<sup>93</sup> [www.epos-ip.org](http://www.epos-ip.org)

network of European Facilities for Earthquake Hazard and Risk (EFEHR)<sup>94</sup>, which provides access to interactive tools, such as seismic hazard models, products and information produced within European research projects like SHARE<sup>95</sup> and SERA<sup>96</sup>.

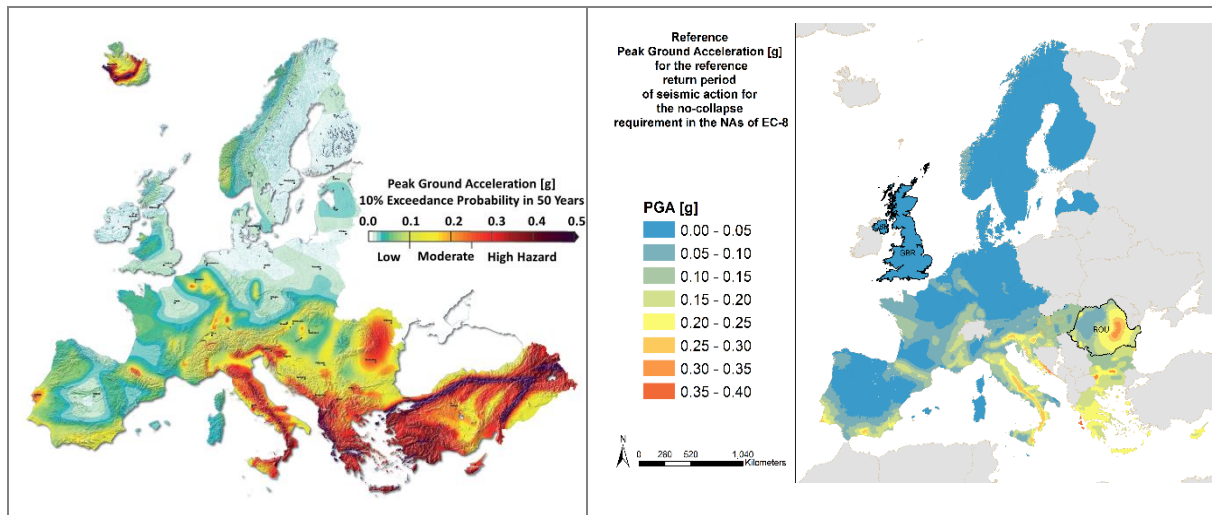
Seismic hazard analysis uses different ground motion prediction equations, leading to results in terms of different intensity measures, for instance, peak ground acceleration, peak ground displacement, spectral acceleration and spectral displacement for the fundamental period of the structure, spectrum intensity, etc.

The analysis is usually carried out for reference rock sites. More reliable site-specific ground motion estimates require geotechnical data and microzonation studies for calculating possible site amplifications. Recently, SERA project has investigated different methods to address soil amplification within seismic risk assessments, from a local to a regional scale (Crowley et al., 2019).

In probabilistic seismic hazard assessment methods, the reference values of intensity measures are calculated for prescribed return periods (e.g. 475 years) or for the probability of exceedance of intensity levels in a period of time (e.g. 10 % in 50 years). A hazard curve provides a relationship between intensity and probability of exceedance. A harmonised seismic hazard model for Europe (Woessner et al., 2015) was produced within the SHARE project (**Figure 31**- left), and is currently being updated and extended in the framework of the SERA project.

Hazard studies serve also as a basis to produce maps of seismic zones for design codes, for example, the Eurocode 8 (CEN, 2004). Within the suite of the Eurocodes<sup>97</sup>, Eurocode 8 applies to the design and construction of buildings and civil engineering works in seismic regions. For this purpose, national territories are subdivided into seismic zones, depending on the local hazard. By definition, the hazard within each zone is assumed to be constant, and is most often expressed in values of peak ground acceleration. It is noted that the seismic zone maps and peak ground acceleration levels given in the National Annexes to Eurocode 8 (**Figure 31**- right) were produced at different times, with different hazard models and data.

**Figure 31:** Left: peak ground acceleration from the SHARE project for 475 years return period. Right: reference peak ground acceleration from the National Annexes to Eurocode 8. All countries adopted a reference return period of seismic action for the no-collapse requirement of 475 years, except Romania that adopted 100 years and UK that adopted 2500 years



Source: (left) adapted from Giardini et al., 2013 and (right) adapted from Palermo et al., 2018

<sup>94</sup> [www.efehr.org](http://www.efehr.org)

<sup>95</sup> [www.share-eu.org](http://www.share-eu.org)

<sup>96</sup> [www.sera-eu.org](http://www.sera-eu.org)

<sup>97</sup> <http://eurocodes.jrc.ec.europa.eu>



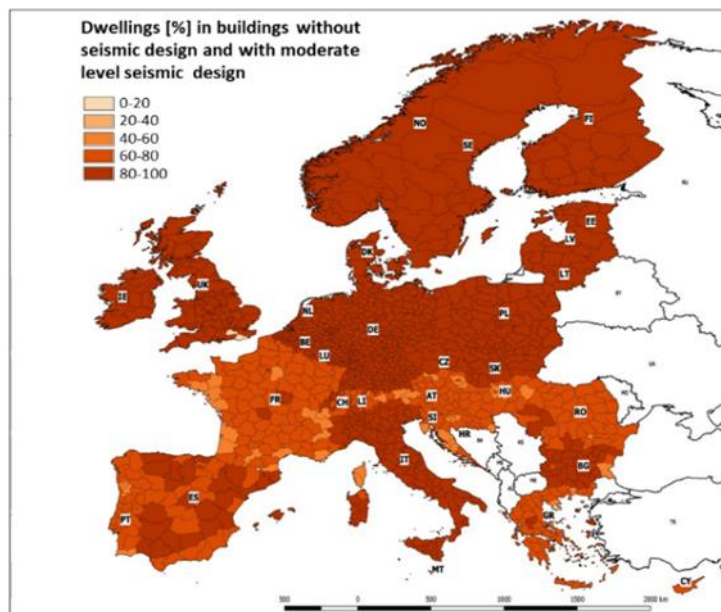
### 14.2.3 Exposure and vulnerability

Exposure databases for seismic risk assessment include data for buildings, infrastructure and population, often incomplete and geographically disaggregated in a non-homogeneously way. Exposure data for buildings have been collected specifically for seismic risk studies, and with a high level of spatial resolution, in a few cities around Europe.

Alternative source of information on the building stock, albeit not fully harmonised across countries, are the cadastres and national housing censuses that may furnish an exhaustive picture of the housing stock in a region. In the framework of the Prompt Assessment of Global Earthquakes for Response (PAGER<sup>98</sup>) system, a global building inventory has been compiled based on harmonised data from various sources (Jaiswal et al., 2010). It provides fractions of building types present in urban and rural regions of each country by their functional use. The quality of data in the PAGER database for most of the high-seismicity countries in Europe is judged medium or high. The NERA<sup>99</sup> project followed a similar procedure with a focus on European countries (Crowley et al., 2012), and its outcomes are currently available through the Global Earthquake Model (GEM) OpenQuake platform. The Global Exposure Database<sup>100</sup> available at the GEM Foundation (Gamba, 2014) is structured at a country, region, local and building level, and distinguishes between urban or rural areas and residential or non-residential buildings. Within the SERA project, this data is being updated and expanded to include industrial and commercial buildings; the first results are being made available through a number of interactive maps<sup>101</sup> at the EFEHR EU Earthquake Risk service<sup>102</sup>.

Exposure data for population is available through the new open and free tool Global Human Settlement<sup>103</sup> that produces global spatial information for assessing human presence on the planet, in the form of built-up maps, population density maps, and settlement maps.

**Figure 32.** Seismic vulnerability of buildings in Europe.



Source: Palermo et al., 2018

The updated UNISDR Terminology on Disaster Risk Reduction<sup>104</sup> defines vulnerability as “the conditions determined by physical, social, economic and environmental factors or processes which increase the

<sup>98</sup> <https://earthquake.usgs.gov/data/pager>

<sup>99</sup> <https://drmkc.jrc.ec.europa.eu/knowledge/PROJECT-EXPLORER/Projects-Explorer#project-explorer/631/projects/detail/3922/nera/main-info>

<sup>100</sup> <https://storage.globalquakemodel.org/what/physical-integrated-risk/exposure-database/>

<sup>101</sup> <https://maps.eu-risk.eucentre.it/>

<sup>102</sup> <http://www.efehr.org/en/efehr/Services-and-Partners/>

<sup>103</sup> <https://ghsl.jrc.ec.europa.eu>

<sup>104</sup> <https://www.undrr.org/terminology#V>

susceptibility of an individual, a community, assets or systems to the impacts of hazards” in the current case, earthquakes.

The majority of buildings in the European stock are vulnerable to earthquakes, as they have been designed without earthquake resistance or with moderate-level seismic codes (**Figure 32**). This is particularly relevant for the countries of moderate and high seismicity in the south and east Europe (**Figure 31**).

#### **14.2.4 Scenario-building process**

Models of ground shaking, vulnerability and fragility functions, and the geographical distribution of exposed assets, are used to evaluate the effects of ground motion, and to compute damage and losses scenarios for a region. A scenario-building process contributes to risk-informed decisions, being particularly useful to prepare emergency plans for civil protection, provide government and insurance companies a first-order estimate for planning, and analysing funding requests in the aftermath of a seismic event (De Martino et al., 2017), or evaluating ground acceleration time histories and duration of ground motion to be used in seismic design and retrofitting (Baker and Lee, 2018; Sousa and Campos Costa, 2009), among others.

An example of an earthquake hazard scenario is the maximum probable or credible earthquake, i.e., the largest earthquake that is reasonable to expect in a region. It is often based on the estimation of the magnitude of the worst historical event reported in the region, and its best-guessed location derived from known geological faults, or seismic source zones. Probabilistic seismic hazard disaggregation analysis is also used to determine the most probable earthquake scenario that controls the hazard at a site. The scenario may be characterized by a pair of magnitude and distance, conditional to a given level of ground motion, or specified return period. The aleatory variability of the ground motion and the fragility of elements at risk are taken into consideration to assess the impact of a historical event or a simulated earthquake hazard scenario in a region.

Probabilistic seismic risk assessment considers all possible earthquakes that may affect a site, together with the respective probabilities of occurrence, and lead to a probabilistic estimation of damage and losses, including relevant uncertainties.

In practice, a seismic risk scenario includes the assessment of several Sendai Framework Indicators<sup>105</sup>, such as number of deaths, injured people, people whose dwellings were damaged or destroyed, direct economic loss in relation to the global gross domestic product, direct economic loss in the housing sector, damage to critical infrastructure, and disruptions to basic services.

Specific regions in Europe are prone to infrequent but extremely severe seismic events; there, earthquakes may be identified as a key risk with low probability and high impact in a regional and national context, causing possible adverse cross-border impacts. For instance, the 1755 great Lisbon earthquake produced unusual devastation having a significant impact in Portugal, Spain and Morocco. The event was felt in other western Europe regions, such as the southern part of France and the north of Italy (Solares and Arroyo, 2004).

### **14.3 Risk analysis**

#### **14.3.1 Damage assessment**

Damage of physical assets at risk is evaluated by means of fragility functions describing the probability that, for a given value of the earthquake intensity, structures of a certain typology will exceed different damage levels. Empirical fragility functions are based on observed damage data from past earthquakes, while numerical ones are produced from the results of numerical simulations of varying degrees of sophistication. Uncertainties in probabilities of damage originate from the variability of the seismic action, geometric and material parameters of the studied structures, type of structural model and analysis, resistance models, the definition of damage states, etc. A collection of fragility curves for buildings, bridges, highway and railway infrastructure, harbour elements, health care facilities, electric power stations, gas and oil distribution networks, water and waste-water systems, may be found in Ptilakis et al. (2014), Yepes-Estrada et al. (2016) and the Global Vulnerability Database<sup>106</sup>. Similar methodologies are used to estimate damage in cultural heritage, taking into consideration the particularities of these structures (Bernardini and Lagomarsino, 2018, Despotaki et al. 2018).

---

<sup>105</sup> [www.preventionweb.net/drr-framework/sendai-framework-monitor/indicators](http://www.preventionweb.net/drr-framework/sendai-framework-monitor/indicators)

<sup>106</sup> <https://platform.openquake.org/vulnerability/list>

Different models have been developed to provide decision-makers with more useful risk metrics describing the impact of earthquakes (ICPD, 2018). The models, presented below, transform earthquake damage (e.g. the number of buildings collapsed) to consequences, such as direct-economic losses, debris estimates, business interruption, casualties or shelter needs.

### **14.3.2 Damage-to-loss models**

Generally, damage-to-loss models assess the total repair cost for a class of buildings, or building typology, correlating a given damage threshold to the repair cost, knowing the building replacement cost in the region (ATC, 1985, D'Ayala et al., 2015, De Martino et al., 2017, FEMA, 2018, Martins et al., 2016, Wehner and Edwards, 2013). Empirical models exist to estimate debris resulting from building collapse (FEMA, 2018, Santarelli et al., 2018). Empirical models, e.g. by Lehman et al. (2004) and Mackie and Stojadinović (2006) for bridges, relate the functionality of basic services and infrastructures to structural damage. The latter can be obtained, for a given earthquake intensity, by fragility functions. Empirical models are also available for estimating business interruption (ATC, 1985, FEMA, 2018) as a function of structural damage.

### **14.3.3 Estimation of casualties**

Injuries and casualties during earthquakes are caused by structural and non-structural damage, accidents, heart attacks, etc. Coburn and Spence (2002) report that more than 75% of deaths in past events were due to building collapse and propose a 'lethality ratio', i.e. the ratio of people killed to the number of people present in a building, to estimate casualties for each building class. This ratio depends on the characteristics of the ground motion, the building type and function, collapse mechanism, occupancy, behaviour of occupants, and search and rescue effectiveness. The models provide, for each typology of collapsed building, the percentage of people that are lightly, moderately or seriously injured, or killed. A large number of casualty models with different degrees of sophistication have been developed (e.g. ATC, 1985, Balbi et al., 2006, Cavalieri et al., 2012, Erdik et al., 2011, Jaiswal et al., 2009, Jaiswal and Wald, 2012, Khazai et al., 2014, So and Pomonis, 2012, So and Spence, 2013, Spence et al., 2011, Zuccaro and Cacace 2011). Most of them highlight the great uncertainty associated with casualty estimations.

### **14.3.4 Estimation of shelter needs**

Data from past earthquakes show that the number of displaced people is almost an order of magnitude higher than the number of collapsed and severely destroyed buildings. Multi-criteria models for estimating displaced households and short-term shelter needs consider the physical habitability of buildings together with the occupants' desirability to evacuate and to seek public shelter (Khazai et al., 2014, FEMA, 2018). The habitability of buildings is based on the physical damage, the loss of utilities (e.g. water and energy supply), and the weather conditions. The desirability to evacuate depends on a number of social factors, such as household tenure and size, household type, age of occupants and perception of security in the area. Lastly, the desirability to seek public shelter is influenced by the fear of aftershocks, residents' income, employment and education level, as well as by the distance and ease of access to shelters. Data for these indicators are available through the national statistical institutes and Eurostat.

### **14.3.5 Probabilistic seismic risk analysis**

Loss exceedance curves are examples of risk metrics that result from the probabilistic analysis of seismic risk. The curves describe the probability of various levels of losses being exceeded. Typically, probabilistic seismic risk analysis looks at the following losses or consequences: fatalities, injuries and economic losses derived from damages. Once the probability distribution of losses is known, other risk metrics can be obtained, for example, average annualized earthquake losses (AEL) or average annualized earthquake loss ratio, AELR (FEMA, 2017). AELR is a useful metric to compare the relative risk across different regions since it is normalized by the replacement value of exposed elements.

### **14.3.6 Tools for seismic risk analysis**

In the last decades several open-source tools with high degree of sophistication and capabilities have been developed for the assessment of loss scenarios, or for the evaluation of earthquake impact on critical infrastructures. Most of the software include libraries with pre-defined hazard and vulnerability models, and also allow the user to input new ones. Examples include:

- HAZUS<sup>107</sup> is a standardised methodology for estimating potential disaster losses from earthquakes, floods, and hurricanes. HAZUS uses GIS technology to estimate physical, economic, and social impacts of disasters. It is used for mitigation and recovery, as well as preparedness and response.
- The CAPRA<sup>108</sup> probabilistic risk assessment platform is an initiative that aims to strengthen the institutional capacity for assessing, understanding and communicating disaster risk, with the ultimate goal of integrating disaster risk information into development policies and programs.
- AFAD – RED is the Turkish national operational tool for seismic risk assessment, prevention, preparedness and response. In its real-time operational configuration, the system combines seismic data with an extensive inventory of buildings, critical facilities and population to provide damage and fatality loss estimates.
- The REAKT<sup>109</sup> project produced the Earthquake Qualitative Impact Assessment tool that uses earthquake data (location and magnitude) and modelling (fault geometry, slip distribution, directivity effects, wave propagation, site effects, etc.) to produce real-time “heads-up” alerts for global earthquakes.
- The SELINA<sup>110</sup> open risk software is a tool to provide earthquake damage and loss estimates. It uses a logic tree approach and allows for deterministic and probabilistic analysis.
- The OpenQuake<sup>111</sup> engine is the Global Earthquake Model Foundation state-of-the-art, free, open-source and accessible software collaboratively developed for earthquake hazard and risk modelling.
- The RASOR<sup>112</sup> project developed a platform to perform a multi-hazard risk analysis to support the full cycle of disaster management, including targeted support to critical infrastructure monitoring, and climate change impact assessment.
- Rapid-N<sup>113</sup> has been developed by the European Commission for the assessment of Natech risks at local and regional levels, and has currently been implemented for earthquakes.

Andredakis et al. (2017) provide further details on these tools. Example applications with pre-loaded exposure data showed that these tools are able to produce an early impact assessment within 5-15 minutes.

Comparison of predicted losses with data recorded after real earthquakes demonstrated that, in general, the order of magnitude of economic losses is accurately predicted, but casualties are overestimated.

Near-real time loss assessment systems provide rapid estimates of ground motion, damage and losses following a seismic event, as long as its magnitude, time of occurrence and location are known. PAGER<sup>114</sup> is a well-known near-real-time loss assessment system, which provides first-order estimates of human and economic losses on a global scale.

### 14.3.7 Recent research

The European Union has provided significant funding for collaborative research projects dealing with the impact of earthquakes, within the Framework Programmes for research and innovation. The projects listed in **Table 11** involved experts from across Europe. They produced state-of-the-art methodologies and models for hazard, vulnerability and risk assessment, developed tools that can be deployed in practice for preparedness, mitigation, planning, and risk management activities. The methodologies, models and tools were used for a large number of illustrative case studies at local (city) or regional level.

**Table 11.** European research projects related to seismic risk assessment

Project	Title	Duration	Website
---------	-------	----------	---------

<sup>107</sup> [www.fema.gov/hazus](http://www.fema.gov/hazus)

<sup>108</sup> <https://ecapra.org>

<sup>109</sup> [www.reaktproject.eu](http://www.reaktproject.eu)

<sup>110</sup> [www.norsar.no/r-d/safe-society/earthquake-hazard-risk/the-selena-open-risk-software](http://www.norsar.no/r-d/safe-society/earthquake-hazard-risk/the-selena-open-risk-software)

<sup>111</sup> [www.globalquakemodel.org/oq-getting-started](http://www.globalquakemodel.org/oq-getting-started)

<sup>112</sup> [www.rasor-project.eu](http://www.rasor-project.eu)

<sup>113</sup> <http://rapidn.jrc.ec.europa.eu>

<sup>114</sup> <https://earthquake.usgs.gov/data/pager>

LESSLOSS	<i>Risk mitigation for earthquakes and landslides</i>	2004-2007	<a href="https://cordis.europa.eu/project/rcn/74272_en.html">https://cordis.europa.eu/project/rcn/74272_en.html</a>
NERIES	<i>Network of research infrastructures for European seismology</i>	2006-2010	<a href="https://cordis.europa.eu/project/rcn/79877_en.html">https://cordis.europa.eu/project/rcn/79877_en.html</a>
SERIES	<i>Seismic engineering research infrastructures for European synergies</i>	2009-2013	<a href="http://www.series.upatras.gr">www.series.upatras.gr</a>
SHARE	<i>Seismic hazard harmonization in Europe</i>	2009-2012	<a href="http://www.share-eu.org">www.share-eu.org</a>
SYNER-G	<i>Systemic seismic vulnerability and risk analysis for buildings, lifeline networks and infrastructures safety gain</i>	2009-2013	<a href="http://www.vce.at/SYNER-G">www.vce.at/SYNER-G</a>
NERA	<i>Network of European research infrastructures for earthquake risk assessment and mitigation</i>	2010-2014	<a href="https://cordis.europa.eu/project/id/262330">https://cordis.europa.eu/project/id/262330</a>
REAKT	<i>Strategies and tools for real time earthquake risk reduction</i>	2011-2014	<a href="http://www.reaktproject.eu">www.reaktproject.eu</a>
STREST	<i>Harmonized approach to stress tests for critical infrastructures against natural hazards</i>	2013-2016	<a href="http://www.strest-eu.org">www.strest-eu.org</a>
INDUSE-2-SAFETY	<i>Component fragility analysis and seismic safety assessment of special risk petrochemical plants under design basis and beyond design basis accidents</i>	2014-2017	<a href="http://www.induse2safety.unitn.it">www.induse2safety.unitn.it</a>
SERA	<i>Seismology and earthquake engineering research infrastructure alliance for Europe</i>	2017-2020	<a href="http://www.sera-eu.org">www.sera-eu.org</a>

Source: Authors

Furthermore, the Global Earthquake Model <sup>115</sup> is engaging with a very diverse community to i) share data, models, and knowledge through the OpenQuake platform, ii) apply GEM tools and software to inform decision-making for risk mitigation and management, and iii) expand the science and understanding of earthquakes.

### 14.3.8 Examples of seismic risk assessment studies

The Italian Civil Protection Department has recently published a comprehensive report (ICPD, 2018) addressing the national risk assessment of the potential major disasters in Italy due to earthquakes, volcanic eruptions, tsunami, hydro-geological/hydraulic events, extreme weather, droughts, and forest fires. With regard to seismic risk, the report echoes the state-of-the-art of practice for assessing earthquake risk, considering the latest advances in the evaluation of probabilistic seismic hazard in Italy, the collection of detailed damage data from eight recent Italian earthquakes, the update of empirical vulnerability models derived from earthquake data, and new fragility models for masonry and reinforced concrete buildings. A new

<sup>115</sup> [www.globalquakemodel.org](http://www.globalquakemodel.org)

tool called IRMA (Italian Risk MAPs) was developed to assess damage scenarios and seismic risk maps for the Italian territory.

A scenario-based approach was followed for the seismic risk assessment in Spain (DGPCE, 2015). This study used the national seismic hazard maps, census and cadastral data, respectively for population and buildings, vulnerability classes according to the period of construction of buildings, and empirical models for impact on people. The analysis yielded the number of buildings at different damage states, the number of casualties and injuries, and the number of homeless people in the event of earthquakes with a return period equal to 500 and 1 000 years.

A probabilistic method was adopted for the assessment of seismic risk in 40 cities in metropolitan France (AFPS, 2014). The study employed hazard curves for cities in different seismic zones, fragility functions for buildings belonging to four vulnerability classes, and models that relate structural damage to the number of victims, and to economic losses. The results are given in terms of probability of collapse of buildings, expected annual losses, and probability of casualties.

The Portuguese National Authority for Civil Protection with the collaboration of several research institutions coordinated two projects for assessing the seismic risk in the metropolitan region of Lisbon and in Algarve; these are the two mainland Portuguese regions most historically impacted by earthquakes (ANPC, 2010, Campos Costa *et al.*, 2010, Costa *et al.*, 2012, Sousa *et al.*, 2010). The projects aimed at providing scientific foundations to support decision-making concerning regional seismic disaster prevention and preparedness. The projects included studies on seismotectonic, updating of seismic catalogues, ground motion at the bedrock and considering site effects, vulnerability to landslides, exposure and vulnerability of buildings, critical infrastructures, lifelines, and population. A near-real-time loss assessment GIS system was developed to evaluate damages and losses considering strong-motion seismic scenarios similar to historical earthquakes that affected both regions. Particularly in the Algarve region, tsunami hazard and the vulnerability of the littoral coast to tsunami incursion was evaluated.

#### 14.4 Risk evaluation

Risk evaluation is the process of comparing the level of risk achieved during the analysis stage with the risk criteria, i.e., the terms of reference against which the significance of a risk is evaluated. Risk evaluation aims to assist the decision about risk treatment (ISO 31 000: 2018). A risk-informed decision, rather than a risk-based decision, allows for adjustments taking into account other relevant factors like political and legal requirements, socio-economic, technical and environmental conditions.

The geographic distribution of risk indicators, for instance, maps of earthquake losses for a given return period, or average annualized earthquake losses are useful tools for communicating the results of the risk analysis, and identifying the most at-risk areas across a country<sup>116</sup>. Note that the comparison of risk maps with the spatial distribution of seismic hazard, vulnerability, and exposure can only provide a qualitative indication on the main drivers of risk, owing to the complexity of the process for evaluating earthquake risk.

Countries may find helpful to compare their risk assessment with the maps carried out at a world level by the GEM Foundation (Silva *et al.* 2018), particularly the profiles for available countries (<https://downloads.openquake.org/>), which include maps of seismic hazard, exposure, average annualized earthquake losses, average annualized earthquake loss ratio, among other information.

Note that society's aversion to events capable of causing a large number of fatalities, such as seismic phenomena, can influence the decision framework. For this reason, the risk of facing death or injuries may be addressed in terms of (i) individual risk, or the risk of a person present in a given location, being exposed to one or more adverse hazardous events, and (ii) societal risk or the risk of a group of people being simultaneously exposed to an adverse hazardous event. Societal risk is often assessed using the so-called F-N curves that provide the probability of exceeding a number of fatalities per year (Stojadinovic, 2016) and incorporate society's aversion to events posing death threats to large populations.

As regards seismic risk, the literature is scarce to guide decisions on acceptable or tolerable levels of life or economic losses. Risk below the acceptability threshold would not require the implementation of reduction measures, whereas risk above the tolerability threshold would require mitigation measures to reduce it to tolerable levels.

---

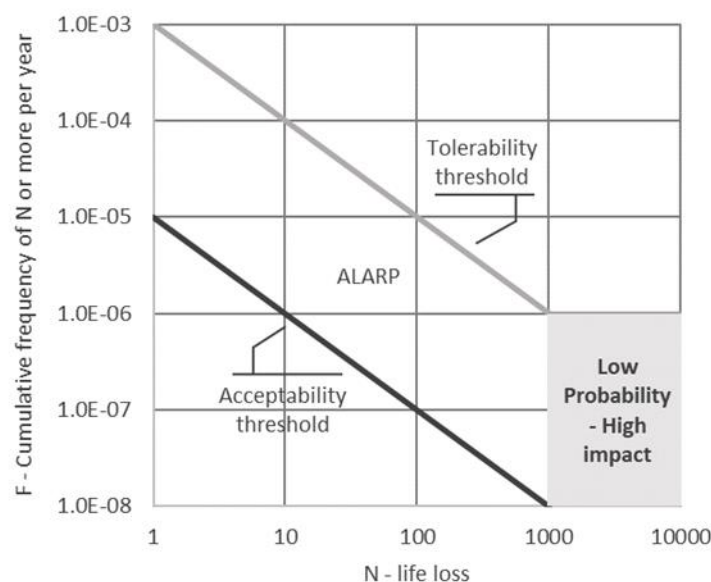
<sup>116</sup> Commission Notice. Reporting Guidelines on Disaster Risk Management, Art. 6(1)d of Decision No 1313/2013/EU (2019/C 428/07)



On this subject, it is worth mentioning the FP7 project STREST<sup>117</sup> (Harmonized approach to stress tests for critical infrastructures against natural hazards) that summarised the European practice regarding the acceptance criteria for fatality risk (STREST Deliverable D4.5, Stojadinovic, 2016). The author suggests that individual risk should be less than  $10^{-6}$  per year, whereas societal risk should be less than  $10^{-3}$  per year for major accidents with up to 1 fatality, and less than  $10^{-5}$  for ten times larger accidents. Considering that the criteria to evaluate societal earthquake risk was still a controversial issue, Sousa et al (2010) used the acceptability threshold for individual risk proposed by ANCOLD (2003) to evaluate the earthquake risk in Lisbon. Accordingly, the acceptability threshold adopted for individual risk was between  $10^{-6}$  and  $10^{-8}$  per year. When risk reduction is impracticable, or the costs to mitigate it are disproportionate to the benefits obtainable (ALARP principle – As Low As Reasonably Practicable), the threshold (tolerability threshold in this case) may drop, e.g., to  $10^{-5}$  for new structures, and to  $10^{-4}$  for existing ones (Sousa et al, 2010).

The risk-informed guidelines for safety decisions in dam projects (FERC, 2016) may provide an indicative reference to identify whether earthquake risk in a region should be addressed as a low-probability and high-impact risk. In fact, a sudden-unexpected dam failure can simultaneously affect a large number of people, as is the case of earthquake disasters. The guidelines define the attributes of a low probability – high consequence region in a F-N chart as follows: incremental life loss estimated to be equal or exceed 1 000 lives with an annual probability of potential life loss less than 1 in 1 000 000 ( $10^{-6}$ ) (see **Figure 33**). However, risk criteria can vary significantly depending on the context and nature of hazards, so the proposed values should be seen as merely indicative.

**Figure 33.** Low-probability and high-impact risk region in a F-N chart



Source: adapted from FERC, 2016

## 14.5 Risk treatment

When a risk evaluation process leads to the decision to undertake risk treatment, the next step is to implement mitigation measures. It is recognised that it is not possible to avoid the occurrence of earthquakes, except in special cases, such as seismicity induced by human activity. However, earthquake effects can be significantly mitigated by either reducing exposure, the vulnerability of built environment, or by implementing non-structural prevention and preparedness measures.

Prevention measures comprise seismic retrofitting of buildings and infrastructure. The application of building codes can considerably reduce the severity of human, structural and economic impacts of earthquakes. The provisions of Eurocode 8 contribute to reduce the vulnerability of buildings by ensuring that, in the event of earthquakes, lives are protected, damage is limited and civil protection structures remain operational. This has been demonstrated in all major earthquakes that occurred worldwide, e.g. the 1995 Kobe, Japan, earthquake

<sup>117</sup> <http://www.strest-eu.org/>

(Ranghieri and Ishiwatari, 2014), and the 2009 earthquake in L'Aquila, Italy (Dolce and Manfredi, 2015), where the large majority of damaged buildings were built with no or low-level provisions for earthquake resistance. The lesson learnt is that building codes have proven to be a valuable mechanism to implement effective mitigation measures, and significantly reduce the high-costs of post-disaster reconstruction in many developed countries. Moreover, post-disaster reconstruction offers an opportunity for introducing or reforming regulatory processes, aiming to “Build Back Better”, i.e., to implement land use planning, to improve the quality and safety of the built environment, to strengthen the resilience of communities to earthquakes, and to capitalise long-term earthquake risk reduction efforts.

Besides building codes, state incentives are a useful instrument to upgrade the building stock. For example, Italy introduced a tax reduction equal to up to 85% of the cost for structural interventions that improve the seismic vulnerability of existing buildings<sup>118</sup>.

Another way to save lives is by implementing non-structural prevention measures, like (i) communicating risk to raise public awareness for earthquake disasters or (ii) implementing early warning systems in urban regions, for instance:

- The communication of risk aims to engage and educate different target groups, from citizens to stakeholders (e.g. infrastructure operators or emergency authorities), regulators and government. The goal is to promote a “risk culture” about the seismic phenomena and to guide the implementation of prevention and preparedness measures, namely: self-protection measures (e.g. shakeout earthquake drill<sup>119</sup>), infrastructure resilience plans, damage and safety procedures for post-earthquake usability of buildings (Baggio et al., 2007), aftermath funding plans, regulations, standards, and policies.
- Early warning systems rely on the difference of arrival time between warning messages and destructive shaking waves. The former is transmitted almost instantaneously when triggered by an earthquake, whereas the latter may take seconds to minutes to arrive to a location. People and automated systems may use this short time delay to activate measures to protect life and property. Japan and Mexico are examples of countries where early warning systems are functioning (Cuéllar, 2014, Fujinawa and Noda, 2013).

## 14.6 Gaps and challenges

The research community is continuously refining seismic hazard, vulnerability, and damage-to-loss models that will be included in upgraded versions of the software for seismic risk analysis. While most software tools are user-friendly, their high degree of sophistication requires a level of expertise to be operated. In addition, for specific risk assessment studies, the software tools may require user-supplied data that is costly and time-consuming to obtain.

It is worth pointing out the high uncertainty on the estimation of casualties, resulting from the wide variability of the number of earthquake victims subject to similar ground motion, and from the poor reliability and large gaps in post-earthquake statistics for casualties.

A major gap in seismic risk analysis is the absence of inventories of georeferenced exposure data, designed specifically for assessing the vulnerability of the built environment at a local scale. Exposure data is mainly available for residential buildings and aggregated in large regions. Inventories should preferably include as many as possible assets (e.g. industrial, commercial and other buildings, networks, critical infrastructures, etc.) in order to provide a more accurate and detailed risk assessment.

Other challenges involve the development of multi-hazard risk assessment procedures on the one hand, and coordinated approaches between disaster risk reduction, climate change adaptation strategies and sustainable development policies, on the other (Poljanšek et al, 2017). Those approaches would provide a relevant contribution to the achievement of the European Green Deal, the United Nations Agenda for Sustainable Development, the objectives of the 2015 Paris Agreement, and the priorities of the Sendai Framework.

---

<sup>118</sup> Legge 27 dicembre 2017, n. 205. Bilancio di previsione dello Stato per l'anno finanziario 2018 e bilancio pluriennale per il triennio 2018-2020.

<sup>119</sup> <https://www.shakeout.org/dropcoverholdon/>



The ongoing project REEBUILD (Integrated Techniques for the Seismic Strengthening & Energy Efficiency of Existing Buildings)<sup>120</sup> is helping to shape the latter mentioned research needs. REEBUILD aims to support a more effective allocation of financial resources and climate change adaptation, proposing a holistic approach for the reduction of seismic vulnerability and the increase of energy efficiency of the European existing building stock.

## 14.7 References

- AFPS, *Quantification effective du risque sismique*, Cahier technique N°32, Association Française du Génie Parasismique, 2014.
- ANCOLD, *Guidelines on risk assessment*, Australian National Committee on Large Dams, ANCOLD Incorporated, 2003.
- Andreadakis, I., Proietti, C., Fonio, C. and Annunziato, A., *Seismic risk assessment tools workshop*, Publications Office of the European Union, Luxembourg, 2017, doi: 10.2760/249272.
- ANPC, *Estudo do risco sísmico e de tsunamis do Algarve*, Autoridade Nacional de Proteção Civil, 2010 (in Portuguese).
- ATC, *Earthquake damage evaluation data for California*, Applied Technology Council, Redwood City, 1985.
- Baker, J.W., and Lee, C., 'An Improved Algorithm for Selecting Ground Motions to Match a Conditional Spectrum', *Journal of Earthquake Engineering*, 2018, 22(4), 708–723.
- Balbi, A., Galasco, A., Giovinazzi, S., Lagomarsino, S. and Parodi, S., "Scenario sismico": a tool for real time damage scenarios', *Proceedings of the 13th World Conference on Earthquake Engineering*, 2006.
- Bernardini, A. And Lagomarsino, S., 'The seismic vulnerability of architectural heritage'. *Proceedings of The Institution of Civil Engineers-structures and Buildings* – PROC INST CIVIL ENG-STRUCT B. 161. 171-181. 10.1680/stbu.2008.161.4.171, 2018.
- Campos Costa, A., Sousa, M.L., Carvalho, A. and Coelho, E., 'Evaluation of seismic risk and mitigation strategies for the existing building stock: application of LNECloss to the metropolitan area of Lisbon', *Bulletin of Earthquake Engineering*, Vol. 8, 2010, pp. 119-134, doi: 10.1007/s10518-009-9160-3.
- Cavalieri, F., Franchin, P., Gehl, P. and Khazai, B., 'Quantitative assessment of social losses based on physical damage and interaction with infrastructural systems', *Earthquake Engineering & Structural Dynamics*, Vol. 41, No 11, 2012, pp. 1569-1589.
- CEN, EN 1998-1 Eurocode 8: Design of structures for earthquake resistance - Part 1: General rules, seismic actions and rules for buildings, European Committee for Standardization, Brussels, 2004.
- Coburn, A. and Spence, R., *Earthquake protection* (second edition), Wiley, 2002.
- Costa, P., Pires, P. and Vicêncio, H., 'Study of seismic risk and tsunamis in Algarve. Estimative of debris and number of damage assessment inspectors', *Proceedings of the 15th World Conference on Earthquake Engineering*, 2012.
- Crowley, H., Özcebe, S., Spence, R., Foulser-Piggott, R., Erdik, M. and Alten, K., 'Development of a European building inventory database', *Proceedings of the 15th World Conference on Earthquake Engineering*, 2012.
- Crowley, H. Weatherill, G., Riga, E., Pitilakis, K., Roullé, A., Tourlière, B. Lemoine, A. and Hidalgo, C.G., 'D26.4 Methods for Estimating Site Effects in Risk Assessments'. WP26 (JRA4: Risk Modelling Framework for Europa) SERA project, 2019.
- Cuéllar, A., Espinosa-Aranda, J. M., Suárez, R., Ibarrola, G., Uribe, A., Rodríguez, F. H., Islas, R., Rodríguez, G. M. and García, A. 'The Mexican seismic alert system (SASMEX): its alert signals, broadcast results and performance during the M 7.4 Punta Maldonado earthquake of March 20th, 2012', in: *Early warning for geological disasters. Advanced technologies in earth sciences*, edited by Wenzel F. and Zschau J., Springer, 2014.
- DGPCE, *Análisis de riesgos de desastres en España*, Dirección General de Protección Civil y Emergencias, 2015.

---

<sup>120</sup> Commission Decision of 28.5.2019 on the adoption of a financing decision and a work programme for 2019 for the implementation of the Pilot Project "Integrated techniques for the seismic strengthening and energy efficiency of existing buildings" to be financed under budget line 13 03 77 26, C(2019) 3874 final.

- D'Ayala, D., Meslem, A., Vamvatsikos, D., Porter, K., Rossetto, T. and Silva, V., *Guidelines for analytical vulnerability assessment of low/mid-rise buildings*, Vulnerability Global component project. doi: 10.13117/GEM.VULN-MOD.TR32014.12, 2015.
- De Martino, G., Di Ludovico, M., Prota, A., Moroni, C., Manfredi, G. and Dolce, M., 'Estimation of repair costs for RC and masonry residential buildings based on damage data collected by post-earthquake visual inspection', *Bulletin of Earthquake Engineering*, Vol. 15, No 4, 2017, pp. 1681-1706, doi: 10.1007/s10518-016-0039-9.
- Despotaki, V., Silva, V., Lagomarsino, S., Pavlova, I. and Torres, J., 'Evaluation of Seismic Risk on UNESCO Cultural Heritage sites in Europe'. *International Journal of Architectural Heritage*. 12. 10.1080/15583058.2018.1503374, 2018.
- Dolce, M. and Manfredi G. (eds), 'Libro bianco sulla ricostruzione privata fuori dai centri storici nei comuni colpiti dal sisma dell'Abruzzo del 6 Aprile 2009', Doppiavoce Edizioni, 2015.
- Erdik, M., Şeşetyan, K., Demircioğlu, M.B., Hancılar, U. and Zülfikar C., 'Rapid earthquake loss assessment after damaging earthquakes', *Soil Dynamics and Earthquake Engineering*, Vol. 31, No 2, 2011, pp. 247-266.
- Fujinawa, Y. and Noda Y., 'Japan's earthquake early warning system on 11 March 2011: performance, shortcomings, and changes', *Earthquake Spectra*, Vol. 29, No S1, 2013, pp. S341-S368.
- FEMA, Multi-hazard loss estimation methodology earthquake model Hazus®-MH 2.1 user manual, Federal Emergency Management Agency, 2018.
- FEMA, P-366, Hazus®. Estimated annualized earthquake losses for the United States, Federal Emergency Management Agency, 2017.
- FERC, 'Risk-informed decision-making (RIDM). Risk guidelines for dam safety', Version 4.1. Federal Energy Regulatory Commission Office of Energy Projects - Division of Dam Safety and Inspections, USA, 2016.
- Gamba, P., *Global Exposure Database: scientific features*, GEM Technical Report 2014-10, GEM Foundation, Pavia, 2014.
- Giardini D. et al., (2013), Seismic Hazard Harmonization in Europe (SHARE): Online Data Resource, doi: 10.12686/SED-00000001-SHARE, 2013. [www.efehr.org/en/Documentation/specific-hazard-models/europe/overview/](http://www.efehr.org/en/Documentation/specific-hazard-models/europe/overview/) [accessed 08.12.2020].
- Gotoh, T., Nishimura, T., Nakata, M., Nakaguchi, Y. and Hiraki, K., 'Air pollution by concrete dust from the Great Hanshin Earthquake', *Journal of Environmental Quality*, Vol. 31, No 3, 2002, pp. 718-723.
- ICPD, National risk assessment. Overview of the potential major disasters in Italy: seismic, volcanic, tsunami, hydro-geological/hydraulic and extreme weather, droughts and forest fire risks. Presidency of the Council of Ministers, Italian Civil Protection Department, Italy, 2018.
- Hill, L.J., Sparks, S. and Rougier, J.C., 'Risk and uncertainty assessment in natural hazards', Chapter 1 in *Risk and uncertainty for natural hazards*, Sparks, R.S.J. and Hills, L.J. Editors, ISBN: 9781107006195, 2013.
- ISO 31 000: 2018(E) *Risk management - Guidelines*. International Standards Organisation, 2018.
- Jaiswal, K. and Wald, D., 'Improving PAGER's real-time earthquake casualty and loss estimation toolkit: challenges', *Proceedings of the 15<sup>th</sup> World Conference on Earthquake Engineering*, 2012.
- Jaiswal, K., Wald, D. and Hearne, M., *Estimating casualties for large earthquakes worldwide using an empirical approach*, Open-File Report 2009-1136, U.S. Department of the Interior, U.S. Geological Survey, 2009.
- Jaiswal, K., Wald, D. and Porter, K. 'A global building inventory for earthquake loss estimation and risk management', *Earthquake Spectra*, Vol. 26, No 3, 2010, pp. 731-748.
- Khazai, B., Daniell, J.E., Düzgün, S., Kunz-Plapp, T. and Wenzer, F., 'Framework for systemic socio-economic vulnerability and loss assessment', in: *SYNER-G: Systemic seismic vulnerability and risk assessment of complex urban, utility, lifeline systems and critical facilities*, edited by Ptilakis, K., Franchin, P., Khazai, B. and Wenzel, H., Springer, 2014.
- Khazai, B., Franco, G., Ingram, J.C., Rumbaitis del Rio, C., Dias, P., Dissanayake, R., Chandratilake, R. and Kannaf, S.J., 'Post-December 2004 tsunami reconstruction in Sri Lanka and its potential impacts on future vulnerability', *Earthquake Spectra*, Vol. 22, No S3, 2006, pp. S829-S844.

- Lehman, D., Moehle, J., Mahin, S., Calderone, A. and Henry, L., 'Experimental evaluation of the seismic performance of reinforced concrete bridge columns', *ASCE Journal of Structural Engineering*, Vol. 130, No 6, 2004, pp. 869-879.
- Lin, W.-T., Lin, C.-Y., Tsai, J.-S. and Huang, P.-H., 'Eco-environmental changes assessment at the Chiufenershan landslide area caused by catastrophic earthquake in Central Taiwan', *Ecological Engineering*, Vol. 33, No 3-4, 2008, pp. 220-232.
- Mackie, K.R. and Stojadinović, B., 'Post-earthquake functionality of highway overpass bridges', *Earthquake Engineering & Structural Dynamics*, Vol. 35, No 1, 2006, pp. 77-93.
- Martins, L., Silva, V., Marques, M., Crowley, H. and Delgado, R., 'Development and assessment of damage-to-loss models for moment-frame reinforced concrete buildings', *Earthquake Engineering & Structural Dynamics*, Vol. 45, No 5, 2016, pp. 797-817.
- Palermo, V., Tsionis, G. and Sousa M.L., 'Building stock inventory to assess seismic vulnerability across Europe', *Proceedings of the 16<sup>th</sup> European Conference on Earthquake Engineering*, 2018.
- Pitilakis, K., Crowley, H. and Kaynia, A. (eds), *SYNER-G: Typology definition and fragility functions for physical elements at seismic risk*, Springer, 2014.
- Poljanšek, K., Marin Ferrer, M., De Groeve, T., Clark, I., (Eds.), *Science for disaster risk management 2017: knowing better and losing less*. EUR 28034 EN, Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-60679-3, doi:10.2788/842809, JRC102482.
- Ranghieri, F. and Ishiwatari, M. (eds), *Learning from megadisasters - Lessons from the Great East Japan Earthquake*, The World Bank, Washington, DC, 2014.
- Santarelli, S., Bernardini, G. and Quagliarini, E., 'Earthquake building debris estimation in historic city centres: From real world data to experimental-based criteria', *International Journal of Disaster Risk Reduction*, Vol. 31, 2018, pp. 281-291.
- Silva, V., Amo-Oduro, D., Calderon, A., Dabbeek, J., Despotaki, V., Martins, L., Rao, A., Simionato, M., Viganò, D., Yepes-Estrada, C., Acevedo, A., Crowley, H., Horspool, N., Jaiswal, K., Journeay, M., Pittore, M., *Global Earthquake Model (GEM). Seismic Risk Map* (version 2018.1), DOI: 10.13117/GEMGLOBAL-SEISMIC-RISK-MAP-2018, 2018.
- Silva, V., Amo-Oduro, D., Calderon, A., Dabbeek, J., Despotaki, V., Martins, L., Rao, A., Simionato, M., Viganò, D., Yepes, C., Acevedo, A., Horspool, N., Crowley, H., Jaiswal, K., Journeay, M., Pittore, M., 'Global Earthquake Model (GEM) Seismic Risk Map' (version 2018.1). DOI: 10.13117/GEM-GLOBAL-SEISMIC-RISK-MAP-2018.1, 2018.
- Silva, V., Dolce, M., Danciu, L., Rossetto, T. and Weatherill, G., 'Geophysical risk: earthquakes', in: *Science for disaster risk management 2017: knowing better and losing less*, edited by Poljanšek, K., Marin Ferrer, M., De Groeve, T. and Clark, I., EUR 28034 EN, Publications Office of the European Union, Luxembourg, 2017, doi:10.2788/842809.
- So, E. and Spence, R., 'Estimating shaking-induced casualties and building damage for global earthquake events: a proposed modelling approach', *Bulletin of Earthquake Engineering*, Vol. 11, No 1, 2013, pp. 347-363.
- So, E. and Pomonis, A. 'Derivation of globally applicable casualty rates for use in earthquake loss estimation models', *Proceedings of the 15<sup>th</sup> World Conference on Earthquake Engineering*, 2012.
- Solares, J.M. and Arroyo, A. 'The great historical 1755 earthquake. Effects and damage in Spain'. *Journal of Seismology*, 8. 275-294. 10.1023/B:JOSE.0000021365.94606.03, 2004.
- Sousa, M.L. and Campos Costa, A., 'Ground motion scenarios consistent with probabilistic seismic hazard disaggregation analysis. Application to mainland Portugal', *Bulletin of Earthquake Engineering*, Vol. 7, No 1, 2009, pp. 127-147.
- Sousa, M.L., Campos Costa, A. and Caldeira, L., 'Apreciação do risco sísmico em Lisboa'. *Revista Portuguesa de Engenharia de Estruturas (RPEE)*, Thematic number on risks, ISSN 0870 – 984X), Lisbon. Portugal, 2010 (in Portuguese).
- Sousa, M.L., Carvalho, A., Bilé Serra, J.P. and Martins, A., 'Simulation of seismic scenarios in Algarve region' *Proceedings of the 14th European Conference on Earthquake Engineering*, 2010.
- Spence, R., So, E. and Scawthorn, C. (eds), *Human casualties in earthquakes: progress in modelling and mitigation*, Springer, 2011.

Stojadinovic, B., 'Development of a coherent definition of societal resilience and its attributes' Deliverable D4.5, WP4 Vulnerability models for the performance and consequences assessment in stress tests of critical infrastructures, FP7 project STREST, 2016.

UNISDR. United Nations Office for Disaster Risk Reduction. Report of the open-ended intergovernmental expert working group on indicators and terminology relating to disaster risk reduction. United Nations General Assembly. 2016.

Wehner, M. and Edwards, M., *Building replacement cost methodology*, version 2.0, Report produced in the context of the Global Exposure Database for the Global Earthquake Model (GED4GEM), 2013, Geoscience Australia.

Woessner, J., Danciu, L., Giardini, D., Crowley, H., Cotton, F., Grunthal, G. and SHARE Consortium, 'The 2013 European seismic hazard model: key components and results', *Bulletin of Earthquake Engineering*, Vol. 13, No 12, 2015, pp. 3553-3596.

Yepes-Estrada, C., Silva, V., Rossetto, T., D'Ayala, D., Ioannou, I., Meslem, A. and Crowley H., 'The Global Earthquake Model physical vulnerability database', *Earthquake Spectra*, Vol. 32, No 4, 2016, 2567-2585.

Zuccaro G., Cacace, F. *Seismic Casualty Evaluation: the Italian Model, an Application to the L'Aquila 2009 Event* in R. Spence et al. (eds.), "Human Casualties in Earthquakes, Advances in Natural and Technological Hazards Research" 29, DOI 10.1007/978-90-481-9455-1\_12, © Springer Science+Business Media B.V, 2011.

## 15 Volcano eruptions

COSTANZA BONADONNA, CORINE FRISCHKNECHT, SUSAN C. LOUGHLIN, DOMENICO MANGIONE, SCIRA MENONI

### 15.1 Context of Risk Assessment

Europe hosts a significant number of active volcanic areas most of which are concentrated in Iceland, Italy, Spain, Portugal and Greece. Many more are located in autonomous regions, European dependencies and territories in the Atlantic Ocean (Canary Islands, Azores, Cabo Verde, Tristan da Cunha, Ascension Island), the Lesser Antilles (Montserrat, Guadeloupe, Martinique, Saba) and the Indian Ocean (La Réunion) (Poljansek et al. 2017, Siebert et al. 2011).

Well-known volcanoes and their historical eruptions and impacts inform much of our knowledge about volcanic risk. For example, Vesuvio (Italy) with its well-studied eruptions and impacts (e.g. AD79 impacts at Pompei and Herculaneum) threatens the large metropolitan area of Naples, the frequently active volcano Etna threatens the large city of Catania and its surroundings on Sicily, Stromboli has recently shown how its sudden and violent explosive activity (e.g. 2019 explosive paroxysms) may impact both the local community and tourism (one tourist lost his life during the July 3rd event). The ongoing long-lived eruption of Soufrière Hills Volcano on Montserrat in the Lesser Antilles that started in 1995 emphasised the challenges of long-lived eruptions on small islands and the complex and cascading consequences over time for displaced populations. Europe is also home to potentially devastating volcanoes with significant exposed populations that have not erupted recently, and their future behaviour is difficult to anticipate. For example, Campi Flegrei (Italy) shows significant unrest but no monitoring data is available associated with the last eruption which occurred in 1538; similarly, Oraefajökull volcano (Iceland) has also shown recent unrest but has not erupted for hundreds of years. Such volcanoes present fundamental challenges in risk management. Volcano monitoring can support decision-making and has aided the timely evacuation of many communities worldwide, especially in recent decades (e.g. Eyjafjallajökull, Fogo, Etna) but prediction of hazardous phenomena, especially during long-lived eruptions, remains challenging (e.g. Barclay et al. 2019). Since the 2010 eruption of Eyjafjallajökull volcano, more countries in Europe have become aware of volcanic risk, the potential transboundary consequences of even small-moderate-sized eruptions and the potential vulnerability of tourists. In 2011, European countries were encouraged to include low probability, high impact events in their National Risk Assessments (NRA).

Despite increasing awareness, and the increasing presence of volcanic scenarios in NRAs, there are considerable differences in how and at what detail volcanic risks are considered across Europe and there is much potential to improve the situation. In particular, the seasonal increase in tourism at many volcanic islands in Europe is not targeted by specific policies as occurs for other risks. In addition, the potential threats of international volcanoes that may affect Member States even if they are not physically located in Europe is rarely considered. Therefore, volcanic risk assessments and related products and services are useful for decision makers such as national and local civil protection organization authorities: before the event (long term) to build successful mitigation policies, including emergency planning; during the event (short term) to facilitate emergency management and decision making; and after the event (long-term) for effective build-back-better policies. Nonetheless, volcanic risk assessments may be very complex, since multiple hazards (e.g. tephra fallout, lava flows) have to be considered that act over time through different spatial scales, often generating additional cascading hazards (e.g. landslides, tsunamis, lahars, forest fires), interacting with dynamic exposure and vulnerability aspects (Bonadonna et al. 2018). It is also interesting to consider how volcanic eruptions have been shown to significantly impact the climate when have injected large quantity of sulfur gases into the stratosphere (e.g. Rampino and Self 1982; Stenchikov et al. 1998); however, global warming can feedback on volcanic eruptions by reducing the plume height and, therefore, the potential to have stratospheric injection of sulfur (Aubry et al. 2016). In addition, the melting of glaciers has been seen to cause an increase in eruption frequency in selected areas (e.g. Iceland) that suggests a potential increase of eruptions worldwide due to global warming, even though such an increase might not become apparent for hundreds of years (Swindles et al. 2018). Given the complexity of volcanic eruptions and of their interaction with both the anthropogenic and natural environment (e.g. cascading impacts, climate), co-design and co-production of a risk assessment can help all actors to proactively engage with the evidence, the process and the results.

## 15.2 Risk identification

### 15.2.1 Volcanic hazards

Volcanic risk is intrinsically multi-hazard, which is what makes volcanic eruptions and their associated Disaster Risk Management particularly challenging. In fact, volcanic eruptions can be associated with one or more of the following main primary phenomena: tephra dispersal and fallout, gas emissions, pyroclastic density currents (PDCs), lava flows. In particular, tephra fallout and dispersal refer to the injection of particles (i.e. fragmented magma) into the atmosphere and the associated sedimentation to the ground. Tephra particles can range from a few meters down to less than one micron and they sediment at progressively increasing distance from the vent up to thousands of kilometres from source. As a result, the associated potential impact also varies significantly with distance from the vent due to the variation in deposits thickness and particle grain size (e.g. Jenkins et al. 2015). Large blocks and bombs as well as thick tephra deposits can cause structural damage to buildings and infrastructures in proximal areas, while the smallest particles (less than a few tens of microns) can persist in the atmosphere for long time posing a serious threat to aviation transport depending on the associated concentration. Gas emissions represent a persistent hazard at many volcanoes even in absence of eruptive activity; in fact, volcanic gas can be very toxic and sometimes lethal (e.g. SO<sub>2</sub>, H<sub>2</sub>S, CO<sub>2</sub>) (Williams-Jones and Rymer 2015). PDCs are hot mixtures of gas and particles of various sizes that flow away from volcanoes reaching variable distances mostly depending on the associated mass. Finally, lava flows are also hot flows that travel down the volcano at variable speeds mostly depending on their viscosity and topography. Both PDCs and lava flows have an immense destructive power due to the high temperature and dynamic pressure (e.g. Blong 2000). People can survive at the margins of PDCs, or inside impacted buildings, but they generally suffer serious and complex burn injuries. The slower velocity of lava flows makes them less dangerous for people, but they are associated with damage and destruction of the built environment and vegetation (e.g. Kīlauea volcano, USA; Poland et al. 2016).

In addition to primary volcanic hazards, the area around active volcanoes can also be affected by secondary hazards, i.e. hazards that are not directly related to the dynamics of the volcanic system. Secondary hazards include lahars, remobilization of pyroclastic deposits by wind, tsunami and landslides. Lahars are flows that are produced by the mixture of solid or liquid water with pyroclastic material and are associated with a variable level of impact both to people and properties depending on the associated volume. The most voluminous lahars are typically those associated with the melting of ice caps (e.g. Nevado del Ruiz 1985, Colombia; Pierson et al., 1990); however, remobilization of pyroclastic material by rainfall can also cause widespread damage (Pinatubo 1991, Philippines; Vallance and Iverson, 2015). In particular, lahars associated with the remobilization of pyroclastic deposits by rainfall can occur a long time after the eruption has ended. Similarly, the wind-induced remobilization of pyroclastic deposits can occur during the eruption as well as a long time after the eruption has ended and can be associated with similar impacts as primary fallout (e.g. Cordon Caulle 2011, Chile; Dominguez et al. 2020). Tsunamis associated with volcanic eruptions do not involve as much mass movement as for those triggered by tectonic earthquakes, nonetheless they can also be highly destructive both for people and properties (e.g., Anak Krakatau 2018, Indonesia; Williams et al. 2019). Finally, landslides associated with flank collapses can occur due to flank deformation and/or alteration and depending on their location they can also cause devastating tsunamis (e.g. Stromboli; Rosi et al. 2019).

Hazard characterization and assessment is the aspect of volcanic risk that has been the most studied and published in the literature. In fact, in the last 20 years, significant advances have been made in the assessment of tephra fallout (e.g. Biass and Bonadonna 2013; Selva et al. 2018), PDCs (e.g. Charbonnier and Gertisser 2012; Neri et al. 2015), lava flows (e.g. Costa and Macedonio 2005; Cordonnier et al. 2015) and lahars (e.g. Cordoba et al. 2015; Mead and Magill 2017). The recent eruptions of Eyjafjallajökull, Iceland in 2010 and Cordón Caulle, Chile in 2011 have also highlighted two important aspects that have been often ignored or overlooked in hazard and risk assessment of explosive volcanism: the far-range atmospheric dispersal of volcanic ash from even moderate-size eruptions (Biass et al. 2014; Kim et al. 2019) and the resuspension of fine ash by wind erosion even years after the end of an eruption (Leadbetter et al. 2012; Mingari et al. 2017; Jarvis et al. 2020). These phenomena have revealed a new facet of global vulnerability of modern societies through direct and cascading effects.

Most hazard assessments published in literature focus on single hazards (e.g. tephra, PDCs, lahars), and often on single aspects of individual hazards (e.g. tephra ground accumulation, atmospheric tephra dispersal). This is driven by the fact that single aspects of hazard processes might be particularly useful in specific phases of emergency management and long-term risk management strategies. As an example, the hazard assessment of tephra ground accumulation is important to long-term risk management of urban environments and land-

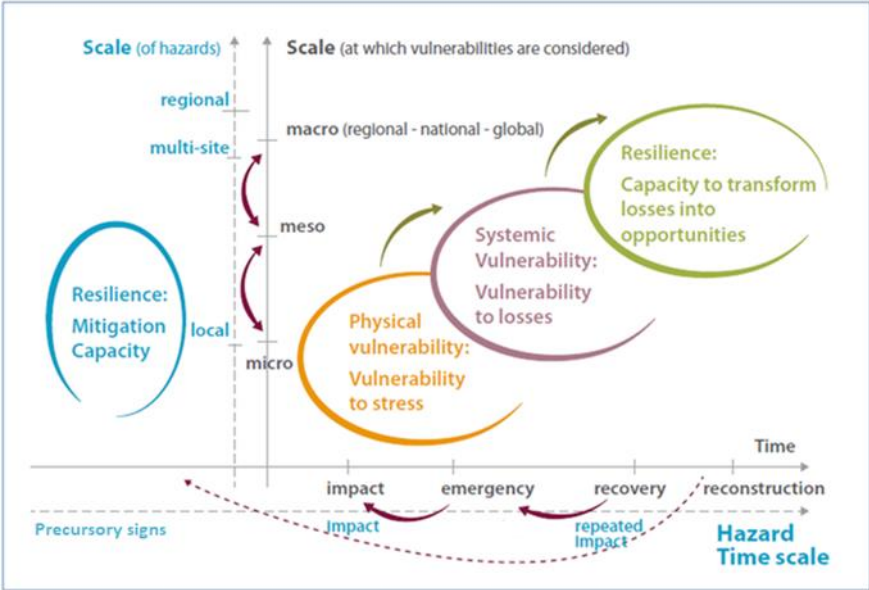
use planning, while hazard assessment of tephra dispersal in the atmosphere is required for both real-time forecasting during volcanic crisis and long-term planning of air traffic. Nonetheless, specific volcanic hazards might impact various systems (e.g. environment, economy) simultaneously (e.g. fallout of ash and lapilli from the plume, gas emissions and sedimentation of ballistic blocks), or sequentially (e.g. tephra fallout and PDCs), and some might even trigger secondary hazards (e.g. tephra-fallout deposits can serve as the source of sediments in lahars in cases involving abundant water) and/or worsen the consequences of simultaneous hazards. As a result of the complexity of volcanic eruptions, local and national authorities are often faced with the management of multiple or compounding hazards much more often than single hazards (e.g. Liu et al. 2016). Multi-hazard assessments of active volcano are, therefore, crucial to effective strategies of risk reduction. Some multi-hazard assessment platforms are available online (e.g. VOLCWORKS, Granados et al., 2012; VHASS, Takarada 2017), but not many examples of multi-hazard assessments exist in literature (e.g. Sandri et al. 2014; Zuccaro et al. 2018). In addition, these studies mostly combine the extent of individual hazards and only rarely account for the interaction amongst individual volcanic processes, e.g. cascading hazards (e.g. Tierz et al. 2017; Baumann et al. 2019).

Various strategies for volcanic hazard assessment exist and can be categorized in three main groups: i) deterministic volcanic hazard assessment; ii) scenario-based volcanic hazard assessment; iii) probabilistic volcanic hazard assessment. In the first case, both eruptive conditions (e.g. plume height, erupted mass, grainsize distribution, lava flow viscosity, velocity) and non-eruptive conditions (e.g. wind speed and direction, rain fall intensity, topography) are fixed; in the second case, both eruptive and non-eruptive conditions are varied and probabilistically analysed assuming that the selected scenario will occur; finally, in a fully probabilistic hazard assessment, both eruptive and non-eruptive conditions are varied and probabilistically analysed and a given probability of occurrence is assigned to each scenario selected. In fact, with the exception of specific complex scenarios where deterministic approaches are preferred (e.g. Deligne et al., 2017), probabilistic modelling is required to describe the intrinsic uncertainty of the system (i.e. aleatoric uncertainty) as well as the uncertainty associated with the lack of knowledge (i.e. epistemic uncertainty).

**15.2.2 Vulnerability aspects**

Vulnerability can be defined as the propensity of elements at risk (e.g. people, assets and systems) to be damaged by a given hazard due to their intrinsic characteristics. Vulnerability can be subdivided in a variety of subcategories, such as physical, functional, social, economic, systemic, institutional and environmental vulnerability (Birkmann 2007). **Figure 34** illustrates the various spatio-temporal scales at which hazards and vulnerabilities intervene according to the framework developed as part of the EU-funded project ENSURE (Enhancing resilience of communities and territories facing natural and na-tech hazards; 2008-2011) and coherently with relevant definitions proposed in literature (Turner et al., 2003).

**Figure 34.** Framework proposed by ENSURE project to describe the interaction between hazard, vulnerability and resilience



Source: adapted from Menoni et al. 2013

The framework displays different axes for the temporal and spatial scales of hazards and vulnerabilities. In particular, the temporal and spatial development of natural phenomena and human response do not necessarily coincide. As for the temporal scale, for example, the possibility of new occurrences of significant events within a short period of time, and while recovery is still occurring, must be considered (e.g., remobilization of ash following its primary deposition). Concerning vulnerability, the physical fragility of structures and infrastructures will determine the size of the consequences at the time of the impact, whilst during the emergency what is most relevant is the residual functional capacity of services and lifelines that depends on their systemic vulnerability.

As for the spatial scale, physical vulnerabilities are mainly addressed at the local scale to analyse intrinsic fragility of structures and infrastructures; systemic vulnerability considers aspects from local to large scale (municipal to provincial or county level) in order to account for aspects of interdependency and redundancy of critical infrastructures. Resilience is seen here as the capacity to mitigate risk before the occurrence of an event and as the ability to transform losses into opportunities after an event in order to improve the pre-event existing conditions and make the built environment more resistant to future natural hazards. When considering the capabilities of populations to recover effectively (i.e., to be resilient), the regional, national and in some cases international levels must be considered. In fact, the resources required to reconstruct areas affected by disaster cut across all levels of society (government, non-profit, for profit, etc.) and depend on the type and strength of relationships among the affected places and a much wider region.

The most studied dimension in volcanology is physical vulnerability and mostly associated with tephra fallout; in particular, various damage scales and fragility curves have been produced that facilitate the combination of hazard assessments with vulnerability assessments (e.g. Blake et al. 2017, Jenkins et al. 2014,2015, Spence et al. 2005, Williams et al. 2017). Nonetheless, a few examples of fragility curves for PDCs and lahars also exist (e.g. Daga et al. 2018, Zuccaro and De Gregorio 2013). Social vulnerability has also been analysed independently to provide a general understanding of risk perception of population (e.g. Gregg et al. 2004, Gaillard 2008, Haynes et al. 2008, Hicks and Few 2015, Few et al. 2017, Lindell and Perry 1993, Perry and Greene, 1983). When social vulnerability has been used to compile risk assessments, it has been typically based on census data and expressed in terms of population composition (urban, rural) and population characteristics (gender, age), education level (ratio of people without a basic level of education on the total population of the administrative unit), and proportion of people with functional and access needs (namely elderly, children and invalids; e.g. Biass et al. 2012). Some examples of systemic vulnerability assessments in areas exposed to active volcanoes can be found, mainly addressing the interconnection, interdependency and redundancy of lifelines (Galderisi et al. 2013).

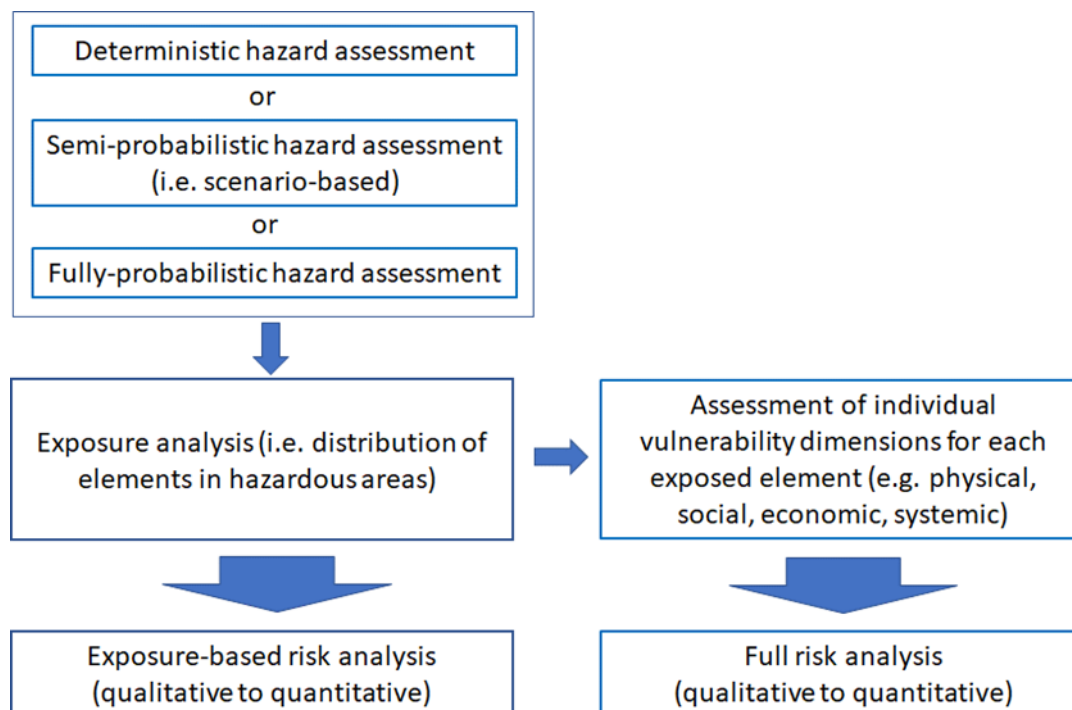
### **15.3 Risk analysis**

For volcanic eruptions to provoke damage, one or multiple hazardous phenomena must impact exposed people, buildings, infrastructures and/or natural areas: pre-event risk analysis provides a forecast of expected damage given volcanic hazards, exposure and vulnerability. Risk analysis can be carried out for various time scales (Bonadonna et al. 2018). The main objective of long-term risk assessment before the event is risk management (e.g. hazard assessment, land use planning, preparedness, implementation of mitigation measures and education). The main objectives of rapid risk assessment during volcanic unrest include update of the likelihood of hazard scenarios (e.g. expert elicitation), structure and demography of population, lifelines, critical infrastructures, and potentially hazardous infrastructures that can cause cascading technological disasters; it can be built on the long-term risk assessment and is important for all the stakeholders (e.g. Civil protection at all levels, decision-makers in national and local level, private sector, communities). The main objective of rapid risk assessment during the event is emergency management (e.g. evaluation of new potential hazard scenarios and their likelihoods, changes in population distribution, population movements, access, population needs); it should be combined with potential impact assessments/impact scenarios to plan and coordinate response. The main objective of risk assessment after the event is reconstruction that should take into account lessons learnt and the potential for building back better; however, some time it is required to fully characterize and assess the overall long-term impacts/damage (not only physical, but also economic and social).

Volcanic risk analysis can be qualitative, semi quantitative or quantitative depending on how hazard, exposure, and vulnerability and their combination are assessed (Figure 35). A complementary distinction is made between probabilistic and deterministic (or scenario-based) approaches. Probabilistic risk assessments are necessarily quantitative, whilst deterministic ones can be qualitative, semi quantitative or quantitative.



**Figure 35.** Generalized sketch for the compilation of a volcanic risk assessment for individual volcanic hazards. Multi-hazard risk assessments should result from the combination of individual analysis associated with each individual hazard. Similarly, individual dimensions of vulnerability need to be treated separately and for each exposed element (e.g. population, buildings, and infrastructures).



Source: Authors

It is increasingly recognised that both qualitative and quantitative approaches are needed, and each bring different advantages and disadvantages. Quantitative approaches may be essential to rigorously support decision-making around significant investments in risk reduction, for example, whereas, qualitative approaches may be better able to capture the wide range of cascading consequences a scenario may lead to.

Volcanic risk assessment requires a combination of hazard assessments with either exposure analysis or vulnerability assessment or both. In case the hazard assessment is only combined with the exposure analysis the risk assessment can be defined as exposure-based and typically provides a quantitative assessment of number of potentially affected people, assets or value of the latter (Figure 35). Given that all volcanic hazards are very different in terms of hazard intensity metrics, even in case of multi-hazard risk assessments, the individual hazards have to be treated separately and then be combined with either exposure only or with exposure and vulnerability. The most common hazard intensity metrics are (Wilson et al. 2017): thickness or mass loading (tephra fallout, pyroclastic density current deposits, lahar deposits), dynamic pressure (pyroclastic density currents, lahar), flow height (lava flow, lahar), presence or absence (lava flow, gas emissions), density per unit area (ballistics), impact energy (ballistics) and concentration (gas emissions, tephra fallout).

Given the associated complexity and the infancy of vulnerability studies associated with a volcanic setting, examples of comprehensive risk assessments that analyse the full spectrum of potential hazards in combination with exposure and the full spectrum of vulnerability dimensions does not yet exist. Most methods model such combination using vulnerability or damage curves that have been developed to relate hazards with exposed elements given their intrinsic fragilities, mainly addressing physical vulnerability. A standardized method for risk analysis that can be used throughout the community still needs to be developed. Nonetheless, some examples exist that show various combinations of hazards, exposure and vulnerability associated with tephra fallout and dispersal (e.g. Biass et al. 2017, Scaini et al. 2014, Spence et al. 2005, Thompson et al. 2016; Alcorn et al. 2013; Bonadonna et al. 2021), PDCs (e.g. Alberico et al. 2008), lava flows (e.g. Bonne et al. 2008, Favalli et al. 2009), lahars (e.g. Lavigne 1999, Leung et al. 2003, Mead et al. 2017), and multi hazards (e.g. Alberico et al. 2011, Alcorn et al. 2013, Deligne et al, 2017, Marti et al., 2016, Neri et al. 2008, Pareschi et al. 2000, Zuccaro and De Gregorio 2013). Even though current EU guidelines consider human life and health, economic losses and socio-political impacts as suitable impact categories for NRAs (EC, 2010), the

current state of art in volcanology is not able to cover such a wide-ranging risk analysis encompassing all societal relevant sectors.

For volcanoes, hazard and risk analyses are developed at the volcano scale focusing on the multi-hazard nature of the threat and likely impacts. Such analyses are typically forward-looking where they exist but may still be grounded in assumptions based on what has happened in the past (geological studies). As noted above, vulnerability data is still largely lacking and for many volcanic hazards (e.g. pyroclastic density currents, lahars) there are assumptions of total destruction (bimodality) which do not enable planning for the more complex reality that not all people impacted are killed (and many may require urgent specialist burns treatment) and not all buildings and land are destroyed but their value may be lost.

In the recent past, some of the most devastating volcanic events in historical times arose from poor responses to a single volcanic hazard arising from a small to moderate-sized eruption, e.g. Nevado del Ruiz, Colombia, in 1985, when a moderate-sized eruption caused melting of the summit ice cap and the generation of voluminous lahars (Pierson et al., 1990). The focus should, therefore, be on impact scenarios and the sequence of events that could lead to them. It is advisable to plan for low frequency, high magnitude events for which there are no historical precedents, and this is particularly important for caldera volcanoes (e.g. Campi Flegrei, Italy). For national planning, it is important to consider impact scenarios at each volcano that could require a national response or that may exceed national capabilities. For volcanoes it is also critical to consider transboundary risks, for example disruption to transport, critical infrastructure or supply chains (e.g. Eyjafjallajökull, 2010) which may have wide-ranging and cascading consequences. For volcanic islands, it is particularly important to consider scenarios with partners in neighbouring islands and countries. For example, a PDC would cause a particular set of challenges on the island but if it enters the sea it may cause completely different hazards (e.g. tsunami) on neighbouring islands and coastlines.

## 15.4 Risk evaluation

Risk evaluation is the process of deciding whether a risk is acceptable or should be reduced considering multiple criteria aimed at saving human lives and preserving economic activities and goods. In the context of an NRA, risk evaluation also includes the process of comparing risks for various reasons including 1) to recognise where risk management (emergency planning and preparedness versus risk mitigation) and finance should be prioritised, 2) to understand potential linkages and interactions between natural and man-made hazards, and 3) to recognise where measures and capabilities that are already developed or being developed for another risk could be adopted or developed for a new risk (OECD, 2018)

Risk matrices are an attempt to distinguish high probability, high impact events from low probability, low impact events; in principle, they should be effective to guide planning priorities but in fact it has been shown that there may be a tendency to under-prioritise low probability, high impact events (Blagden 2018), such as volcanic eruptions. Differently, risk ladders express risk from low to high on a vertical scale (Visschers et al., 2009) and have been used in volcanology (e.g. Montserrat; Sparks et al. 2013) to compare the societal risk (loss of life) between volcanoes, earthquakes, hurricanes and other risks (e.g. traffic, public health); this enables stakeholders including the public to place infrequent and unfamiliar hazards in context with more frequent and familiar hazards.

In the UK, a 'Natural Hazards Partnership' has been developed to enable collaboration and discussion across hazards between national institutions involved in the process but in addition, academia, the private sector and civil society need to be involved. Transparency of the process is essential if all stakeholders are to have confidence in methods, comparison of risks, ownership of risks and emergency planning. In order to achieve transparency, it is essential that metadata (source data, assumptions, model limitations) are made available and uncertainties unveiled.

As volcanic unrest and eruptions are multi-hazardous and last for weeks, months or years, so hazards may interact with other natural or anthropogenic hazards that are generally considered separately in NRAs but may actually occur concurrently, in succession or be interconnected especially before, during or after an eruption affecting a wide variety of sectors at different temporal and spatial scales. Available methods to consider such multi-risk conditions exist ranging from the simplest qualitative table listing possible additional hazards and their interconnections (Gill and Malamud, 2014, 2017) to probabilistic multi-hazard methods (e.g. Marzocchi et al. 2012; Bernal et al, 2017; Tierz et al. 2017).

Not all populations, sectors, infrastructures and environments are equally resilient. Analysed vulnerabilities and risk often assume the steady-state of a given population, building or infrastructure. However, a more

dynamic consideration of the impact of unrest and eruption over a significant period of time must be taken into account. As an example, evacuations, loss of livelihoods, separation of families, development of chronic health problems due to repeated ash fall and gas/aerosol emissions must be considered. The UK NRA plots likelihood versus impact for each 'reasonable worst-case scenario' together on the same graph, there is also a separate likelihood versus impact matrix for each type of natural hazard, which may include a reasonable worst-case, maximum and minimum scenario.

## 15.5 Risk treatment

National Risk Assessments can help national governments decide how much investment is proportionate to the risk, but given the impossibility of 'zero risk' as a result of mitigation, a political understanding of the tolerability of the residual risk after mitigation measures have been taken is needed. For volcanoes, the challenge may vary dramatically depending on situation, so an island government/authority dealing with a few thousand people or less will likely have a different view on 'acceptable risk' to a national government managing risk to millions of people. For any nation with a volcano, the highest risk is geographically focused and although theoretically this enables focus, political decisions on appropriate investment and the setting of realistic and transparent mitigation and planning targets can be challenging. For most countries with volcanoes, the most difficult challenge is to set goals reflecting what is factually and politically feasible and to justify these goals by reference to a risk assessment that does not (and cannot) account for these kinds of political judgement.

A starting point for effective planning, preparedness, response and recovery from volcanic eruptions at local to national scales is to have an effective and appropriately resourced official volcano monitoring institution (often supported by other scientific institutions) working closely with civil protection (local to national) (see Box 10 on Campi Flegrei as an example).. For emergency response, the roles and responsibilities of each institution must be clear, leading to the development and implementation of procedures and emergency plans, as well as provision of appropriate resources. At-risk populations must be able to receive timely alerts and act appropriately upon them. This requires development of emergency plans at all levels from households to government, thorough understanding of risk, effective communication systems linked to monitoring and regular practice. This should all be in place before any disaster occurs. An assessment of the vulnerabilities and exposure of critical institutions needed to respond to volcanic events should be part of any risk assessment since a breakdown in coordination, communication and/or capacity can have devastating consequences. There have been good examples worldwide of exercises led by scientists working in partnership with civil protection to raise awareness and participation in communities at-risk (e.g. Hicks et al. 2017; Deligne et al. 2017; Ricci et al. 2013).

### Box 10: Campi Flegrei (Italy)

Campi Flegrei is a volcanic field (caldera) located in the Neapolitan area (Italy), extending from Monte di Procida to Posillipo, created by several past important explosive eruptions. The last eruption of Campi Flegrei occurred in 1538 which generated in few days the Monte Nuovo cone. Since then the volcano is quiescent but has always shown signs of activity including seismicity, gas emissions and deformations. The typical continuous uplift/downlift episodes of the caldera floor is known as "bradyseism". Last important uplift episodes occurred in 1969-1972 and in 1982-1984, in association with significant seismic swarms, which forced people to evacuate the Rione Terra in Pozzuoli. Since 2012, a new uplift phase is ongoing (cumulating 61 cm up to 2020) along with changes in the geochemical parameters of the fumarolic gases and some seismic swarms.

Long-term civil protection planning in case of reactivation of Campi Flegrei represents a significant challenge due to the uncertainties related to the possible size, to the location of the vent of the next eruption, to the expected hazards and their impact and to the very high number of exposed people. Moreover, there is a large number of stakeholders involved in the civil protection planning process, which adds further complexities.

The first important goal achieved was to define a long-term scenario-based hazard assessment. This task was performed by a working group made of scientists coming from volcanic observatories and academia. The scenario includes (1) the spatial distribution of medium-long term probabilities of future vent opening areas, (2) the definition of the eruptive classes (from small to very large) with associated conditional probability of occurrence considering the last 5,000 years of activity, (3) the expected hazards and (4) specific physical vulnerability studies for earthquakes and tephra fall.

The results of these studies enabled the National Civil Protection Department, in close connection with the Regione Campania civil protection and the Municipalities, to define suitable risk management policies for the chosen Volcanic Explosivity Index 4 eruption (i.e. medium size eruption). As a result, the high risk zone, named "red zone", and the "yellow zone" were defined. They represent the backbone of the National Civil Protection plan for volcanic risk in Campi Flegrei.

The red zone is the area that includes the Municipalities, or part of them, which could be most likely invaded by PDCs, according to the results of the hazard assessment studies. Given the deadly and destructive impact of PDCs on human life, the only risk mitigation measure considered is the total evacuation of the population (almost 500,000 people) before the eruption starts. People could either choose an autonomous place to stay outside the red zone or receive governmental assistance from the Region twinned with each Municipality. In case of pre-eruptive seismic crises, buildings located along the evacuation routes may be severely damaged significantly impacting the evacuation process. Therefore, physical vulnerability studies for seismic hazard in these areas will also be considered in the mobility plan.

Based on dedicated hazard modelling and physical vulnerability assessment, the yellow zone includes the Municipalities that could be most likely affected by heavy tephra fall and suffer major disruptions, including roof collapses. The entire yellow area counts about 840,000 people, but only part of it will be affected by ash and evacuated depending on the wind direction. So, each Municipality of the yellow area must update its own civil protection plan to include appropriate contingency measures.

The National volcanic warning system is based on colour coded alert levels (from green to red) that describe the evolution of the volcanic activity status towards an eruption, based on monitoring data and observed phenomena. Alert levels are declared by the National Civil Protection Department based on information provided by INGV-Osservatorio Vesuviano volcanic observatory and on the advice of the "Commissione Grandi Rischi", which is a scientific advisory group appointed by a Prime Minister's Decree. Operational phases (base, attention, pre-alarm, alarm) define the actions that all members of the National civil protection system must undertake. The activation of the base and attention operational phases is declared by the National Civil Protection Department while pre-alarm and alarm phases are declared by the Prime Minister.

Following the unrest phase started in 2012, the National Civil Protection Department raised the volcanic alert level from green to yellow and the operational phase from "base" to "attention". In October 2019, a National full-scale exercise took place simulating the response of the entire National civil protection system, which also includes scientists, for each alert level and operational phase. Within the exercise, a volcanic risk awareness campaign for the local population named "Io non rischio" was conducted in the Municipalities of Campi Flegrei included in the red zone.

For longer-term planning there are important opportunities to align with existing risk management activities. For example, planning for different anthropogenic and natural hazardous events e.g. earthquakes, landslides, tsunami, poor air quality and flooding may also be appropriate for volcanic risks. Land use, spatial and urban planning are crucial to reduce in particular volcanic risk associated with some phenomena such as lava and pyroclastic flows for which measures addressing the physical vulnerability of structures and infrastructures are not likely to work and do not guarantee human survival. Tools generally adopted by planners, such as relocation, zoning, definition of acceptable population density, more appropriate urban patterns, organisation of settlements with respect to accessibility factors, location of critical facilities, are all based on decisions and design in which damage reduction and exposure avoidance can be mainstreamed as shown by some best practices (Saunders and Kilvington, 2016).

In Europe both long- and short-term mitigation are crucial, given the high population density of some of the areas that are exposed to volcanic threat, and the potential impact on economic sectors, such as tourism, particularly in areas that are considered peripheral, such as volcanic islands. Furthermore, the cross-border dimension of volcanic related risks on critical infrastructures should be better understood and planned for. As discussed by Wilson et al. (2017), lifelines such as power and telecommunication are extremely vulnerable to some of the volcanic related phenomena and outages in such systems may provoke widespread cascading effects in Europe on entire economic sectors as well as on other critical infrastructures.

## **15.6 Gaps and challenges/conclusions**

Volcanic risk assessment analysis is in its infancy and a variety of critical gaps and challenges still exist and can be used to guide future research and practice developments (Bonadonna et al. 2018). Collaborative research and partnership building across scientific disciplines and stakeholders have to be developed. The adoption of a common terminology (e.g. UNDRR; <https://www.undrr.org/terminology>) would also help to facilitate collaboration, optimize the research effort across disciplines and enhance uptake of science by national governments. The development of good practice in volcanic risk analysis would help in the collection of relevant and useful data (e.g. non-traditional data - social media, internet; citizen science; communities/authorities), in common formats and the storage and sharing of data (e.g. USHAHIDI; <https://www.ushahidi.com/>). There is a need to develop a framework to record and catalogue post-eruption damage data that is widely accepted, recognized and used by the volcanic risk community (as it is done, for example, by the European seismic risk community with the European Macroseismic Scale 98). Such data may support improved analysis of the key drivers behind eruptive impacts permitting to learn from real events and identify more clearly what combinations of hazards and vulnerabilities over time are most important in terms

of casualties, health impacts, building and infrastructure damage, business and network disruption, loss of livelihoods.

Existing approaches for assessing various dimensions of vulnerability (e.g. physical, social, systemic, economic) should also be refined and better adapted to the volcanic case. More effort should be invested into studying interdependencies and systemic links between hazards and vulnerabilities with impacts encompassing all societal sectors. A dynamic and comprehensive volcanic risk framework should integrate multiple hazards and different dimensions of vulnerabilities at multiple spatial and temporal scales. Propagation of uncertainty from the assessment of hazard, exposure and vulnerability to the compilation of risk assessment should be evaluated and incorporated in the final outcomes. The challenges relating to recovery need to be better addressed to improve communities' adaptation during long-lived eruptions or associated with frequently active volcanoes. This would require further investigation into phased evacuation, displaced populations and migration in relation to volcanic risk. Critical gaps between knowledge and actions to increase preparedness should also be identified.

Ideally, communities at-risk (or their representatives) should participate in risk assessments because they can provide knowledge, context and meaning to data that are collected. Risk assessments and related science-based services and products should be co-designed and co-produced by a variety of stakeholders including not only scientists, but also representatives of the society because they should be inclusive and answer specific needs. In particular, volcano observatories need to play a crucial role in the identification of volcanic hazards and in the co-production of risk assessments together with scientists and civil protection authorities. Such approaches can help to build trust (e.g. transparency, impartiality, participation). Nonetheless, there should be consistent messaging across all entities and with the public and all media. Volcanoes produce transboundary hazards and risks; so, there is also the opportunity to collaborate across nations in the analysis of, planning and preparation for risks. The rapidly increasing number of seasonal visitors to volcanic areas means that their exposure and vulnerability (and services required to manage them in a crisis) must also be considered in risk assessments, especially on volcanic islands. Working closely with governmental stakeholders at all levels and with managers of critical infrastructures, a better understanding of the information and methods required by risk analysis undertaken for different purposes (e.g. risk to life, insurance purposes) and at different time scales (before, during and after a hazardous event) should be investigated. Specific systems should also be assessed in relation to the different phases of the disaster risk cycle (e.g. transport system should be especially assessed in the framework of an emergency-based risk assessment).

Given the complexity of volcanic eruptions and their strong relation with the anthropogenic and natural environment over multiple spatial and temporal scales, co-design and co-production of knowledge and information on volcanoes and eruptions' impact can help all actors to proactively engage to develop usable risk assessment products and services supporting more evidence-based decisions.

## 15.7 Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731070 and by Fonds National Suisse project "FROM VOLCANIC HAZARD TO RISK ASSESSMENT" (IZSEZO\_181030).

## 15.8 References

- Alberico I., Lirer L., Petrosino P., Scandone R. (2008) Volcanic hazard and risk assessment from pyroclastic flows at Ischia island (southern Italy), *Journal of Volcanology and Geothermal Research*
- Alberico I., Petrosino P., Lirer L., (2011). Volcanic hazard and risk assessment in a multi-source volcanic area: the example of Napoli city (Southern Italy). *Nat. Hazards Earth Syst. Sci.* 11, 1057e1070.
- Alcorn R., Panter K.S., Gorsevki P.V. (2013) A GIS-based volcanic hazard and risk assessment of eruptions sourced within Valles Caldera, New Mexico, *Journal of Volcanology and Geothermal Research*
- Aubry T., Jellinek A. M., Degruyter W., Bonadonna C., Radić V., Clyne M., Quainoo A. (2016) Impact of global warming on the rise of volcanic plumes and implications for future volcanic aerosol forcing, *Journal of Geophysical Research: Atmospheres*, doi: 10.1002/2016JD025405

- Barclay J., Few R., Armijos M.T., Phillips J.C., Pyle D.M., Hicks A., Brown S.K. and Robertson R.E.A. (2019) Livelihoods, Wellbeing and the Risk to Life During Volcanic Eruptions. *Front. Earth Sci.* 7:205. doi: 10.3389/feart.2019.00205
- Baumann V., Bonadonna C., Cuomo S., Moscariello M., Biass S., Pistolesi M., Gattuso A. (2019) Mapping the susceptibility of rain-triggered lahars at Vulcano island (Italy) combining field characterization, geotechnical analysis, and numerical modelling, *Natural Hazards and Earth System Science*
- Bernal G.A., Salgado-Gálvez M.A., Zuloaga D. et al. (2017) Integration of Probabilistic and Multi-Hazard Risk Assessment Within Urban Development Planning and Emergency Preparedness and Response: Application to Manizales, Colombia. *Int J Disaster Risk Sci* 8, 270–283. <https://doi.org/10.1007/s13753-017-0135-8>
- Biass S., Bonadonna C. (2013) A fast GIS-based risk assessment for tephra fallout: the example of Cotopaxi volcano, Ecuador. *Natural Hazards* 65(1):477-495
- Biass S., Frischknecht C., Bonadonna C. (2012) A fast GIS-based risk assessment for tephra fallout: the example of Cotopaxi volcano, Ecuador-Part II: vulnerability and risk assessment. *Natural Hazards* 64(1):615-639
- Biass S., Scaini C., Bonadonna C., Folch A., Smith K., Höskuldsson A. (2014) A multi-scale risk assessment for tephra fallout and airborne concentration from multiple Icelandic volcanoes - Part 1: Hazard assessment. *Natural Hazards and Earth System Sciences* 14(8):2265-2287
- Biass S., Todde A., Cioni R., Pistolesi M., Geshi N., Bonadonna C. (2017) Potential impacts of tephra fallout for a Plinian eruption of Sakurajima volcano, Japan, *Bulletin of Volcanology* 79: 73.
- Birkmann J. (2007). Indicators and criteria for measuring vulnerability: theoretical bases and requirements. In J. Birkmann (Ed.), *Measuring vulnerability to natural disasters* (pp. 55e77). United Nations University Press.
- Blagden D. (2018) The flawed promise of National Security Risk Assessment: nine lessons from the British approach, *Intelligence and National Security*, 33:5, 716-736, DOI: 10.1080/02684527.2018.1449366
- Blake D.M., Deligne N.I., Wilson T.M., Wilson G. (2017) Improving volcanic ash fragility functions through laboratory studies: example of surface transportation networks, *J Appl Volcanol.*
- Blong R. (2000) Volcanic Hazards and Risk Management in *Encyclopedia of Volcanoes*, 1st Edition, Editors: Sigurdsson H., Houghton B. Rymer H., Stix J., McNutt S., Academic Press, San Diego, 1215-1227
- Bonadonna C., Biass S., Calder E.S., Frischknecht C., Gregg C.E., Jenkins S., Loughlin S.C., Menoni S., Takarada S., Wilson T. (2018), "1st IAVCEI/GVM Workshop: "From Volcanic Hazard to Risk Assessment", Geneva, 27-29 June 2018," <https://vhub.org/resources/4498>.
- Bonadonna C, Biass S, Menoni S, Chris EG (2021) Assessment of risk associated with tephra-related hazards, In: In: Papale, P (Ed.). *Forecasting and Planning for Volcanic Hazards, Risks, and Disasters*: Elsevier, 329-378. (Hazards and Disasters)
- Bonne K., Kervyn de Meerendre M., Cascone L., Njome S., Van Ranst E., Suh E., Ayonghe P.J. and Ernst G. (2008) A new approach to assess long-term lava flow hazard and risk using GIS and low-cost remote sensing: the case of Mount Cameroon, West Africa, *International Journal of Remote Sensing*
- Charbonnier S.J., Gertisser R. (2012) Evaluation of geophysical mass flow models using the 2006 block-and-ash flows of Merapi Volcano, Java, Indonesia: Towards a short-term hazard assessment tool. *Journal of Volcanology and Geothermal Research* 231:87-108
- Córdoba G., Villarosa G, Sheridan M., Viramonte J, Beigt D, Salmuni G (2015) Secondary lahar hazard assessment for Villa la Angostura, Argentina, using Two-Phase-Titan modelling code during 2011 Cordón Caulle eruption, *Natural Hazards And Earth System Sciences*
- Cordonnier B., Lev E. and Garel F. (2015) Benchmarking lava-flow models. Geological Society, London, Special Publications, 426
- Costa A., Macedonio G. (2005) Computational modeling of lava flows: A review. *Geological Society of America Special Papers* 396:209-218
- Dagá J., Chamorro A., de Solminihac H., and Echaveguren T. (2018) Development of fragility curves for road bridges exposed to volcanic lahars, *Nat. Hazards Earth Syst.*

- Deligne N. I., Horspool N., Canessa S., Matcham I., Williams G.T., Wilson G., and Wilson T.M. (2017). Evaluating the impacts of volcanic eruptions using RiskScape. *Journal of Applied Volcanology*
- Dominguez L., Bonadonna C., Forte P., Jarvis P.A., Cioni R., Mingari L., Bran D., Panebianco J.E. (2020) Aeolian remobilisation of the 2011-Cordón Caulle tephra-fallout deposit: example of an important process in the life cycle of volcanic ash, *Frontiers in Earth Sciences*
- Favalli M., Tarquini S., Fornaciai A., Boschi E. (2009) A new approach to risk assessment of lava flow at Mount Etna, *Geology*
- Few R., Armijos M.T. and Barclay J. (2017). Living with Volcan Tungurahua: the dynamics of vulnerability during prolonged volcanic activity. *Geoforum* 80: 72-81
- Gaillard J.-C. (2008) Alternative paradigms of volcanic risk perception: The case of Mt. Pinatubo in the Philippines, *J. Volcanol. Geoth. Res.*
- Galderisi A., Bonadonna C., Delmonaco G., Ferrara F.F., Menoni S., Ceudech A., Biass S., Frischknecht C., Manzella I., Minucci G., Gregg C. (2013) Vulnerability Assessment and Risk Mitigation: The Case of Vulcano Island, Italy,. In: *Landslide Science and Practice, Social and Economic Impact and Policies*. Springer Berlin Heidelberg
- Gill J., & Malamud B. D. (2014). Reviewing and visualizing the interactions of natural hazards. *REVIEWS OF GEOPHYSICS*, 52(4), 680-722. <https://doi.org/10.1002/2013RG000445>
- Gill J., & Malamud B. D. (2017). Anthropogenic processes, natural hazards, and interactions in a multi-hazard framework, *Earth-Science Reviews*, 166, 246-269
- Granados H. D., Guzman R. R., Befitex J. L. V., and Sanchez, T. G. (2012). VOLCWORKS: a suite for optimization of hazards mapping. *EGU Gen. Assem. Abstr.* 14, EGU2012-EGU12809.
- Gregg C. E., Houghton B. F., Johnston D. M., Paton D., and Swanson D. A. (2004) The perception of volcanic risk in Kona communities from Mauna Loa and Hualalai volcanoes, Hawaii, *J. Volcanol. Geoth. Res.*
- Haynes K., Barclay J., and Pidgeon N. (2008) Whose reality counts? Factors affecting the perception of volcanic risk, *J. Volcanol. Geoth. Res.*, 172, 259-272
- Hicks A., Few R. (2015) Trajectories of social vulnerability during the Soufriere Hills volcanic crisis. *Journal of Applied Volcanology* 4:10
- Hicks A., Armijos M.T., Barclay J., Stone J., Robertson R., Cortés G.P. (2017) Risk communication films: Process, product and potential for improving preparedness and behaviour change. *International Journal of Disaster Risk Reduction* 23: 138-151.
- Jarvis PA, Bonadonna C, Dominguez L, Forte P, Frischknecht C, Bran D, Aguilar R, Beckett F, Elissondo M, Gillies J, Kueppers U, Merrison J, Varley N and Wallace KL (2020) Aeolian Remobilisation of Volcanic Ash: Outcomes of a Workshop in the Argentinian Patagonia. *Front. Earth Sci.* 8
- Jenkins S.F., Spence R.J.S., Fonseca J.F.B.D., Solidum R.U., Wilson T.M. (2014) Volcanic risk assessment: Quantifying physical vulnerability in the built environment. *Journal of Volcanology and Geothermal Research* 276:105-120
- Jenkins S.F., Wilson T., Magill C., Miller V., Stewart C., Marzocchi W., Boulton M., Bonadonna C., Costa A. (2015) Volcanic ash fall hazard and risk, In: *Global Volcanic Hazard and Risk*, Editors: Loughlin SC, Sparks S, Brown SK, Jenkins SF, Vye-Brown C, Cambridge University Press, ISBN: 978-1-107-11175-2
- Kim S., Lee J., Oh S., Yoon Y. (2019) Assessment of the volcanic hazard of Mt. Paektu explosion to international air traffic using South Korean airspace, *Natural Hazards*
- Lavigne F. (1999) Lahar hazard micro-zonation and risk assessment in Yogyakarta city, Indonesia, *GeoJournal*
- Leadbetter S.J., Hort M.C., von Lowis S., Weber K., Witham C.S. (2012) Modeling the resuspension of ash deposited during the eruption of Eyjafjallajökull in spring 2010. *Journal of Geophysical Research-Atmospheres* 117
- Leung M.F., Santos J.R., Haines Y.Y. (2003) Risk Modeling, Assessment, and Management of Lahar Flow Threat, *Risk Analysis*
- Lindell M.K. and Perry R.W. (1993). Risk area residents' changing perceptions of volcano hazard at Mt. St. Helens. In F. Siccaldi, J. Nigg and J. Nemeč (Eds.) *Prediction and Perception of Natural Hazards* (pp. 159-166). Amsterdam: Kluwer Academic Publishers.

- Liu B, Siu YL and Mitchell G (2016) Hazard interaction analysis for multi-hazard risk assessment: a systematic classification based on hazard-forming environment. *Natural Hazards and Earth System Sciences*, 16 (2). pp. 629-642. ISSN 1561-8633
- Martí J., Bartolini S., and Becerril L. (2016). Enhancing safety in a volcano's shadow. *EOS* 97. doi: 10.1029/2016E0054161
- Marzocchi W., Garcia-Aristizabal A., Gasparini P., Mastellone M.L. and Di Ruocco A.. (2012) Basic principles of multi-risk assessment: a case study in Italy. *Natural Hazards* 62(2):551-573
- Mead S.R., Magill C., Lemiale V., Thouret J.C., and Prakash M. (2017) Examining the impact of lahars on buildings using numerical modelling, *Nat. Hazards Earth Syst. Sci.*, 17, 703–719
- Menoni S., Molinari D. Parker D., Ballio F., Tappes S. (2012) Assessing multifaceted vulnerability and resilience in order to design risk mitigation strategies, *Natural Hazards*, 10.1007/s11069-012-0134-4, pp. 1-26
- Menoni S., Modaresi H., Schniderbauer S., Kienberger S., Zeil P. (2013), Risk research. Ensuring to move ahead, European Union, Luxemburg, pp. 1-39, ISBN: 978-92-79-27026-0
- Mingari L.A., Collini E.A., Folch A., Báez W., Bustos E., Osoro M.S., Reckziegel F., Alexander P., Viramonte J.G. (2017). Numerical simulations of windblown dust over complex terrain: The Fiambalá Basin episode in June 2015. *Atmos. Chem. Phys.* 17, 6759–6778.
- Neri A., Aspinall W., Cioni R., Bertagnini A., Baxter P.G., Zuccaro G., Andronico D., Barsotti S., Cole P.D., Esposti Ongaro T., Hincks T.K., Macedonio G., Papale P., Rosi M., Santacroce R., Woo A. (2008). Developing an event tree for probabilistic hazard and risk assessment at Vesuvius. *J. Volcanol. Geotherm. Res.* 178, 397e415
- Neri A., Bevilacqua A., Esposti Ongaro T., Isaia R., Aspinall W.P., Bisson M., Flandoli F., Baxter P.J., Bertagnini A., Iannuzzi E., Orsucci S., Pistolesi M., Rosi M. and Vitale S. (2015) Quantifying volcanic hazard at Campi Flegrei caldera (Italy) with uncertainty assessment: 2. Pyroclastic density current invasion maps, *Journal of Geophysical Research*
- OECD, 2018, National risk assessment. A cross country perspective, OECD Publishing, Paris, <http://dx.doi.org/10.1787/9789264287532-en>
- Pareschi M.T., Cavarra I., Favalli M., Giannini F. and Meriggi A. (2000) GIS and Volcanic Risk Management, *Natural Hazards* 21, 361–379 <https://doi.org/10.1023/A:1008016304797>
- Perry R.W. and Greene M.R. (1983). *Citizen Response to Volcanic Eruptions: The Case of Mt. St. Helens*. New York: Irvington Publishers.
- Pierson T. C., Janda R. J., and Borrero C. A., 1990. Origin, flow behavior, and deposition of eruption-triggered lahars on 13 November 1986, Nevado del Ruiz volcano, Colombia. *Journal of Volcanology and Geothermal Research*, 41, 17–66.
- Poland M., Orr T.R., Kauahikaua J.P., Brantley S.R., Babb J.L., Patrick M.R., Neal C.A., Anderson K.R., Antolik L., Burgess M., (2016). The 2014–2015 Pāhoā lava flow crisis at Kīlauea Volcano, Hawai‘i: Disaster avoided and lessons learned. *GSA Today* 26, 4–10.
- Poljansek K., Montserrat M.F., De Groot T., Clark I. - Science for disaster risk management 2017, DOI 10.2788/688605
- Rampino, M.R., and Self S., 1982: Historic eruptions of Tambora (1815), Krakatau (1883), and Agung (1963), their stratospheric aerosols, and climatic impact. *Quat. Res.*, 18, 127-143, doi:10.1016/0033-5894(82)90065-5.
- Ricci T., Nave R., Barberi F. (2013) Vesuvio civil protection exercise MESIMEX: survey on volcanic risk perception, *INGV Annals of Geophysics*
- Rosi M., Levi S.T., Pistolesi M. et al. Geoarchaeological Evidence of Middle-Age Tsunamis at Stromboli and Consequences for the Tsunami Hazard in the Southern Tyrrhenian Sea. *Sci Rep* 9, 677 (2019). <https://doi.org/10.1038/s41598-018-37050-3>
- Sandri L., Thouret J.-C., Constantinescu R., Biass S., Tonini R. (2014) Long-term multi-hazard assessment for El Misti volcano (Peru). *Bulletin of Volcanology* 76(2):1-26



- Saunders W., Kilvington M. (2016) Innovative land use planning for natural hazard risk reduction: A consequence-driven approach from New Zealand, *International Journal of Disaster Risk Reduction* 18: 244–255.
- Scaini C, Biass S, Galderisi A, Bonadonna C, Folch A, Smith K, Höskuldsson A (2014) A multi-scale risk assessment for tephra fallout and airborne concentration from multiple Icelandic volcanoes - Part 2: Vulnerability and impact. *Natural Hazards and Earth System Sciences* 14(8)
- Selva J., A. Costa, G. De Natale, M.A. Di Vito, R. Isaia, G. Macedonio (2018) Sensitivity test and ensemble hazard assessment for tephra fallout at Campi Flegrei, Italy, *Journal of Volcanology and Geothermal Research*, 351, 1-28
- Siebert L., Simkin T.S., *Volcanoes of the world*, 2011, University of California Press, ISBN: 9780520268777
- Sparks R., Aspinall W., Crossweller H., & Hincks T. (2013). Risk and uncertainty assessment of volcanic hazards. In J. Rougier, S. Sparks, & L. Hill (Eds.), *Risk and Uncertainty Assessment for Natural Hazards* (pp. 364-397). Cambridge: Cambridge University Press. doi:10.1017/CBO9781139047562.012
- Spence R.J.S., Kelman I., Baxter P.J., Zuccaro G., Petrazzuoli S. (2005) Residential building and occupant vulnerability to tephra fall. *Natural Hazards and Earth System Sciences*
- Stenchikov G.L., Kirchner I., Robock A., Graf H.F., Antuna J.C., Grainger R.G., Lambert A., and Thomason L. (1998): Radiative Forcing from the 1991 Mount Pinatubo volcanic eruption. *J. Geophys Res.*103(D12), pp. 13837-13857.
- Swindles G.T., Watson E.J., Savov I.P., Lawson I.T., Schmidt A., Hooper A., Cooper C.L., Connor C.B., Gloor M., Carrivick J.L. (2018) Climatic control on Icelandic volcanic activity during the mid-Holocene. *Geology*; 46 (1): 47–50. doi: <https://doi.org/10.1130/G39633.1>
- Takarada S. (2017) The Volcanic Hazards Assessment Support System for the Online Hazard Assessment and Risk Mitigation of Quaternary Volcanoes in the World, *Front. Earth Sci.*
- Thompson M.A., Lindsay J.M., Wilson T.M., Biass S. and Sandri L. (2017) Quantifying risk to agriculture from volcanic ashfall: a case study from the Bay of Plenty, New Zealand. *Nat Hazards* 86, 31–56. <https://doi.org/10.1007/s11069-016-2672-7>
- Tierz P, Woodhouse MJ., Phillips JC., Sandri L, Selva J, Marzocchi W, Odbert HM. (2017) A Framework for Probabilistic Multi-Hazard Assessment of Rain-Triggered Lahars Using Bayesian Belief Networks, *Front. Earth Sci.*
- Turner B.L., Kasperson R.E., Matson P.A., McCarthy J.J., Corell R.W., Christensen L., Eckley N., Kasperson J.X., Luers A., Martello M.L., Polsky C., Pulsipher A., Schiller A. (2003) A framework for vulnerability analysis in sustainability science, *PNAS*, 100 (14): 8074-8079
- Vallance J.W., and Iverson R.M., 2015, Lahars and their deposits, in *The Encyclopedia of Volcanoes*, 2nd edition, Sigurdsson H., Houghton B., McNutt S. R., Rymer H. and Stix J. (Eds.), Elsevier, Amsterdam, 649–664
- Visschers V., Meertens R., Passchier W., de Vries N. (2009) Probability Information in Risk Communication: A Review of the Research Literature, *Risk Analysis*, 29:2
- Williams G.T., Kennedy B.M., Wilson T.M., Fitzgerald R.H., Tsunematsu K., Teissier A. (2017). Buildings vs. ballistics: Quantifying the vulnerability of buildings to volcanic ballistic impacts using field studies and pneumatic cannon experiments. *J. Volcanol. Geotherm. Res.* 343, 171–180.
- Williams R., Rowley P., Garthwaite M.C. (2019) Reconstructing the Anak Krakatau flank collapse that caused the December 2018 Indonesian tsunami. *Geology*, 47 (10): 973–976. doi: <https://doi.org/10.1130/G46517.1>
- Williams-Jones G. and Rymer H. (2015) Hazards of Volcanic Gases, – in *The Encyclopedia of Volcanoes*, 2nd Edition, Sigurdsson H., Houghton B., McNutt S. R., Rymer H. and Stix J. (Eds.), Elsevier, Amsterdam, (Eds.), Elsevier, Amsterdam, 985-992
- Wilson G, Wilson T, Deligne N.I., Blake D.M. and Cole J.W. (2017) Framework for developing volcanic fragility and vulnerability functions for critical infrastructure, *Journal of Applied Volcanology*
- Wisner B. (2016) Vulnerability as Concept, Model, Metric, and Tool, *Oxford Research Encyclopedia of Natural Hazard Science*, Oxford University Press, <https://oxfordre.com/naturalhazardscience/view/10.1093/acrefore/9780199389407.001.0001/acrefore-9780199389407-e-25>, accessed 21 Jan. 2020.

Zuccaro G. and De Gregorio D. (2013) Time and space dependency in impact damage evaluation of a sub-Plinian eruption at Mount Vesuvius, *Natural Hazards*, 68, 1399-1423

Zuccaro G, De Gregorio D., Leone M.F. (2018) Theoretical model for cascading effects analyses, *International Journal of Disaster Risk Reduction*, 30, 199-215

## 16 Biological disasters

ANNE SOPHIE LEQUARRE

### 16.1 Introduction

Biological disasters gather all the events linked to the uncontrolled spread of pathogens or pests affecting humans, animals or even plants. Well-known examples with huge economic costs are the food and mouth crisis in UK in 2001 with the culling of over 6 million of cows and sheep or, right now, the wipe out of millions of ancient olive trees in Italy due to the infection by deadly bacteria with no cure<sup>121</sup>. In human a number of epidemics (e.g. cholera or Spanish flu) have had previously devastating consequences on our populations but thanks to the development of vaccines or appropriate treatments health crisis are now fortunately scarce in most countries. However this stability can be shaking down as illustrated by the recent outbreak of measles after a decrease in vaccine coverage, especially in Ukraine<sup>122</sup> or the threat of the Ebola virus leading to thousands of deaths in West Africa with a few imported cases reported in Europe in 2014.

Outbreaks, the sudden rise in the incidence of a disease, occur when pathogen agents and target hosts are present in adequate numbers. It may result from an increase in the amount or in the virulence of the agent, but also a change in the susceptibility of the host and/or the introduction of the agent into a setting where it has not been before (emerging pathogen). International transportation, trade, urbanization, environmental change, agricultural practices could pave the way to new emerging epidemics in Europe or globally. Accidental release of an infectious agent from a laboratory or from the importation of goods has also to be taken into consideration. Potential malicious discharge should not to be discarded either.

Anticipating and managing outbreaks is complicate. In contrast with other disasters, outbreaks have very different profiles and impact according to the responsible agent and targeted host. Drafting generic risk assessment is challenging as this exercise strongly depends on the pathogen accountable and its host(s).

An epidemic is the widespread occurrence of an infectious disease in a community or population. A pandemic is the extension to many populations worldwide, crossing international boundaries and affecting a large number of people. Zoonosis is any disease or infection that is naturally transmissible from vertebrate animals to humans.

They can be extremely disruptive to lives, livelihoods, and the political and socioeconomic stability of affected communities so well illustrated by what we are experiencing in 2020 with the COVID-19 pandemic.

Epidemics and pandemics have a unique characteristic, the responsible pathogens continue to circulate, spread and evolve and thus present ongoing and changing challenges in terms of assessment, impact and persistence, further complicating risk management, control and recovery.

### 16.2 Human epidemics

#### 16.2.1 Risk identification and the policy context

The extent of an outbreak depends on pathogen's features (host range, transmission mode, virulence, pathogenicity, etc.), characteristics of the host (numbers, especially population density, natural or acquired resistance, possibility of asymptomatic carriers, vaccination status, etc.) and the availability of countermeasures (vaccine, treatment, isolation and quarantine). So the first step is the identification and characterisation of pathogens that could be responsible for outbreaks as well as the host populations that would be affected.

##### 16.2.1.1 International Public Health policies

After the SARS outbreak (severe acute respiratory syndrome due to a coronavirus) in 2005 the new International Health Regulations (IHR)<sup>123</sup> entered into force binding on 196 countries across the globe. The IHR define the rights and obligations of countries to report all public health emergencies of international concern in order to help the international community to prevent and respond to acute health risks having the potential to cross borders and threaten people worldwide. The diseases under concerns are all epidemic prone diseases,

<sup>121</sup> [https://ec.europa.eu/food/plant/plant\\_health\\_biosecurity/legislation/emergency\\_measures/xylella-fastidiosa\\_en](https://ec.europa.eu/food/plant/plant_health_biosecurity/legislation/emergency_measures/xylella-fastidiosa_en)

<sup>122</sup> <http://www.euro.who.int/en/countries/ukraine/news/news/2018/05/ukraine-restores-immunization-coverage-in-momentous-effort-to-stop-measles-outbreak-that-has-affected-more-than-12-000-this-year>

<sup>123</sup> [https://www.who.int/topics/international\\_health\\_regulations/en/](https://www.who.int/topics/international_health_regulations/en/)

food borne diseases, accidental and deliberate outbreaks, toxic chemical accidents and radio nuclear accidents as well as environmental disasters.

The IHR also specify procedures for the determination of a Public Health Event of International Concern (PHEIC) with the corresponding recommendations to prevent or reduce the international spread of disease and avoid unnecessary interference with international traffic. During a PHEIC, countries may request assistance with the management of the epidemic. However, the overall capacity to control and prevent the occurrence of epidemics or a pandemic is only as good as the weakest link in the chain and, similarly, the effectiveness of an international alert system will only be as good as its implementation.

### **16.2.1.2 EU policies controlling human communicable diseases**

Within the European Union, the European Centre for Disease Prevention and Control (ECDC) is responsible for identifying, assessing and communicating current and emerging threats to human health posed by infectious diseases. WHO Europe and the ECDC work together to develop a single European reporting and response system, and the ECDC assists EU Member States in certain aspects of IHR implementation, via Decision 1082/2013/EU.

Decision 2119/98/EC<sup>124</sup> established the network for epidemiological surveillance and control of communicable diseases, with implementing measures and a reference list of communicable diseases and case definitions. In 2013 it was replaced by Decision No 1082/2013/EU<sup>125</sup> on serious cross-border threats to health. This new Decision revived the network for the epidemiological surveillance of communicable diseases. It laid down rules on data and information that national competent authorities should communicate and provided for coordination of the network by the European Centre for Disease Prevention and Control (ECDC). The list of diseases and case definitions are regularly updated to reflect changes in disease incidence and prevalence, and in light of new scientific information, and evolving laboratory diagnostic criteria and practices.

Apart from communicable diseases, a number of other sources of danger to health, in particular related to other biological or chemical agents or environmental events, which include hazards related to climate change, could by reason of their scale or severity, also endanger the health of citizens in the entire Union and are included in the regulation.

Once a year, all EU MS & 3 EEA countries (Iceland, Liechtenstein, Norway) send data from their surveillance systems to ECDC. All data relate to occurrences of cases of communicable diseases and health issues under mandatory EU-wide surveillance. A number of conclusions drawn from these data are presented in the ECDC Annual Epidemiological Report.

List of human priority diseases: To perform a ranking of human pathogens and zoonosis ECDC has developed a tool based on a multi-criteria decision analysis (MCDA), with several steps to follow<sup>126</sup> for prioritisation such as criteria to assess a disease (e.g. probability of exposure, vulnerability of the population, consequences) and the weighting of criteria according to their importance in the society.

The impact of an epidemic depends on the number of cases, the severity of the disease but also the burden on society (missed work, hospital capacity, and public services). Unlike disasters such as earthquakes or floods, basic physical infrastructures will remain intact but the danger is a lack of personnel for public services. For example at the height of a pandemic flu up to 40% of employees could be out of work for a period of at least two weeks. Key measures to be taken include plans for maintaining a workable level of staff and ensure the continued health of necessary workers. In consequence national governments have to build scientific mechanisms to anticipate, identify, and address such threats.

### **16.2.2 Risk analysis and risk evaluation**

Risk assessment terminology is well established for chemical hazards to health (OECD, 2003)<sup>127</sup>, but the terms used in the areas of diseases differ somewhat as hazard characterisation and consequence assessment both deal with the effects of exposure.

When an alert is notified, (when a communicable disease from the reference list or another event which could endanger the health of citizens in the entire Union is reported), the Commission shall make promptly available

<sup>124</sup> <https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:31998D2119>

<sup>125</sup> [https://ec.europa.eu/health/sites/health/files/preparedness\\_response/docs/decision\\_serious\\_crossborder\\_threats\\_22102013\\_en.pdf](https://ec.europa.eu/health/sites/health/files/preparedness_response/docs/decision_serious_crossborder_threats_22102013_en.pdf)

<sup>126</sup> [https://ecdc.europa.eu/sites/portal/files/documents/Tool-for-disease-priority-ranking\\_handbook\\_0\\_0.pdf](https://ecdc.europa.eu/sites/portal/files/documents/Tool-for-disease-priority-ranking_handbook_0_0.pdf)

<sup>127</sup> [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=ENV/JM/MONO\(2003\)15&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=ENV/JM/MONO(2003)15&docLanguage=En)

to the national competent authorities a risk assessment of the potential severity of the threat to public health, including possible public health measures. The risk assessment shall be carried out by:

1. ECDC in accordance in the case of communicable diseases
2. European Food Safety Authority (EFSA) in matters of food safety and animal health
3. Other relevant Union agencies.

If the risk assessment needed is totally or partially outside the mandates of the agencies, and it is considered necessary for the coordination of the response at EU level, the Commission shall, upon request of the Health Security Committee (HSC) or its own initiative, provide an ad hoc risk assessment.

The Commission shall make the risk assessment available to the national competent authorities promptly through the EWRS<sup>128</sup> (Early warning and response system, centralized mechanism for the secure exchange of information in the occurrence of events with the potential to endanger public health in the EU). Where the risk assessment is to be made public, the national competent authorities shall receive it prior to its publication. The risk assessment shall take into account, if available, information provided by other entities, in particular by the WHO in the case of a public health emergency (PHE) of international concern. A guide for RRA methodology of PHE was released in 2012 by WHO<sup>129</sup>.

### 16.2.3 Risk Assessment methodology for human diseases

ECDC technical report "Operational guidance on rapid risk assessment methodology"<sup>130</sup>

The risk from a communicable disease is dependent on the likelihood of transmission in the population (probability) and the severity of disease (impact). Risk may be influenced by the environment in which the threat occurs, including political, public, media interest and perception of risk. Probability and impact are based on both the nature of the infectious agent (i.e. incubation period, mode of transmission, available interventions, vectors/reservoir species) and details of the incident (e.g. characteristics of the population at-risk including immune status, prevention, treatment and control measures available, and potential for international spread).

Rapid risk assessment, undertaken at the initial stages of an event of public health concern, is a core part of public health response, widely undertaken by public health professionals. However it is not often done in a formalised way but based on consensus opinion of experts. There are a limited number of examples of a more systematic and transparent approach to rapid risk assessment in the literature:

- A qualitative method for assessing the risk from emerging infections in UK (Morgan et al.2009) using algorithms to consider the probability of an infection occurring in the population, its potential impact, and identifying gaps in knowledge or data
- A prioritisation approach to rank emerging zoonoses posing the greatest threat in the Netherlands, based on 7 criteria (including probability of introduction, likelihood of transmission, economic damage, morbidity and mortality) to aid decision-making<sup>131</sup>.

#### **Rapid Risk Assessment methodology (when an outbreak is occurring, produced in a short time period with often limited information and circumstances possibly evolving quickly)**

1. Collecting event information: who has reported the incident, where, what is the agent, what are the symptoms, how many cases, what are the specimens taken and tests performed, what is the potential exposure to the agent, what are the protection means, etc.
2. Performing structured literature search/systematically collecting information: Identify basic facts about the disease and aetiological agent from a reference text (ideally less than 5 years old). Basic disease information/determinants
  - Occurrence: time, place, person, endemic, routes of introduction, Seasonal/temporal trends
  - Reservoir (if zoonotic, which species affected)
  - Susceptibility: are specific risk groups at increased risk of exposure/infection,

<sup>128</sup> <https://ewrs.ecdc.europa.eu/>

<sup>129</sup> [http://www.who.int/csr/resources/publications/HSE\\_GAR\\_ARO\\_2012\\_1/en/](http://www.who.int/csr/resources/publications/HSE_GAR_ARO_2012_1/en/)

<sup>130</sup> <https://ecdc.europa.eu/en/publications-data/operational-guidance-rapid-risk-assessment-methodology>

<sup>131</sup> <https://www.rivm.nl/bibliotheek/rapporten/330214002.html>

- Infectiousness: Mode of transmission, Incubation period
  - Clinical presentation: Disease severity (morbidity; mortality); Complications, specific risk groups
  - Laboratory investigation and diagnosis
  - Treatment and control measures
  - Previous outbreaks/incidents
3. Extracting relevant evidence: Role of the experts: Identify and seek advice from key experts, including public health, microbiology, infectious disease and other disease-specific experts or specialists within country and internationally
  4. Appraising evidence: The quality of evidence is the confidence in the truth of the information or data. Triangulation of evidence, including specialist expert knowledge, may be important to reach a consensus. Ensure a minimum of 2 to 3 data sources and agreement between these.
  5. Estimating the risk: assess the risk posed by the threat using the risk assessment algorithms. Two approaches are presented, one combines probability and impact into a single algorithm resulting in a single overall risk level, the second assesses probability and impact separately.

**Option 1 (combined approach), in Figure 36, includes consideration of the following:**

- Potential for transmission within the Member States:
- Potential for transmission within the EU (routes of introduction/spread)
- Threat unusual or unexpected,
- Availability of interventions (alters the course, influence the outcome)
- Severity of disease in this population/risk group

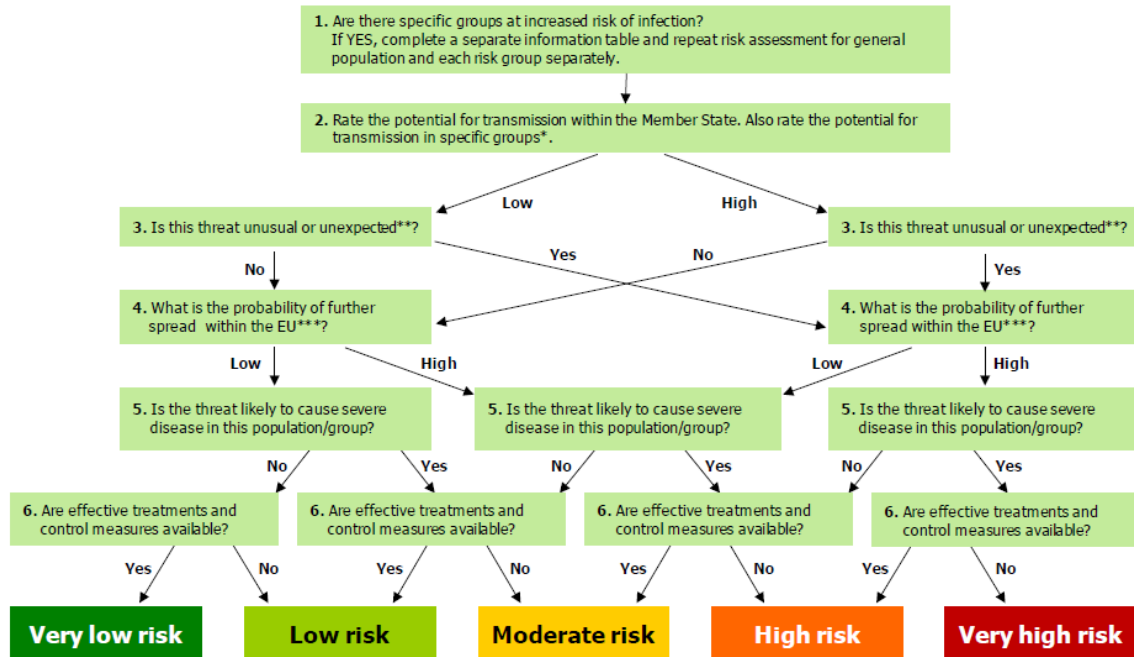
**Option 2 (separate algorithms for probability and impact): 3 separate algorithms**

1. Probability of infection in the MS (depends on likelihood of further exposure, infectiousness of the disease, susceptibility of the population)
2. Probability of infection in the EU (depends on availability of routes of introduction/spread, exposure, population susceptibility, infectiousness)
3. Impact: severity of disease in the population (morbidity, mortality, complications), infectiousness, mode of transmission, period of communicability, length of incubation and asymptomatic period, availability of treatment, prophylaxis and other control measures.

**These algorithms (Figure 37) are gathered in the risk-ranking matrix to produce an overall risk level.**

**Figure 36.** Single algorithm combining probability and impact resulting in single overall risk level (combined approach – option 1).

If in doubt (e.g. due to insufficient evidence), select the higher-risk option.



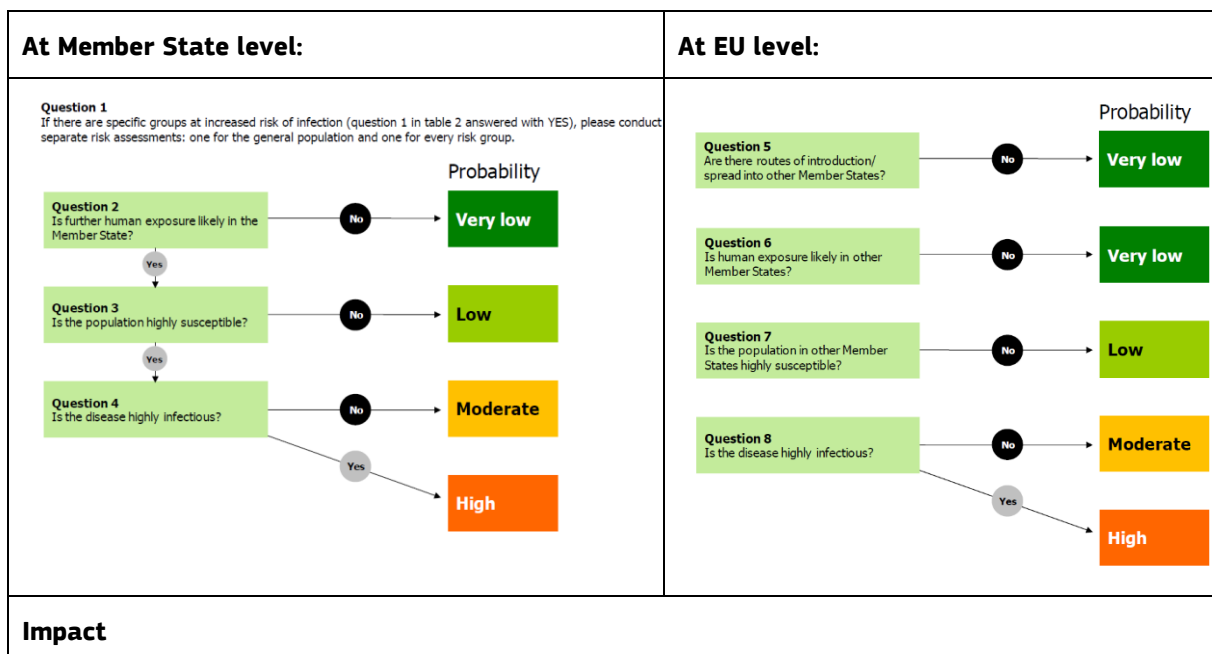
\* Depends on exposure, infectiousness, susceptibility of population.

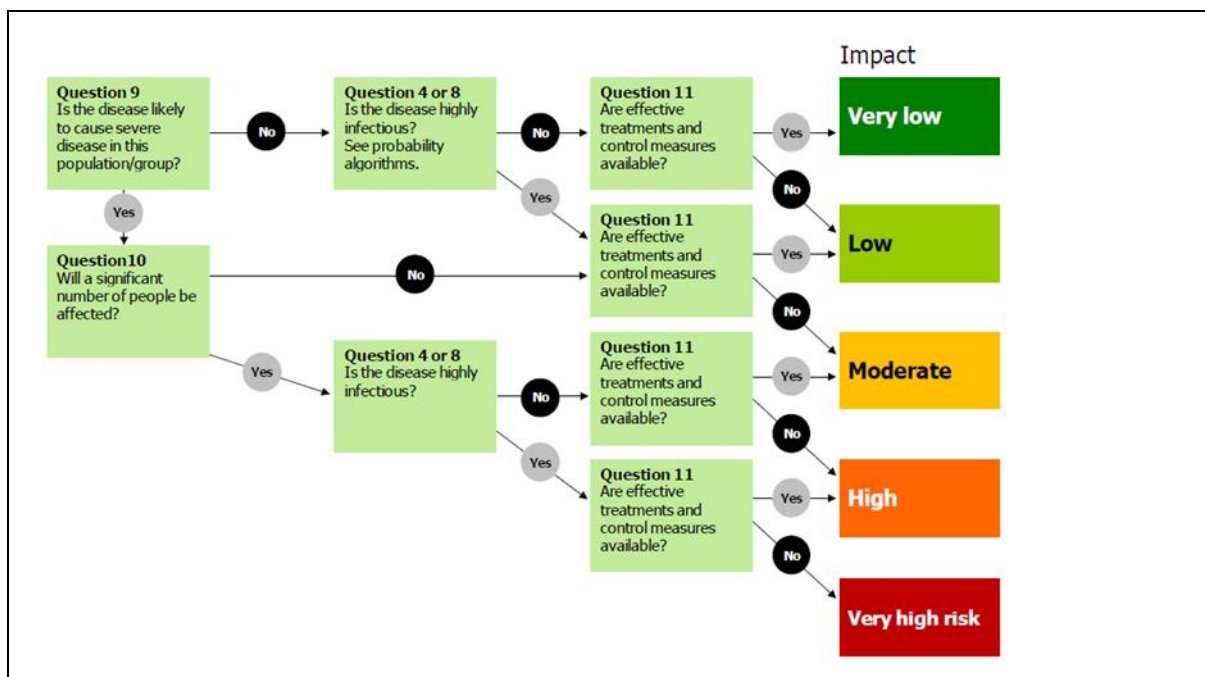
\*\* For example: unusual disease, setting, affected population group, increase in disease above expected threshold, appearance of a previously unreported disease. Where disease would not occur in population group, 'No' option should be chosen.

\*\*\* Depends on availability of routes of introduction/spread, exposure, population susceptibility, infectiousness.

Source: ECDC, 2011

**Figure 37.** Algorithm for calculating probability and impact (option 2).





### Matrix

Probability (part A) x impact (part B) = risk (part C)

Probability \ Impact	Very low	Low	Moderate	High
Very low	Very low risk	Low risk	Low risk	Moderate risk
Low	Low risk	Low risk	Moderate risk	Moderate risk
Moderate	Low risk	Moderate risk	Moderate risk	High risk
High	Moderate risk	Moderate risk	High risk	High risk
Very high	Moderate risk	High risk	High risk	Very high risk

Source: Author

### 16.2.4 Risk Treatment

As said drafting a generic risk assessment for communicable diseases is challenging as it strongly depends on the pathogen accountable, its host(s) and the environmental conditions. Consequently it is highly important to support extensive surveillance systems in order to react quickly and to build national capacities for a proper response for each disease.

The decision on cross-border threats to health<sup>5</sup> lays down rules on epidemiological surveillance, monitoring, and early warning of serious threats and includes preparedness and response planning, in order to coordinate and complement national policies. The MS shall, on the basis of the information from their monitoring systems, inform each other through the EWRS about developments of the threat. The EC collaborates with MS within the Health Security Committee (HSC), with relevant EU Agencies, in particular ECDC, and international organizations, such as the World Health Organization (WHO), to organise preparedness planning, alerts and appropriate assessment of the risks for the EU, and to coordinate the response.



MS shall provide every 3 years an update on the latest situation with regard to preparedness and response planning at national level<sup>132</sup> with the following:

**Status of the implementation of the core capacity standards for preparedness and response planning as determined at national level for the health sector, in accordance with IHR**

**Measures for ensuring interoperability between the health sector and other sectors including the veterinary sector, identified as critical in the case of an emergency, in particular:**

- Coordination structures in place for cross-sectoral incidents;
- Emergency operational centres (crisis centres);

**Description of the business continuity plans, measures or arrangements aimed at ensuring the continuous delivery of critical services and products.**

## 16.3 Animal diseases

### 16.3.1 Risk identification and the policy context

A distinction is made between epizootic – not transmittable to humans (e.g. foot-and mouth disease) and zoonotic – diseases transmittable from vertebrate animals to humans (e.g. avian influenza). Zoonosis are under higher concerns as they may represent a threat for human health however epizooties can impact heavily the economy of a country deeply involved in livestock production. The amount of animals concerned by a specific disease, their density, the contamination process and the breeding system used are all significant factors to be considered for assessing the risk of an outbreak. Similarly the measures to fight against a transmissible disease are based on the nature of the agent, its transmission route (direct contact or indirectly via contaminated equipment), geographical distribution, health impacts and evolution in the population.

#### 16.3.1.1 International Animal Health policies

Diseases previously classified by the World Organisation for Animal Health (OIE) within the list A represent fast spreading diseases of major economic importance. Such epidemics can result in substantial losses for governments, farmers and all stakeholders involved in the livestock production chain. In countries with a highly industrialised agricultural sector, vulnerability to the spread of such diseases is particularly high. Here is the list:

Foot and mouth disease	Vesicular stomatitis
Swine vesicular disease	Rinderpest
Peste des petits ruminants	Contagious bovine pleuropneumonia
Lumpy skin disease	Rift Valley fever
Bluetongue	Sheep pox and goat pox
African horse sickness	African swine fever
Classical swine fever	Highly pathogenic avian influenza
Newcastle disease	

The OIE lists A & B have now been replaced by one single list of notifiable terrestrial AND aquatic animal diseases (117 diseases in total)<sup>133</sup> counting several severe zoonotic diseases such as anthrax, Crimean Congo haemorrhagic fever, brucellosis, Rift Valley fever virus, Japanese encephalitis, Q fever, Tularemia and West Nile fever. OIE standards represent an international reference with no "legal" power of enforcement if not transcribed into the national legislation. OIE standards are only "binding" for Members which are Parties to the WTO (World Trade Organisation) SPS (Sanitary and Phytosanitary Measures) Agreement.

<sup>132</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0504&from=EN>

<sup>133</sup> <http://www.oie.int/animal-health-in-the-world/oie-listed-diseases-2018/>

### 16.3.1.2 EU policies controlling animal diseases

Under Directive 2003/99<sup>134</sup> MS shall ensure that all data on zoonotic agents and antimicrobial resistance are collected, analysed and published. These data should allow the identification of hazards and assessment of exposures. Monitoring must take place at the food chain level. Each MS shall transmit to the EC every year a report on trends and sources of those hazards. The reports are analysed by the European Food Safety Authority (EFSA) for the publication of annual summary Reports.

Since 2016 one single, comprehensive EU animal health law<sup>135</sup> (AHL: EU2016/429) supports the livestock sector with early detection and control of animal diseases, including emerging diseases linked to climate change. The Regulation lays down general and specific rules for the prevention and control of transmissible animal diseases (with a risk based approach) and ensures a harmonised approach to animal health across the Union. Diseases targeted are:

- Foot and mouth disease
- Classical swine fever
- African swine fever
- Highly pathogenic avian influenza
- African horse sickness

As well as around fifties of them listed in the Annex II.

### 16.3.2 Risk analysis and risk evaluation

As reported, in matters of food safety and animal health, risk assessment shall be carried out by the European Food Safety Authority (EFSA)<sup>136</sup>.

EFSA also provides guidance to national authorities on how to carry out monitoring and reporting activities on zoonoses, food-borne outbreaks and antimicrobial resistance. MS collect data and transmit a yearly report to EFSA for analysis. EFSA identifies risk factors that contribute to the prevalence of zoonotic micro-organisms in animal populations and makes recommendations on prevention and reduction measures for these pathogens.

Risk assessment for animal disease is a multi-analysis decision-support system, involving different type of experts. First the responsible pathogen is identified with a range of adverse events it might cause (e.g. clinical disease, death, spread within the same species or to other species, maybe public health consequences if it is a zoonotic pathogen or a pathogen carrying antibiotic resistance). A recent understanding of the problem should be made available (e.g. sources of pathogen, susceptible species, nutrition or space required by the species, import routes, exposure routes, import quantities etc.). Then the epidemiology of the infection should be described in time and space (modelling). The time component refers to the incidence over time, while space means the description of the geographical entities of interest with meaningful epidemiological or political boundaries. The latter often determine the disease control policy and options. Finally the potential management options must be described. They include measures which might control or eradicate the risks, current policy etc. The wider impact (e.g. economic, welfare) are also defined. Only realistic management measures merit consideration, it includes practicality (time and cost), and effectiveness with respect to infection, disease, animal welfare, and public health consequences. Risk assessment consequently is strongly dependent on the responsible pathogen; an illustration of such modelling exercise is given for an epidemic of classic swine fever (Gamado K et al. 2017). For new/emerging pathogens risk assessment means the evaluation of the likelihood and the biological and economic consequences of entry, establishment and spread of a hazard within the territory of an importing country. A risk assessment framework for emerging vector-borne livestock disease is comprehensively explained in a report from Wageningen University (de Vos et Al.)<sup>137</sup>

For zoonosis, the figure hereunder categorizes the evidence of zoonotic potential into 4 levels (**Figure 38**) by considering three key stages in the transmission of zoonoses (Palmer et al, 2005).

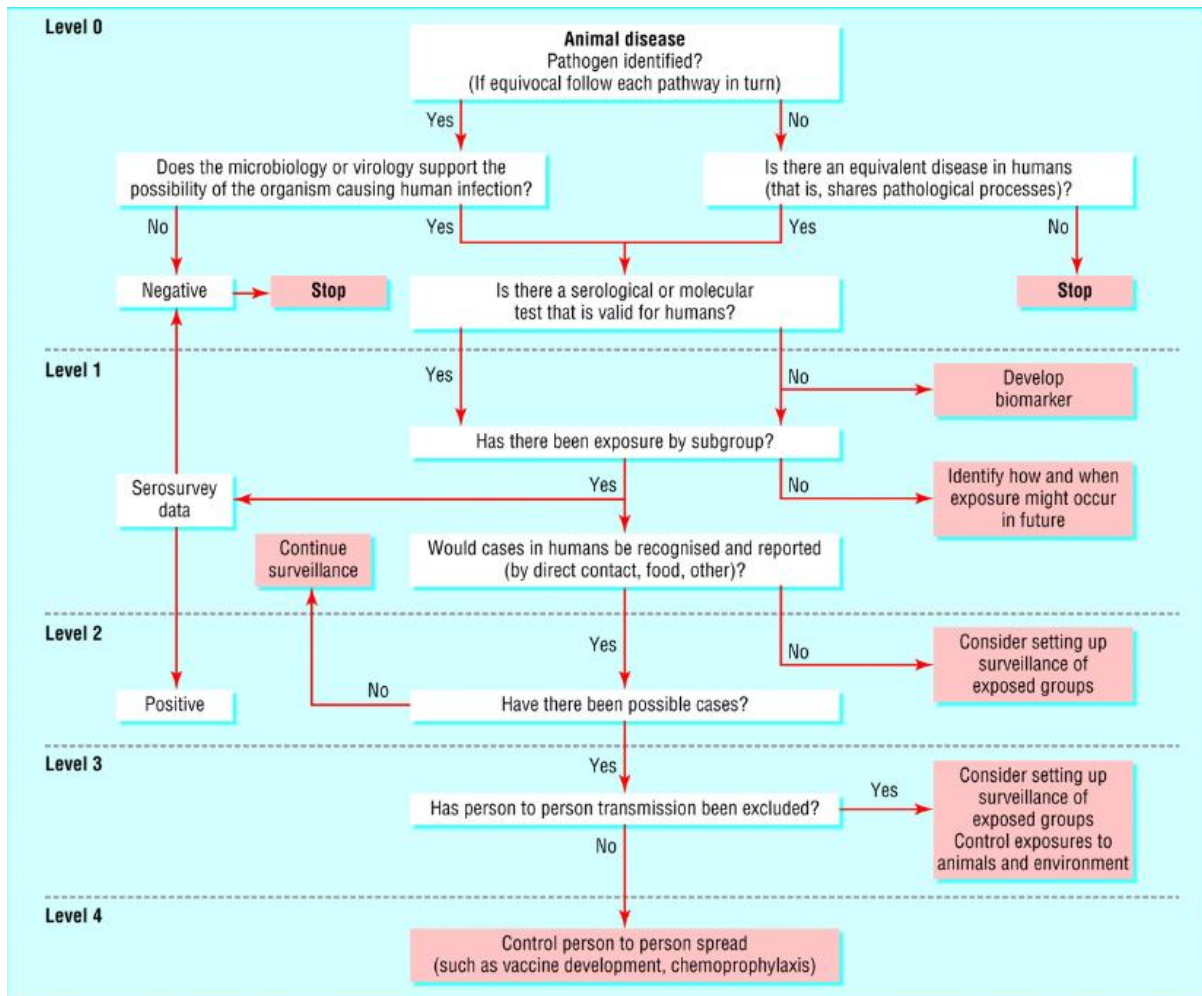
<sup>134</sup> <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32003L0099>

<sup>135</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0429>

<sup>136</sup> <https://efsa.onlinelibrary.wiley.com/doi/pdf/10.2903/j.efsa.2007.550>

<sup>137</sup> [https://www.wur.nl/upload\\_mm/5/f/8/d77e2ef6-cfe2-4b14-8cca-70bce8d355c5\\_RiskAssesmentFrameworkEmergingVectorBorneLivestock.pdf](https://www.wur.nl/upload_mm/5/f/8/d77e2ef6-cfe2-4b14-8cca-70bce8d355c5_RiskAssesmentFrameworkEmergingVectorBorneLivestock.pdf)

**Figure 38.** Categorization of zoonotic potential



Source: Author

### 16.3.3 Risk treatment

Risk assessment highly depends on the responsible pathogen, its host(s) and environmental conditions, it is therefore quite important to support extensive surveillance systems for all potential hosts (livestock, wildlife and pets) in order to respond quickly and to build national capacities for a proper response adapted to each species and diseases.

The animal health law<sup>138</sup> is laying down the rules for the prevention and control of animal diseases. These rules provide for surveillance, early detection, notification and reporting of diseases, as well as for disease awareness, preparedness and control. The competent authority in MS shall conduct appropriate surveillance to detect the presence of listed diseases and MS shall submit their surveillance programme to the Commission with regular reports on the results. MS shall immediately notify the Commission and other MS of any outbreaks of listed diseases. The competent authority should initiate the first investigations to confirm or rule out the outbreak, put in place preliminary disease control measures to prevent the spread of the disease, and should undertake an epidemiological enquiry.

For preparedness MS shall draw up and keep up to date, contingency plans and detailed instruction manuals laying down the measures to be taken in the event of the occurrence of a listed disease or of an emerging disease, in order to ensure a high level of disease awareness and preparedness and the ability to launch a rapid response. The competent authority shall ensure that simulation exercises concerning the contingency plans are carried out regularly.

<sup>138</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0429>

As soon as a listed disease is confirmed, the competent authority should take the necessary disease control measures, if necessary including the establishment of restricted zones, to eradicate and prevent the further spread of that disease. The Commission should adopt immediately measures such as stocking, supply, storage, delivery of antigen, vaccine and diagnostic reagent banks, special rules on movements for animals, emergency measures, and the listing of third countries and territories for the purposes of entry into the Union.

The measures taken are based on a risk assessment elaborated on the available scientific evidence and undertaken in an independent, objective and transparent manner. Due account should also be taken of the opinions of the European Food Safety Authority (EFSA).

## **16.4 High-security level biological laboratories**

### **16.4.1 Risk identification and the policy context**

The presence of laboratories manipulating pathogens, toxins or GMOs needs also to be taken into consideration for assessing biological risk. The consequences of laboratory acquired SARS infections in Asia (2004) raised concerns and triggered the improvement of national biosafety policies. WHO has published a laboratory biosafety manual (2004) and a biosecurity guidance (2006). Organisms targeted are pathogens and toxins but also biological materials such as reference strains, GMOs, vaccines or other pharmaceutical products for the sake of health and biodiversity.

#### **16.4.1.1 International conventions and agreements on biosecurity**

The Cartagena Protocol on Biosafety (2003) aims to ensure the safe handling, transport and use of living modified organisms (LMOs). Under the Biological Weapons Convention (1972), States Parties have accepted to provide annual reports on specific activities with data on research centres & laboratories, information on vaccine production facilities, information on national biological defence research, information on outbreaks of infectious diseases and occurrences caused by toxins, publication of results and contacts, information on legislation, regulations and other measures.

#### **16.4.1.2 EU policies on biosafety and biosecurity**

The EU Directive 2000/54/EC lays down minimum requirements for the health and safety of workers exposed to biological agents at work and the Directive 2009/41/EC governs the contained use of genetically modified micro-organisms. Reporting of incidents and/or accidents in laboratories is included in national regulations but there is no common European mechanism. Furthermore facilities and practices in containment level 3 laboratories throughout the EU are not of a comparable standard.

### **16.4.2 Risk analysis and risk evaluation**

The outcome of a pathogen risk assessment is its risk group (see WHO biosafety manual 2004<sup>139</sup>), which helps determining the minimum physical containment requirements, operational practice requirements, and performance and verification testing requirements for the safe handling and storing of the pathogen.

However international standards for biosafety and biosecurity are lacking which could lead to significant risk of accidental releases of infectious agents. National biosecurity risk management frameworks are often inconsistent. Several guidance documents are trying to integrate biosafety and biosecurity into a comprehensive biorisk management framework (Johnson B and Casagrande R. 2016).

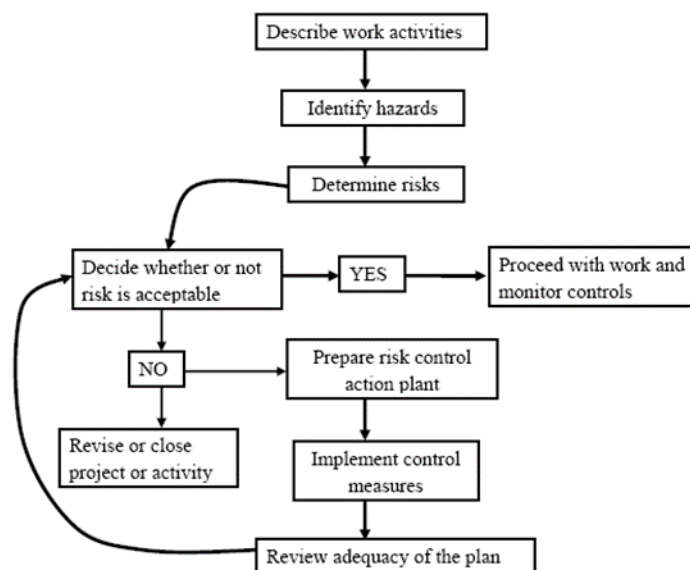
At EU level the CWA15793<sup>140</sup> (CEN Workshop Agreement) was released in 2011, it sets the requirements necessary to control the risks associated with handling or storage and disposal of biological agents and toxins in laboratories and facilities. This standard is voluntary, without the force of regulation. It aims at improving biorisk management system with adequate resources (Abad 2014) with RA process (**Figure 39**).

---

<sup>139</sup> [https://www.who.int/csr/resources/publications/biosafety/WHO\\_CDS\\_CSR\\_LYO\\_2004\\_11/en/](https://www.who.int/csr/resources/publications/biosafety/WHO_CDS_CSR_LYO_2004_11/en/)

<sup>140</sup> [ftp://ftp.cenorm.be/CEN/Sectors/TCandWorkshops/Workshops/CWA15793\\_September2011.pdf](ftp://ftp.cenorm.be/CEN/Sectors/TCandWorkshops/Workshops/CWA15793_September2011.pdf)

**Figure 39.** Framework to be followed in decision-making of all activities carried out in the facility.



Source: Abad, 2014.

For GMOs a network of inspectors, the European Enforcement Project (EEP) was founded in 1997 with the aim to exchange knowledge and experience from inspection of GMO contained use laboratories and of field (deliberate) releases of GMOs and resolve challenges and impasses and promote the harmonization of enforcement practice and strategies across the EU and beyond (de Wildt et al. 2015)

Finally, according to the EU CBRN action plan (2014) each MS should establish:

- a registry of facilities possessing any of the substances on the EU list of high risk biological agents and toxins
- a process to verify whether security arrangements of these facilities are adequate, including diagnostic laboratories
- a mechanism within facilities storing those biological agents and toxins to regularly review the need of such biological agents and toxins while keeping a good record of stored materials.

## 16.5 References

- Abad X. 2014. CWA 15793: When the Biorisk Management is the Core of a Facility Biosafety, Vol 3(2): 119
- Canadian Biosafety Guideline Pathogen Risk Assessment. 2018. <https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/guidance/pathogen-risk-assessment/document.html>
- de Vos C. et al. 2011. Risk Assessment Framework for Emerging Vector-Borne Livestock Diseases. Project: BO-10-009-002. AMB Express
- de Wildt P, et al. 2015. The European Enforcement Project on Genetically Modified Organisms Applied Biosafety Vol. 20, No. 1.
- EFSA. 2007. Opinion of the Scientific Panel on Animal Health and Welfare on the "Framework for EFSA AHAW Risk Assessments" Journal 550, 1-46.
- Gamado K, Marion G, Porphyre T. 2017. Data-Driven risk assessment from small scale epidemics: estimation and Model choice for spatio- Temporal Data with application to a classical swine Fever Outbreak. Front Vet Sci.4:16
- Johnson B and Casagrande R. 2016. Comparison of International Guidance for Biosafety Regarding Work Conducted at Biosafety Level 3 (BSL-3) and Gain-of- Function (GOF) Experiments. Applied Biosafety: Journal of ABSA International, Vol. 21(3) 128-141
- Morgan et al. 2009. Assessing the risk from emerging infections. Epidemiol Infect. 137:1521-30)

National Academy of Sciences and National Research Council. 2012. Biosecurity Challenges of the Global Expansion of High Containment Biological Laboratories Washington, DC: National Academies Press

Palmer S et al. 2005. Early qualitative risk assessment of the emerging zoonotic potential of animal diseases. *BMJ*; 331

OIE 2011. TERRESTRIAL ANIMAL HEALTH CODE. VOLUME II. Recommendations applicable to OIE Listed diseases and other diseases

## 17 Natech accidents

SERKAN GIRGIN, AMOS NECCI, ELISABETH KRAUSMANN

The impacts of natural hazard events on hazardous industrial facilities, pipelines, offshore platforms and other infrastructure that handles, stores or transports hazardous substances can cause cascading events such as fires, explosions, and toxic or radioactive releases (Showalter and Myers, 1994; Cruz and Krausmann, 2009; Girgin and Krausmann, 2016, Krausmann et al., 2019). These so-called Natech accidents are a recurring but often overlooked feature in many natural disasters and have often had significant human, environmental and economic impacts.

Major Natech accidents may involve multiple and simultaneous releases of hazardous substances over extended areas, damage or destroy safety systems and barriers, and down lifelines often needed for the prevention and mitigation of the consequences (Krausmann et al., 2010; Girgin, 2011). Emergency responders are also often neither equipped nor trained to handle a high number of concurrent hazardous incidents, in particular as they also have to respond to the natural hazard consequences in parallel. The 2002 river floods in Europe that resulted in significant hazardous substance releases, including chlorine and dioxins (Hudec and Lukš, 2004; Gautam and Van der Hoek, 2003), the 2011 Tōhoku earthquake and tsunami that caused a meltdown at a nuclear power plant and raging fires and explosions at oil refineries (Krausmann and Cruz, 2013), and Hurricane Sandy in 2012 that triggered multiple hydrocarbon spills are just a few examples of recent major events that highlight the importance of the possible consequences of Natech accidents. Especially the Tōhoku earthquake is a textbook example of a multi-hazard cascading risk. Between the earthquake and the tsunami, numerous Natech accidents were triggered. While the earthquake itself caused only limited damage due to the stringent protection measures in place, the tsunami and its impact on a nuclear power plant resulted in the most severe technological disaster ever recorded in the region whose adverse effects still persist (Krausmann and Cruz, 2013).

Natech accidents are events that cascade between natural and technological hazards and which feature complex consequences due to synergistic effects between the two different types of hazard. Therefore, targeted prevention, preparedness and response plans are needed to prevent Natech accidents and mitigate their consequences. Unfortunately, natural disaster risk reduction frameworks do mostly not consider technological hazards and technological accident prevention and preparedness programmes often overlook the specific aspects of Natech risk, resulting in a lack of dedicated methodologies and guidance for risk assessment and management both for industries and authorities (Krausmann et al., 2017).

Natech risks exist both in developed and developing countries where hazardous industrial sites are located in natural hazard regions. Natech events are often assumed to occur only during major natural events, e.g. strong earthquakes or floods. However, it does not necessarily require a natural disaster to cause a Natech accident; they can be triggered even by more frequent, minor natural hazard events (Necci et al., 2018). Human development (industrialisation, urbanisation) coupled with climate change will increase the risk of such events in the future. Successfully controlling a Natech accident has often turned out to be a major challenge where no prior risk assessment and proper preparedness planning have taken place. A comprehensive multi-sectoral and multi-hazard national Natech risk assessment is therefore crucial to pinpoint potential risk hotspots and see the overall picture including potential economic and environmental consequences that require special attention. A detailed discussion on how and in which setting Natech risks should be assessed in the NRAs is given by Girgin et al. (2019).

### 17.1 Risk Assessment Context

Hazardous industrial installations are inherent vulnerabilities for the socio-economic systems in which they are nested. Therefore, Natech risk assessment and management requires a comprehensive understanding of the interdependencies of the related natural, technological and societal systems. The risk assessment can be challenging even for the impact of a single natural hazard on a single industrial installation. Consideration of multiple natural hazards and multiple installations at the same time while bearing in mind possible secondary hazardous events that can be triggered by the primary Natech events (i.e. domino events) requires a regional, multi-hazard and multi-vulnerability risk assessment involving a complex chain of risk scenarios with multiple cascading events.

Some hazardous industries with Natech potential, especially the ones in the energy sector such as refineries, power plants, and oil and gas pipelines, are usually considered as critical infrastructure. It is common practice to analyse critical infrastructure as a separate pillar in national risk assessment (NRA) by focusing on natural-hazard related interdependency and business continuity aspects. However, it is also important to consider

Natech scenarios for such critical infrastructure due to the large quantities of hazardous substances that they contain, so that they can be protected effectively to ensure service continuity. Therefore, in some cases national Natech risk assessments should also be multi-sectorial.

Due to these complexities, Natech risk assessment requires a multidisciplinary approach involving stakeholders from both the natural and man-made hazards fields. It concerns on the one hand industry operators and authorities in charge of chemical accident management and on the other hand the public and civil protection. Occasionally, natural hazard conditions may result in hazardous consequences that might cross country boundaries. Especially flood hazards have a high potential to create cross-boundary Natech accidents (UNEP/OCHA, 2000). When countries share environmental resources or critical infrastructure, commerce and supply chains which might be affected by such accidents, they can face significant economic and social disruptions (Lindell and Perry, 1997). Therefore, in some cases national Natech risk assessment may also need multinational involvement.

Although recognised and even highlighted as an important emerging issue, Natech risk is currently not considered in a systematic way in NRAs. Usually Natech scenarios are only taken into account for some hazards, but not for others. This heterogeneity becomes a problem in the national risk evaluation when hazards that include the Natech risk in their assessment are ranked alongside the hazards that do not include the Natech risk. The key point for a proper Natech NRA is to consider all natural hazards and their interactions when assessing the potential for Natech accidents due to the presence of technological hazards. For this purpose, Natech risk can be calculated as part of the risk assessment for each natural hazard separately, or they can be considered as part of the risk due to technological hazards. In the first case, the Natech contribution to the overall natural-hazard risk is better represented which is useful for hazard ranking purposes, whereas in the second case the importance of different Natech scenarios can be better spotted. In fact, consideration of both aspects can be beneficial, but it is important not to count the overall Natech risk contribution both under natural and technological hazards, as this leads to double-counting of the same risk and the related impacts that could mislead the final evaluation. Good documentation and book-keeping practices would allow Natech-related contributions to be recorded properly, so that they can be easily separated from the overall analysis if necessary.

As many natural hazards have regional extent, the EU NRA guidelines suggest localised risk assessment only for advanced risk assessment. However, industrial installations are usually point assets at national or regional level. They are also not uniformly distributed but concentrated in certain regions for operational or logistic purposes. Therefore, technological hazards are usually localised and this aspect needs to be considered in the NRA. Consequently, it is necessary that Natech-related assessments are performed at local or regional level, and then subsequently combined at higher levels.

In order to assess Natech risk, industrial installations located in natural hazard zones should be identified and the expected on-site severity and impact potential of each natural hazard should be determined separately. This requires not only natural-hazard specific information, but also detailed technical data on the installations. Information that is already gathered through related regulations, but more specifically in the other sections of the NRA framework (e.g. natural hazard risk maps, industrial equipment data), should be utilized as much as possible in a time- and cost-effective manner. Considering Natech aspects during hazard-specific data collection and effective coordination of data collection and analysis activities may prevent repetition and duplication of work for Natech-specific needs. For this reason, the authority designated to manage the NRA should open communication channels with each actor and involve them in the Natech risk assessment process in an effective way.

Natech risk assessment methodologies are mainly based on industrial risk assessment methodologies that vary from qualitative to fully quantitative approaches. For Natech risk assessment, these methodologies need to consider equipment damage models for natural-hazard impacts, the possibility of multiple events at several equipment units or installations simultaneously, release and consequence scenarios considering natural hazard conditions, and the unavailability or malfunctioning of accident control and mitigation measures including lifelines due to natural hazard impact. Some technological risk control regulations (e.g. the EU Seveso III Directive) require that hazardous installations assess accident scenarios triggered by natural hazards and document the results in safety reports. Besides their original purpose, such information can also be utilized for NRA purposes. Frequently, however, industries carry out the assessment of natural hazards autonomously for these studies and although providing valuable information for the Natech hazard at the facility level, some of the natural-hazard related assumptions and scenarios may not be compatible with those used in the NRA. A better approach for assessing the Natech hazard in the NRA is one in which the authority provides the information about the risk scenarios used in the framework of the NRA for each natural



hazard to industry. In turn, industry can identify and build relevant Natech risk scenarios that are coherent with all the other risk scenarios chosen for the NRA. Following a systematic selection approach, possible Natech scenarios can be reduced into a manageable set of reasonably-to-be-expected or worst-case scenarios which should be analysed in detail for each installation separately. For consistency at the regional or national level, the Natech scenario building and analysis methods should be standardized throughout the NRA study and use of significantly different methods for different installations should be avoided.

The systematic evaluation of Natech risks in the NRA framework will not only result in informed decision making, but also in a better identification and prioritization of protection measures which can be implemented to reduce and control Natech risks in a cost- and time-effective manner.

## **17.2 Risk Identification**

The first step in national Natech risk assessment should be the identification of the industrial installations which might be affected by natural hazards. Natural disasters can impact large areas and Natechs can occur at any hazardous installation in the affected area, meaning that potentially multiple and simultaneous releases of hazardous substances can be triggered at various locations. Natural hazards having such an impact potential are normally covered in their own hazard-specific sections under the NRA. Therefore, the available natural hazard and natural risk information including maps can be utilized for Natech risk assessment. However, not only natural disasters but also high frequency-low impact natural hazards can result in cascading effects at individual installations if vulnerabilities exist and risks are not handled properly (Pescaroli and Alexander, 2015). Therefore, such hazards should also be considered whenever possible.

Industrial risk control and prevention regulations usually focus on industrial production and storage facilities that are located onshore. In addition to these facilities, other industrial installations such as offshore platforms, onshore and offshore pipeline systems, and onshore transportation systems handling or storing hazardous substances should also be included in national Natech risk assessment. Consideration of hazardous military installations, mining activities, and polluted sites which are usually excluded from the conventional industrial risk management process, is also recommended for the sake of completeness of the assessment.

Because each natural hazard has the potential to affect different geographic areas with different intensities, some industrial installations are not vulnerable to specific natural hazards simply because they are not located within their impact area. However, the national Natech risk assessment should always start with the complete inventory and exclude installations on a case-by-case basis depending on location. Linear and networked infrastructure, such as pipeline and transportation systems, which usually cross long distances through a wide range of climatic and geographical zones, require special consideration. Especially pipelines are usually located in the countryside where the detection of releases can be delayed, leading to major spills and significant economic damage particularly at special locations such as river crossings (Girgin and Krausmann, 2016). Time-variant operational characteristics should be further assessed for transportation systems.

If the number of industrial installations that should be analysed is large, a hazard ranking of the installations by using a preliminary but systematic methodology that considers Natech-specific constraints is suggested to select the most critical installations. For major natural hazards, which have a potential of multiple and simultaneous Natech events, not only major but also medium-sized installations should be included in the ranking, as they may result in a significant overall impact although their individual impacts may not be extensive. The list of upper and lower-tier industrial establishments covered by the Seveso III Directive (2012/18/EC) can be utilized as a baseline industrial facility inventory, which should be complemented with other industrial installations (e.g. pipelines, offshore platforms). As the tiers are determined according to the hazard characteristics and qualifying quantities of hazardous substances potentially present at the installations, the list can also be used for ranking purposes. In order to simplify the analysis, industrial parks or industrial zones where multiple installations are located in close proximity can be handled as single entities.

Following the identification of the Natech-prone installations, potential Natech scenarios should be developed for each installation. The main hazard scenarios in case of Natech accidents are fires, explosions and releases of toxic or radioactive materials. These hazards are obviously linked with the hazardous properties of the substances involved, but also with other factors such as, the substance inventory, the energy factor, the time factor, the intensity-distance relations, exposure and intensity-damage/injury relationships (Lees, 2012). All the methods available for hazard identification for conventional industrial accidents (e.g. checklists, hazard surveys, hazard and operability studies, and safety reviews) can be used for building Natech scenarios, provided that they take into account Natech-specific conditions:

- For a complete Natech analysis all the release events resulting from each possible damage mode should be addressed.
- Performance variations due to natural hazard impact should be introduced in the hazard identification and each release event should be fully developed
- Experts should carefully assess the potential unavailability or malfunctioning of industrial equipment and components, in particular barriers and protection layers
- Scenarios should consider not only the Natech-related release events but also their evolution given the potential contemporary unavailability of protection barriers and resources.

A damaged piece of equipment is very likely to produce uncontrolled performance variations, but impacts on performance can be expected in undamaged items, as well. Examples of such scenarios are explosions of chemical reactors due to loss of reaction control or the release of substances into the environment, instead of being captured or thermally degraded. Complex industrial processes may result in a large number of hazardous situations given the same operational deviations. Therefore, such scenarios should be carefully analysed when considering natural hazard conditions.

Natural-hazard specific mitigation measures (e.g. flexible connections, anchorage) may increase the resilience of equipment to certain natural hazards. It should be noted, however, that there is the misconception that structural and organizational protection measures in place to prevent and mitigate conventional industrial accidents would be sufficient to also protect against Natech events (Krausmann et al., 2017). In contrast, the natural event that damages or destroys industrial buildings and equipment can also render unavailable safety instrumentation (e.g. sensors, alarms), engineered safety barriers (e.g. containment dikes, deluge systems) and lifelines (e.g. power, water, communication) needed for preventing an accident or mitigating its consequences and avoiding its further escalation. Generally, for conventional technological accidents, emergency management systems consider that all safety systems are available, while for Natech events many of these could actually be unavailable at the same time. Assumptions on the availability of safety measures and personnel drastically affect the Natech scenarios. Therefore, care should be taken in scenario development when considering Natech-specific conditions.

Electricity is critical for the proper operation of an industrial installation and it is a lifeline that might be unavailable due to natural hazard conditions. This includes the primary power grid, but also back-up generators. Cable snapping, short circuits and floods are frequent causes of onsite power loss at industrial installations. As documented in past events, power loss alone can trigger a Natech accident (ARIA, 2009). In addition, safety systems and barriers implemented to prevent or mitigate accidents may be unserviceable due to lack of electricity. Water supply, both external and internal, might also be unavailable in case of a natural disaster. Underground pipes and connections, as well as water reservoirs, tanks, and pumping systems, are frequently damaged in earthquake, tsunami and flood events (Girgin, 2011). The natural disaster may either damage the equipment directly or cut the power supply required for its operation. Besides acting as the primary firefighting agent, water also serves for cooling purposes to control dangerous exothermic reactions. Therefore, a lack of water may not only hamper effective response activities, but may also result in adverse cascading events. Safety barriers play an important role in the prevention and mitigation of accidents. Due to natural hazard impacts, some or all of these systems may become unavailable or unserviceable. Affected barriers can be structural (e.g. containment dikes, deluge systems) or organizational (e.g. communication). For example, containment bunds lose their capacity to retain accidental spills during flood events. Similarly, firefighting equipment, such as sprinkler systems, can fail to activate after being damaged in earthquakes.

With respect to crisis response, onsite response teams may be hampered by natural hazard conditions. For instance, the industrial site may be flooded and may hence only be accessible by boat. In some cases, response personnel may be adversely affected by hazardous substance releases, rendering them unable to combat the consequences of the Natech accident. Fear and worry for their own lives and the lives of their families possibly affected by the natural hazard, can result in underperformance, as well. Offsite response teams may not always be available as they might be overwhelmed by having to respond to requests related to natural-disaster impacts on the population. In some cases, even if they are available they may not be able to reach the accident site as access routes can be blocked or otherwise rendered unusable (Necci et al., 2018).

### **17.3 Risk analysis**

Once the risk scenarios have been determined, the impacts of each scenario can be analysed by using available conventional methods that calculate the relations between natural hazard impact, physical or

operational damage, release of hazardous substance, consequences of the incident, and the impact area. Analysis priority can be given to the scenarios which are expected to result in the highest impact. Natech risks should be considered in all impact categories, i.e. human, economic and socio-political impacts. A Natech accident may not only result in short-term harm to public health and the environment, but also cause significant business interruption.

The severity of the hazardous consequences (i.e. fire, explosion, toxic dispersion) following the physical damage depends on several factors. The quantity of hazardous material and the rate at which it is released are probably the two most important factors. In conventional industrial risk assessment, different top events are often grouped into release categories having certain scenarios. This is because different top events, even though they originate from different mechanisms, could indeed release a similar amount of substance. This principle is at the basis of the bow-tie approach for industrial risk analysis and Natech accidents are no exception. Christou (1998) provides a generic but concise overview of the most common consequence phenomena and the associated models used in the analysis. TNO (2005) give a more detailed description of available models and the conditions under which they should be used.

The nature and extent of the consequences also highly depend on the environmental conditions. For this reason, conventional industrial accident scenarios are generally built on assumptions regarding the typical conditions at the facility and its surroundings. For Natech scenarios, environmental conditions might be significantly different from such typical conditions. For example, in case of weather-related events (e.g. storm, hurricane) the atmospheric conditions are usually close to extreme and unstable conditions rather than typical stable conditions. Similarly, the release environment might be different from the normal environment (e.g. release "into water" instead of "on ground" in case of flooding). For accurate results, such hazard-specific environmental conditions should be properly considered in the analysis. For a coherent analysis, environmental data from natural hazard scenarios that are part of the same NRA should be used by the experts performing the Natech risk analysis, when possible.

Natech accidents may result in exposed areas in all environmental compartments (i.e. air, soil, groundwater, and surface waters) that are much greater than for conventional industrial accidents. For example, if a flood causes an overflow of containment dikes at an installation, any released substance that would normally be captured within the containment dikes can easily be dispersed by the flood waters and contaminate the environment up to hundreds of kilometres through a river system (UNEP/OCHA, 2000). In the case of earthquakes, cracks that occur in containment dike floors due to ground movement may leak liquid substances that can eventually lead to significant groundwater pollution (Girgin, 2011). When the vulnerabilities due to the natural hazard are manifold, potential multiple releases from different parts of an installation and also from multiple installations simultaneously should be taken into account when assessing exposure. The possibility of on- and off-site secondary cascading events (i.e. domino effects) should be considered as well. In case of multiple simultaneous or cascading toxic releases, the overall extent of the toxic cloud can be significantly larger compared to a conventional chemical accident with a release from a single source.

The exposure and vulnerability of the population may also significantly vary during Natech conditions. For instance, when there is toxic atmospheric dispersion caused by an earthquake, shelter in-place might not be possible because of structural damage to buildings. Also, evacuation from the location of a Natech accident might not be feasible because of the blockage of escape routes by debris or flooding. In addition, people might be reluctant to evacuate a hazardous area if relatives are still trapped under the debris (Girgin, 2011, Steinberg et al., 2008). Such factors should be considered in undertaking exposure and vulnerability analysis.

In order to identify the Natech likelihood, the entire ensemble of industrial equipment at risk of damage (i.e. targets) should be assessed. Targets may sustain physical damage if the intensity of the natural hazard is sufficiently high or simply malfunction in case of lower impact severities. Damaged targets may directly release hazardous substances or trigger events that lead to loss of containment, while others can create an uncontrolled deviation in the system that can eventually result in a release. Some targets may have the function to control or mitigate undesirable events; hence, their failure can contribute to a release or amplify the consequences.

The Natech likelihood depends strongly on the vulnerability of equipment to the natural hazards at each site. The vulnerability to different natural hazards varies for a given equipment type. Atmospheric storage tanks, especially those with floating roofs, appear to be particularly vulnerable to natural hazards. This is critical from a risk point of view, as these units usually contain the largest amount of hazardous substances. In addition, in case of flammable releases the likelihood of ignition is high in earthquake and lightning triggered Natech accidents, which may escalate into major fires or explosions and result in cascading (domino)

accidents (Krausmann et al., 2011). Tanks can be subject to many different failure modes, for example: buckling of the tank shell, displacement of the tank (e.g. by floating or shifting), external impact (e.g. collision with other equipment items), or collapse of tanks supports (e.g. foundation or legs) (GDL Natech, 2016). Other equipment (e.g. reactors, columns, separators, pumps, heat exchangers) also retain significant amounts of hazardous substances and can be affected by natural hazards similar to storage tanks. Onsite pipes and pipework are also frequently damaged by the displacement of equipment or by external impact such as collision with moving (e.g. floating, falling) objects usually launched by the natural hazard. In a detailed Natech risk assessment, besides direct physical damage, indirect effects such as uncontrolled operational variations can also be assessed.

The damage from the natural hazard is directly linked to the failure modes that produced the damage. It should also be noted that the same unit may be affected in many different ways and, as a consequence, experience different types of damage due to the same natural hazard. In principle, all failure modes should be analyzed for every vulnerable unit. This kind of assessment utilizes detailed numerical methods that describe the mechanisms that produce the damage with great accuracy. However, the information required for such a detailed Natech risk assessment is usually not available. In addition, the associated time and resource demand can be prohibitive for large projects. One solution is to perform the analysis only for the most critical units. The analyst would typically select the units with the biggest potential for harm in case of an accident (extent of damage), although the ranking could incorporate additional information (e.g., known vulnerability of units, occurrence of Natech accidents in the past). The drawback of this approach is that potentially relevant Natech information of the excluded units is not captured.

Unless detailed numerical methods are used, the conventional approach for the damage assessment is based on damage states (DS) which group different and possibly numerous damage conditions under a set of qualitative damage categories ranging from no damage (DS1) to total collapse (DS5). For most industrial equipment, historical Natech accident and near-miss data is used to deduce reliable damage probabilities for each damage state. Simplified fragility functions in the form of fragility curves are available for storage tanks for earthquakes (Fabbrocino et al., 2005), floods (Landucci et al., 2012), and lightning (Necci et al., 2013). However, these curves cover only specific conditions (e.g. equipment characteristics, operational conditions) and for other conditions and also for other equipment some expert judgement is usually necessary in the assessment process. The actual damage that may happen in case of a certain natural hazard impact depends on a number of factors such as construction characteristics (e.g. design criteria, material), current physical state (e.g. corrosion, aging, fatigue), and operative conditions (e.g. filling level, pressure). For this reason, it is hard to establish a priori what damage state is to be expected for a given equipment for a given natural hazard scenario. Therefore, in most cases all plausible damage states should be analyzed. Because the damage states are usually defined in qualitative terms (e.g. minor, moderate, extensive), it is difficult to associate a damage state to a well-defined release event and current practice is limited to the use of very generic scenarios that are based on expert judgement.

Each Natech scenario has a conditional probability of occurrence given a natural hazard trigger. The overall Natech event probability can be calculated by summing a set of conditional event probabilities including damage, release, and consequence-related events (e.g. ignition, explosion), which can be calculated by various methods (Lees, 2012). For estimating the conditional probability of release following a damage, the most simplified assumption is to select a single release scenario for each damage state considered. While it can be straightforward to assign a single release scenario and a single probability to a damage state, some analysts may consider multiple release scenarios for some damage states. In that case, a different probability of occurrence should be assigned to every release event assessed and all events (including the “no release” scenario) should be regarded as mutually exclusive. Unfortunately, there is no established method to determine conditional release probabilities for Natech accidents. Therefore, in case of multiple release scenarios for each damage state, conditional release probabilities are either taken as equal to one or assigned by expert judgment. It is usually recognised that the vulnerability of an asset changes if two independent hazards occur in a short time lapse. However, intermittent natural hazards, even if they are not major events may also affect the vulnerability of industrial equipment. For example, high flow conditions during medium-sized floods may increase riverbed scouring which reduces the cover on pipelines at river crossings, eventually leading to pipe breaks due to excess external forces or debris impacts (Girgin and Krausmann, 2016). Whenever it is feasible, such factors should be considered while estimating the probability of possible damage.

## 17.4 Risk evaluation

Being an inherent cascading multi-hazard risk, the adequate evaluation of Natech risk requires proper handling and ranking of cascading risks in the NRA process. Natech risk can be evaluated:

- as a part of the risk assessment of a natural hazard in the so-called multi-hazard risk analysis;
- as part of the risk assessment of technological hazards;
- as a separate dedicated risk assessment.

In the process of ranking the risks, it should be clearly stated if Natech risks are included for each risk, and how they are assessed. As a general rule, risks that include Natech risk assessment should not be directly compared with risks that do not include this assessment. Comparison could still be carried out, provided that the contribution of Natech risk was fully explicated. Keeping track of Natech risk contributions also allows the comparison of the level of Natech risk with the risk of the other natural and man-made hazards.

Consequences beyond the local extent are quite common especially if critical infrastructure is directly involved or affected by the Natech events, or if the impacts areas are extended, e.g. during floods. This results in amplified economic impacts, which can sometimes be as big as or much bigger than the impact of the natural hazard itself. For example, the March 5, 1987 earthquake in Ecuador (Ms 6.9) caused the destruction of more than 40 km of the Trans Ecuatorian Oil Pipeline due to massive debris flows following the earthquake. Approximately 100,000 bbl of oil spilled into the environment and the loss of revenue during the five months required for repair was 800 million USD, equal to 80% of the total earthquake losses (NRC, 1991). Therefore, it is important to quantify Natech damage not only considering the cost of direct physical damage, but also considering all cascading consequences. Similar to industrial and nuclear risks, the long-term adverse effects of released environmentally persistent and carcinogenic substances on human health and the environment should be evaluated for Natech risk while evaluating socio-economic impacts.



















Besides ecological damage, large areas may become unfit for human use (e.g. agriculture, drinking water, living), and comprehensive clean-up and restoration may be needed. Especially groundwater and surface water clean-up operations are very costly and may require long time periods. Similar to other hazards, the socio-economic implications of Natech accidents are difficult to quantify. Nevertheless, historically all major Natech accidents have had a strong impact on both the EU's and member states' policies. Therefore, this aspect is important for overall evaluation.

The potential impacts of Natech accidents are numerous and target-specific. On top of this, the perception and acceptance of decision makers and the public to different types of technological consequence scenarios are usually very different. This makes difficult the quantification and evaluation of consequences, especially if they are originating from multi-hazard cascading events. Usually shared decision making by all stakeholders is required similar to the other hazards considered by the NRA. Specific to Natech risk, the stakeholder group should include both natural and man-made hazard related actors. The following guidelines may be useful for the evaluation of the impacts:

- Toxic vapour clouds may have the largest impact on the population, but lower impact on the environment and almost no impact on the asset.
- Fires and explosions may have the largest impact on the asset, but lower impact on the people and very low impact on the environment.
- Liquid spills of chemicals, solvents or fuels may have the largest impact on the environment, but lower impact on the asset and almost no impact on the population.
- Nuclear accidents with loss of radioactive material may have high impact on both the population and the environment and lower impact on the asset.

Figure 40 summarizes the expected maximum impact of some of the most common major accident typologies in case of Natech accidents.

**Figure 40.** The maximum potential levels of socio-economic impacts as ranked for different types of consequences.

						
Very High						Political/Social
						
High						Environmental
						
Medium						Economic
						
Low						Human
	Toxic Vapor Cloud	Fire - Explosion	Liquid spill	Nuclear accident		

Source: JRC

The EU NRA guidelines emphasise the importance of a periodic review of NRAs to keep them updated as risks emerge and evolve. For Natech risks, such reviews need to consider two aspects: 1) changes in natural hazard risks (e.g. due to new or improved models, or changes in natural hazard frequency/severity caused by climate change), and 2) changes in the industrial installations due to process or capacity modifications and upgrades which are quite common during the operational lifeline of an installation.

Risk analysis methodologies for both natural and technological hazards have inherent uncertainties that need to be stated explicitly in the analysis phase and considered in the decision-making process. Because Natech risk assessment unites methods from both fields, it also compounds and amplifies uncertainties. Therefore, the results should be evaluated with care. Documentation of the Natech scenarios and the analysis methods utilized to estimate the probable extent and impact of hazardous consequences is important not only for keeping track of uncertainties, but also for being able to merge and compare the results properly, especially if local or regional assessments are conducted as part of national assessment.

## 17.5 Good Practices

Being an emerging risk, even in developed countries Natech risk is hardly assessed by national competent authorities in a comprehensive manner. Although there are no detailed NRAs, there are national and international programs and regulations that require the assessment of Natechs in safety documents of hazardous installations and adoption of measures necessary to reduce the related risks. Usually these rules have been implemented in the aftermath of one or several major Natech accidents (Lindell and Perry, 1997).

In the European Union, Directive 2012/18/EC on the control of major-accident hazards involving dangerous substances (Seveso III Directive) that regulates chemical accident risks at fixed industrial installations explicitly addresses Natech risks and requires the installations to routinely identify environmental hazards, such as floods and earthquakes, and to evaluate them in safety reports. With its latest amendment, the directive also requires an assessment of accident scenarios triggered by natural hazard impact. In France, the new zoning regulation for industrial installations in seismic areas divides industrial establishments into two risk groups to identify Natechs risks and to facilitate emergency planning: normal risk and special risk (Decrees 210-1254<sup>141</sup> and 2010-1255<sup>142</sup>). Installations in the second category have to guarantee the containment of hazardous materials under seismic loading by complying with specific mechanical resistance requirements to ensure a structure's capability to withstand a given value of ground acceleration, chosen in accordance with the seismic zone it is in (Planseisme, 2016). In Germany, the rule TRAS 310 requires industrial establishments with major chemical accident potential to assess the risk of flood-triggered accidents at their installations, to take necessary risk reduction measures, and to consider the possibility of an increase of flood risk due to climate change (TRAS 310, 2012). They also introduce the innovative concept of

<sup>141</sup> <https://www.legifrance.gouv.fr/eli/decret/2010/10/22/2010-1254/jo/texte>

<sup>142</sup> <https://www.legifrance.gouv.fr/eli/decret/2010/10/22/2010-1255/jo/texte>

"accident despite precautions", which requires the inclusion of Natech scenarios into emergency plans, even if their risk has been mitigated.

The Natech Addendum to the OECD Guiding Principles on Chemical Accident Prevention, Preparedness and Response contains amendments to the guiding principles for guidance on Natech accidents (OECD, 2015). In Japan, the Law on the Prevention of Disasters in Petroleum Industrial Complexes and Other Petroleum Facilities was updated after the Tokaichi-oki earthquake triggered several fires at a refinery in 2003 (CAO, 2012). Moreover, the amended Japanese High Pressure Gas Safety (HPGS) Law requires companies to take any additional measure necessary to reduce the risk of accidents, to protect its workers and the public from any accidental releases caused by earthquake and tsunami (Cruz and Okada, 2008). In the US, the state of California released the Accidental Release Prevention (CalARP) program, which calls for a risk assessment of potential hazardous materials releases due to an earthquake (CalARP, 2014).

No risk assessment tool that is currently available can capture all aspects of Natech risk. However, recently, risk assessment tools and methodologies capable of estimating regional Natech risk have become available. The JRC's Rapid Natech Risk Assessment and Mapping System (RAPID-N), which is publicly available at <http://rapidn.jrc.ec.europa.eu>, allows quick local, regional and national Natech risk assessment including natural hazard damage assessment and accident consequence analysis with minimum data requirement (Girgin and Krausmann, 2012; Girgin and Krausmann, 2013). Other available tools are ARIPAR for a quantitative treatment of the problem (Antonioni et al., 2009), and PANR for a qualitative assessment methodology (Cruz and Okada, 2008). Although currently limited to selected natural hazards and certain types of installations, the tools are in active development to cover additional hazards and industries, and they can significantly facilitate NRA studies.

## 17.6 Gaps and Challenges

A number of research and policy challenges and gaps exist that can prevent effective Natech risk management. These include a lack of data on equipment vulnerability against natural hazards, and the unavailability of a consolidated methodology and guidance for Natech risk assessment, which has, for instance, resulted in a lack of Natech risk maps (Krausmann and Baranzini, 2012). The few existing Natech risk maps are usually only overlays of natural hazards with industrial site locations and are therefore only Natech hazards maps. Proper Natech risk maps must also include an estimate of the potential consequences, which may differ significantly from site to site. Attention should be paid to the inherent limitations of existing equipment vulnerability models originating from non-Natech applications if these are used to substitute for Natech-specific models.

By analysing past Natech accidents, conclusions can be drawn concerning the vulnerability of industrial equipment to different natural hazards, common damage and failure modes, and the hazardous substances mostly involved in the accidents. Incident databases are important tools for this purpose. The JRC's Natech accident database (eNatech) is such a database specifically designed for the systematic collection, analysis, and dissemination of worldwide Natech accident data. It is publicly available at <http://enatech.jrc.ec.europa.eu>.

## 17.7 References

- Antonioni, G., Bonvicini, S., Spadoni, G. and Cozzani, V. (2009) Development of a framework for the risk assessment of Na-tech accidental events, *Reliability Engineering and System Safety*, 94:1442-1450, doi:10.1016/j.res.2009.02.026.
- ARIA (2009) Report No 40197 - 23/07/2009 - ALLEMAGNE - 00 - IBBENBÜREN C20.14 - Manufacture of other organic basic chemicals, available at [https://www.aria.developpement-durable.gouv.fr/fiche\\_detaillee/40197\\_en/?lang=en](https://www.aria.developpement-durable.gouv.fr/fiche_detaillee/40197_en/?lang=en).
- CalARP (2014) Guidance for California Accidental Release Prevention (CalARP) Program, Seismic Assessments, CalARP Program Seismic Guidance Committee.
- CAO (2012) Petroleum Refinery Complex, Etc. Disaster Prevention Law, Cabinet Office, Government of Japan, available at [http://www8.cao.go.jp/kisei-kaikaku/oto/otodb/english/houseido/hou/lh\\_05080.html](http://www8.cao.go.jp/kisei-kaikaku/oto/otodb/english/houseido/hou/lh_05080.html).
- Christou, M.D. (1998) Consequence analysis and modelling, in: Kirchsteiger, C., Christou, M.D., Papadakis, G.A. (Eds.) *Risk assessment and management in the context of the Seveso II Directive*, Industrial Safety Series, Vol. 6, Elsevier, Amsterdam.

- Cruz, A. M. and Krausmann, E. (2009) Hazardous-materials releases from offshore oil and gas facilities and emergency response following Hurricanes Katrina and Rita, *Journal of Loss Prevention in the Process Industries*, 22(1):59-65, doi:10.1016/j.jlp.2008.08.007.
- Cruz, A. M. and Okada, N. (2008) Methodology for preliminary assessment of Natech risk in urban areas, *Natural Hazards*, 46(2):199-220, doi:10.1007/s11069-007-9207-1.
- Fabbrocino, G., Iervolino, I., Orlando, F. and Salzano, E. (2005) Quantitative risk analysis of oil storage facilities in seismic areas, *Journal of Hazardous Materials*, 123(1-3):61-69, doi:10.1016/j.jhazmat.2005.04.015.
- Gautam, K.P and Van der Hoek, E.E. (2003) Literature study on environmental impacts of flood, Delft Cluster Publication - DC1-233-13.
- GDL NATECH (2016) "Metodologia per la gestione di eventi Natech" Valutazione e Gestione del Rischio negli Insediamenti Civili ed Industriali, Istituto Superiore Antincendi, Roma, 13-15 Settembre 2016.
- Girgin, S. (2011) The natech events during the 17 August 1999 Kocaeli earthquake: aftermath and lessons learned, *Natural Hazards and Earth System Sciences*, 11(4):1129-1140, doi:10.5194/nhess-11-1129-2011.
- Girgin, S. and Krausmann, E. (2012) Rapid Natech risk assessment and mapping tool for earthquakes: RAPID-N, *Chemical Engineering Transactions*, 26:93-98, doi:10.3303/CET1226016.
- Girgin, S. and Krausmann, E. (2013) RAPID-N: Rapid natech risk assessment and mapping framework, *Journal of Loss Prevention in the Process Industries*, 26(6):949-960, doi:10.1016/j.jlp.2013.10.004.
- Girgin, S. and Krausmann, E. (2016) Historical analysis of U.S. onshore hazardous liquid pipeline accidents triggered by natural hazards, *Journal of Loss Prevention in the Process Industries*, 40:578-590, doi:10.1016/j.jlp.2016.02.008.
- Girgin, S., Necci, A., Krausmann, E. (2019) Dealing with cascading multi-hazard risks in national risk assessment: The case of Natech accidents, *International Journal of Disaster Risk Reduction*, 35, doi:10.1016/j.ijdrr.2019.101072.
- Hudec, P. and Lukš, O. (2004) Flood at Spolana a.s. in August 2002, *Loss Prevention Bulletin*, 180:36-39.
- Krausmann, E., Cruz, A.M. and Affeltranger, B. (2010) The impact of the 12 May 2008 Wenchuan earthquake on industrial facilities, *Journal of Loss Prevention in the Process Industries*, 23(2):242-248, doi:10.1016/j.jlp.2009.10.004.
- Krausmann, E., Renni, E., Campedel, M. and Cozzani, V. (2011) Industrial accidents triggered by earthquakes, floods and lightning: lessons learned from a database analysis, *Natural Hazards*, 59(1):285-300, doi:10.1007/s11069-011-9754-3.
- Krausmann, E. and Baranzini, D. (2012) Natech risk reduction in the European Union, *Journal of Risk Research*, 15(8):1027-1047, doi:10.1080/13669877.2012.666761.
- Krausmann, E. and Cruz, A.M. (2013) Impact of the 11 March 2011, Great East Japan earthquake and tsunami on the chemical industry, *Natural Hazards*, 67(2):811-828, doi:10.1007/s11069-013-0607-0.
- Krausmann, E., Cruz, A.M. and Salzano, E. (2017a) Natech risk assessment and management: reducing the risk of natural-hazard impact on hazardous installations, Elsevier, Amsterdam, ISBN 9780128038079.
- Krausmann, E., Girgin, S. and Necci, A. (2019) Natural hazard impacts on industry and critical infrastructure: Natech risk drivers and risk management performance indicators, *International Journal of Disaster Risk Reduction*, 40, 101163, <https://doi.org/10.1016/j.ijdrr.2019.101163>.
- Landucci, G., Antonioni, G., Tugnoli, A. and Cozzani, V. (2012) Release of hazardous substances in flood events: Damage model for atmospheric storage tanks, *Reliability Engineering and System Safety*, 106:200-216, doi:10.1016/j.ress.2012.05.010.
- Lees, F. (2012) *Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control*, 4th Edition, ISBN 978-0-12-397189-0, doi:10.1016/C2009-0-24104-3.
- Lindell, M. K. and Perry, R. W. (1997) Hazardous Materials Releases in the Northridge Earthquake: Implications for Seismic Risk Assessment, *Risk Analysis*, 17(2):147-156, doi:10.1111/j.1539-6924.1997.tb00854.x.
- Necci, A., Antonioni, G., Cozzani, V., Krausmann, E., Borghetti, A., and Nucci, C. A. (2013) A model for process equipment damage probability assessment due to lightning, *Reliability Engineering and System Safety*, 115:91-99, doi:10.1016/j.ress.2013.02.018.



Necci, A., Krausmann, E. and Girgin, S. (2018) Emergency planning and response for Natech accidents, In: NEA (2018) Towards an all-hazards approach to emergency preparedness and response: Lessons learnt from non-nuclear events, OECD Publishing, Paris, doi:10.1787/9789264289031-en.

NRC (1991) The March 5, 1987, Ecuador Earthquakes: Mass Wasting and Socioeconomic Effects, The National Academies Press, Washington D. C., ISBN 978-0-309-04444-8, doi:10.17226/1857.

OECD (2015) Addendum Number 2 to the OECD Guiding Principles for Chemical Accident Prevention, Preparedness and Response (2nd Ed.) to address natural hazards triggering technological accidents (Natechs), Series on Chemical Accidents No. 27, ENV/JM/MONO(2015)1.

Pescaroli, G. and Alexander, D. (2015) A definition of cascading disasters and cascading effects: going beyond the "toppling dominos" metaphor, *Planet@Risk*, 2(3):58-67, Global Risk Forum, Davos.

Planseisme (2012), ICPE « à risque spécial » (in French), Ministère du Développement Durable, available at <http://www.planseisme.fr/ICPE-a-risque-special-1476b>.

Showalter, P. S. and Myers M. F. (1994) Natural disasters in the United States as release agents of oil, chemicals, or radiological materials between 1980-1989: analysis and recommendations, *Risk Analysis*, 14(2):169-182, doi:10.1111/j.1539-6924.1994.tb00042.x.

Steinberg, L.J., Sengul, H. and Cruz, A.M. (2008) Natech risk and management: an assessment of the state of the art, *Natural Hazards*, 46(2):143-152, doi:10.1007/s11069-007-9205-3.

TNO (2005) Methods for the calculation of physical effects due to releases of hazardous materials (liquids and gases) (Yellow Book, CPR 14E), Committee for the Prevention of Disasters, The Hague, The Netherlands.

TRAS 310 (2012), "Technical Rule on Installation Safety: Precautions and Measures due to Precipitation and Floods", German Federal Cabinet, BMU, non-official short version, available at [http://www.kas-bmu.de/publikationen/tras/TRAS\\_310\\_GB\\_shortversion.pdf](http://www.kas-bmu.de/publikationen/tras/TRAS_310_GB_shortversion.pdf).

UNEP/OCHA (2000) Cyanide Spill at Baia Mare, Romania. REPORT - Joint UNEP/OCHA Environment Unit - Disaster Response Branch UN Office for the Coordination of Humanitarian Affairs Palais des Nations - CH-1211 Geneva 10, Switzerland.

## 18 Chemical Accidents

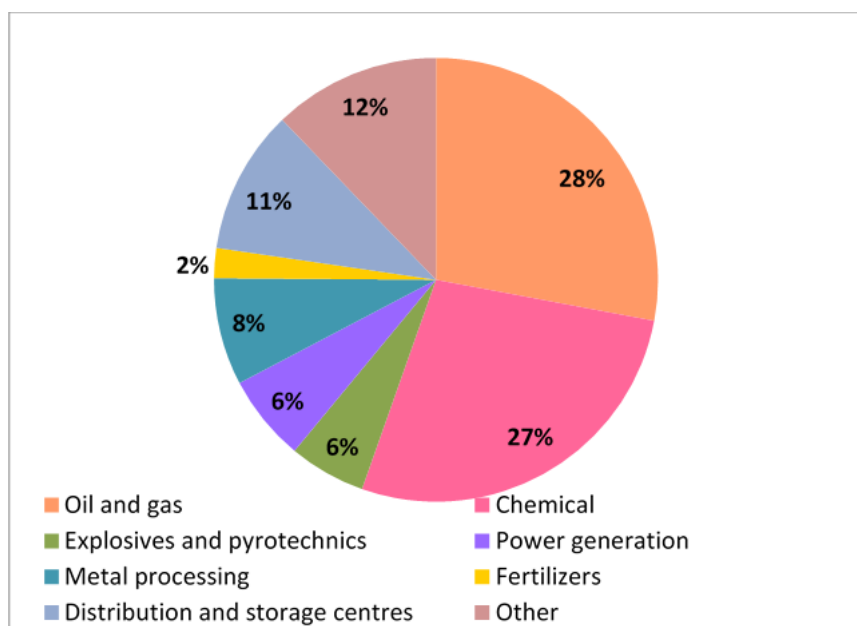
MAUREEN WOODS, RICHARD GOWLAND

### 18.1 Overview

Chemical incidents are significantly different from natural hazards and even distinctly apart from other kinds of well-known technological disasters, notably in the nuclear industry and aviation. Unlike these technological disaster types, the term “chemical accident” is not associated with a specific industry. Rather, significant chemical accident risks are present in a wide variety of industries characterized by vast differences in the substances, processes, technology and equipment that create the risk (**Figure 41**). Chemical accident risk<sup>143</sup> consists of several components and therefore, understanding accident causality, i.e., why chemical accidents happen in the first place, is critical to effective risk management and finding dependable means to measure risk management performance.

Chemical accident risk is highly dependent on the activity of the site, the processes it operates and the types of dangerous substances it uses. There are hundreds of processes in oil and gas or chemicals processing industries alone. They may be present in land-based establishments (also known as “fixed facilities), pipelines, transport by rail, road and water, and offshore oil exploration platforms. Explosives industries, involving manufacture and/or storage of explosives, fireworks and other pyrotechnic articles, are also prominent sources of chemical accident risk. The high use of dangerous substances, such as cyanide and arsenic, in metals processing also has elevated the mining industry into the high risk category.

**Figure 41.** Distribution of the ~10,000 Seveso Directive sites (high hazard fixed facilities) in the European Union as reported by countries in 2014. In addition, numerous other industries that are not part of these hazardous chemicals industries also can be sources of chemical accident risk.



Source: EC-JRC eSPIRS database, 2018.

### 18.2 Prevention and mitigation of chemical releases

The bow tie diagramme is commonly used for illustrating the dynamics of a chemical accident and for focusing attention on prevention and mitigation opportunities. As noted in **Figure 42**, the Loss of Containment is the point that distinguishes between measures that are prevention (measures implemented before the loss of containment) and measures that are part of mitigation (measures taken after the loss of

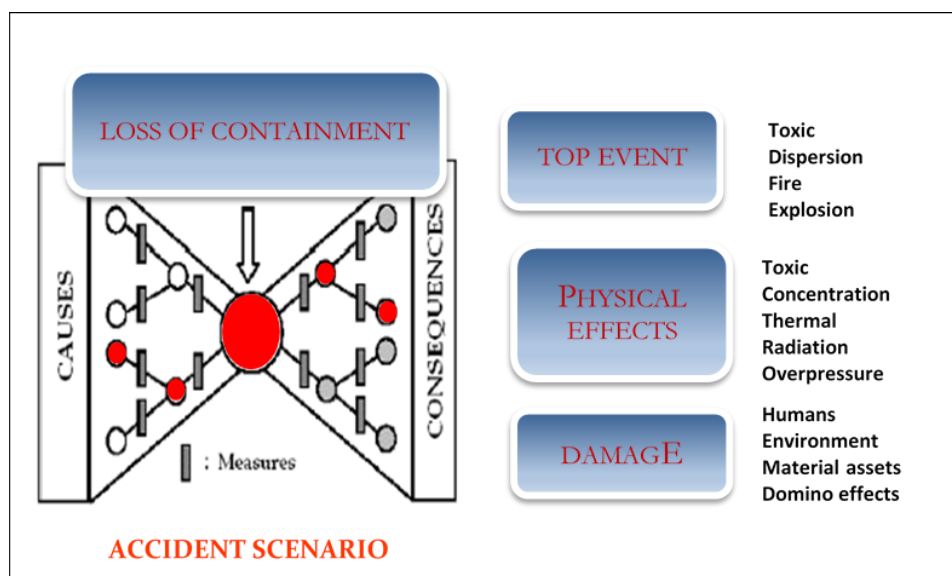
<sup>143</sup> In this section, we will refer to chemical accident risk for the sake of simplicity, but the principles can equally applied to analysis and management of chemical incidents from intentional acts (e.g., sabotage, terrorism). While the causality may require different prevention and mitigation solutions, the potential consequences (fire, explosion or toxic release) are the same and the analysis of the scenario to make decisions about how to prevent, control or respond to it, is the same.

containment). That is, once the substance has escaped from its pipe or vessel, prevention measures have failed and mitigation measures must be launched to keep the event from turning into a dangerous phenomenon, that is, a fire, explosion or toxic release.

The main factors that directly contribute to chemical accident risk are usually defined as

- The dangerous substance(s) involved (flammable, toxic, or explosive and any combination thereof).
- Process and equipment, that is, their properties and conditions (e.g., pressure, temperature, reactions involved, pipes and vessel, safety controls, equipment age and mechanical condition, etc.).
- Safety management systems, including operations, hazard assessment, maintenance, inspections, resource planning, personnel selection and training, performance monitoring, and emergency preparedness
- The dangerous phenomena produced (fire, explosion, toxic release) as a result of substances, involved, process, equipment and various site conditions.

**Figure 42.** Box tie illustration of chemical accident sequence of events.



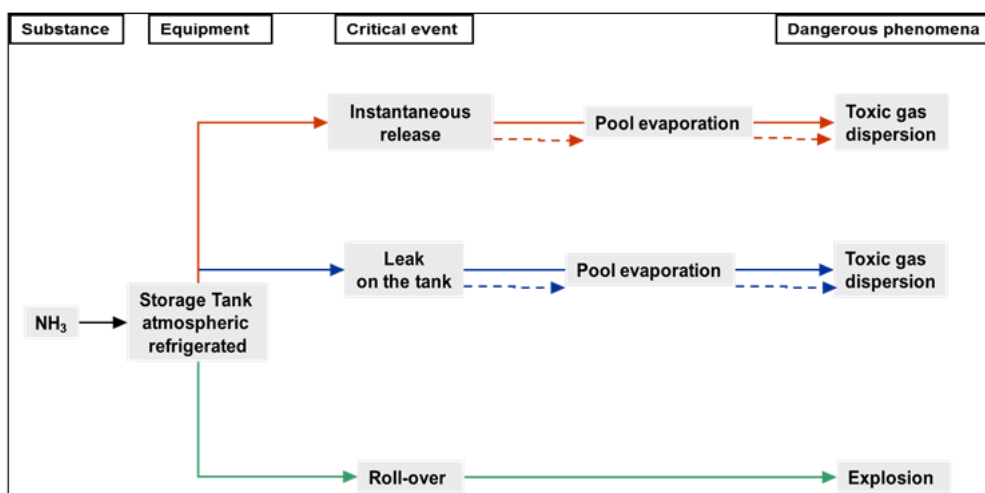
Source: Author

To illustrate, **Figure 43** shows a typical scenario associated with the storage of anhydrous ammonia from Gyenes et al., 2017<sup>144</sup>. The “critical event” column indicates that three different types of loss of containment that can occur in connection with this process. They are 1) an instantaneous release (rupture of the tank, e.g. from an external shock, or excess of pressure or temperature), 2) a leak on the tank, and 3) roll-over (rapid release of vapours caused by stratification of the liquid into different layers of density). Using this scenario, an operator will implement a number of risk management measures, to prevent and mitigate a potential release, and to control any dangerous phenomenon that may result. A first set of measures, typically embedded in equipment design, maintenance routines, and operating practices, will be intended to prevent the loss of containment. These are measures represented on the left-hand side of the bow tie. In the event that these measures fail, and a rupture, leak or roll-over event occur, measures would be in place to detect that a release has occurred, e.g., ammonia sensors, maintenance and inspection practices, at which point some automated mitigation measures, such as pressure relief valves and ventilation systems may be activated. These measures are on the right-hand side of the bow tie. Trained emergency responders may initiate further actions to prevent the release from turning into a major emergency, and precautionary measures, such as site evacuation, may be launched. At the very far right end of the bow tie, that is, the very last element of preparedness in the potential sequence of events, are emergency response measures to combat the toxic

<sup>144</sup> Gyenes, Z., M. Wood and M. Struckl. 2017. Handbook of Scenarios for Assessing Major Chemical Accident Risks. European Commission Joint Research Centre. EUR 28518 EN <https://minerva.jrc.ec.europa.eu/en/shorturl/minerva/publications>

release, contain secondary impacts from any explosion, and to limit damages to workers, the community and the environment.

**Figure 43.** Scenarios for anhydrous ammonia atmospheric pressure refrigerated storage tank.



Source: Gyenes et al., 2017

Controlling and eliminating all causes of chemical accidents is theoretically possible but logistically difficult. Such control requires perfect understanding of process and equipment conditions at any point in time and how process substances will behave under these conditions. It also means controlling all the decisions that govern any particular process and ensuring that they too are perfect at all times. Given this reality, most experts are skeptical that chemical accident risks can be reduced sufficiently such that they are no longer a concern for society. Therefore, mitigation of chemical accident risks to reduce impacts as well as land-use planning and emergency response are equally important elements of risk management strategy.

### 18.3 Principles of effective risk assessment and management

The likelihood of an accident occurring depends significantly on how well the risks are managed (the safety management system) and by decisions of the organisation(s) that affect the functional effectiveness of the safety management system. (These causal factors are usually referred to as “underlying causes”.) In current times, there is considerable agreement on the fundamental principles of process safety management which, if understood and properly applied, would prevent a large majority of chemical accidents that still occur today.

Risk assessment for chemical accident risk follows a similar simple structure that is generally applicable to all technological risks. This structure is composed of three simple questions, often called the risk triplet:

- What can go wrong?
- How likely is it that it will happen?
- If it does happen, what are the consequences?

### 18.4 Performing a risk assessment

The scope of this section is to describe different decision pathways bridging the risk analysis to land-use and emergency planning for chemical accident risk. Criteria for decisions may vary depending on the national context, but generally depend on various social and economic conditions, cultural attitudes towards industrial risk and historical events that may have shaped these attitudes.

The core of risk assessment is the consequence analysis, that is, the fire, explosion or toxic release that could result from an unplanned release of a dangerous substance. The core of the consequence analysis is the accident scenario (or scenarios), that is, the specific sequence of events that could lead to a major fire, explosion or toxic release.

All approaches require a consequence analysis. The consequence analysis has numerous and very specific data requirements. Typical inputs include data on substance properties (boiling point, vapour pressure, etc.), the source term (how the substance was released, e.g., whether a leak or a rupture, how big was the size of the hole, etc.), process conditions (pressure, temperature, etc.), the surrounding environment (outside temperature, open space versus a building, etc.), human health thresholds in relation to certain impact thresholds (toxicity, thermal and explosive effects), population in the surrounding area, and other data of specific relevance to the accident scenario selected. With the exception of substance properties, the data cannot be generalized but must be based on actual conditions at the site in question. The Seveso Directive requires operators of upper tier sites (highest hazard sites) to produce risk estimates in the safety report. The site operators are generally responsible for providing risk estimates but regulators may run their own calculations using the data provided by the site.

### **Risk managers have several options in terms of risk assessment methodology.**

The options for risk assessment approaches are divided into two categories and then divided further into two subcategories. The main difference between the two categories is whether or not numeric frequencies of accident events are taken into account. The categories and subcategories are as follows:

#### **Probabilistic approaches**

- Quantitative approach producing a numeric risk estimate
- Semi-quantitative approach producing a numeric risk estimate

#### **Deterministic approaches**

- Deterministic approach that estimates spatial distribution and severity of effects and implicitly takes account of frequencies
- Distance approach that uses table of fixed distances based on generalized estimates of the results of the deterministic approach

The decision to choose a particular method depends on national attitudes to chemical risk. Years of experiencing in implementing the Seveso Directive in the European Union has proved that the decision on risk assessment of chemical accidents is closely identified with the country's culture, history, and economic, and social conditions. In addition, the decision to use a probabilistic approach may require a consideration as to whether adequate data on frequency for certain types of chemical processes are readily available. For example, it may be important to know how many times a pressure relief valve did not function as expected under certain process conditions. If these data are not available, it may be necessary to choose a deterministic approach.

The probabilistic approach (sometimes called the quantitative approach) is characterized by a final decision based on a numerical risk figure, that is, an estimate of the probability of an event, e.g.,  $1 \times 10^{-5}$ . The numeric estimate of frequency is combined with a numeric estimate of severity to produce a risk figure. It is very important to understand that this risk estimate represents a relative risk, rather than an absolute risk. Data inputs to produce this figure are usually generalized from datasets that are not necessarily representative of the universe of possibilities. Therefore, these inputs carry with them a high degree of uncertainty. The resulting estimates of probability are characterized by uncertainty as well. Based on these results, risks are classified in terms of ranges of probability, with the probability estimates considered as indicative rather than absolute measures.

In contrast, the deterministic approach does not select scenarios on the basis of a numeric likelihood, nor does it produce a numeric estimate of risk. The selection of data inputs (e.g., the volume of hazardous substance released, threshold of harmful effects, etc.) are selected on the assumption that they represent higher frequency events. The output is generally framed in terms of the distribution of certain effects across a certain area, usually divided into spatial zones within a certain distance from the source relative to higher likelihood of death or level of injury. The fixed distance approach simply calculates a fixed distance on the basis of scenarios involving specific substances based on calculations of these spatial zones.

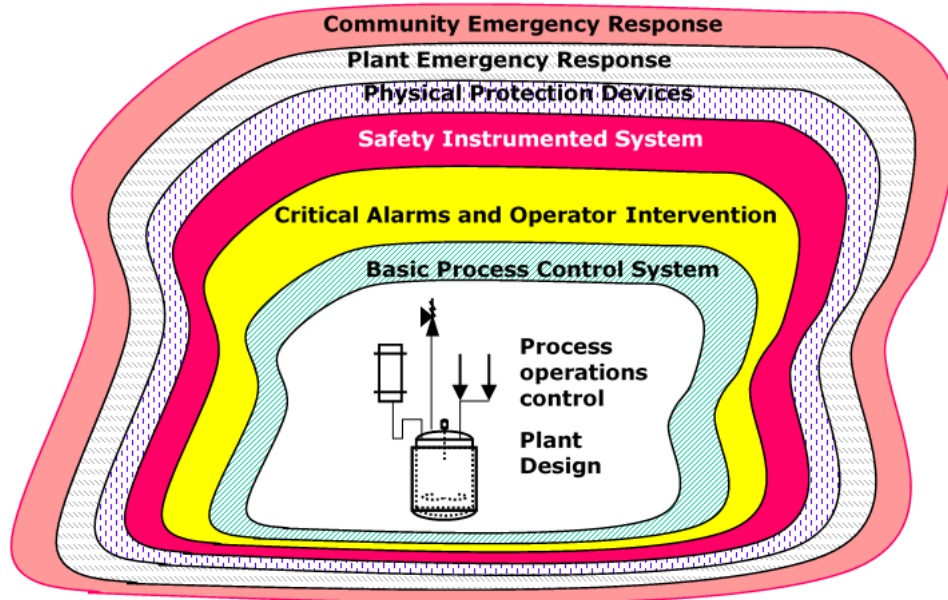
## **18.5 Selecting accident scenarios for the risk assessment**

The selection of accident scenarios follows the risk triplet, by first identifying what can go wrong and then subsequently determining how likely it is to happen and how serious the impacts will be.

### 18.5.1 Hazard identification (what can go wrong)

The consequence analysis relies on the selection of an accident scenario or scenarios. A major hazard site may have one or many accident scenarios, with different likelihood of occurrence or severity. The number of scenarios depends on the complexity of the site. For example, a large petroleum refinery could have 50 or 100 process units and each one of them may have one or more scenarios. On the other end of the spectrum, an LPG storage facility may have only a few scenarios.

**Figure 44.** Layers of Protection Model for a Chemical Plant



Source: CCPS, 2001

The selection of scenarios generally starts with the hazard identification that has been conducted by the operator. There are numerous hazard evaluation methods, of which the most common include, checklists, relative ranking systems (e.g., the Dow Index, the Substance Hazard Index), preliminary hazard analysis, What – If Analysis, What – If & Checklist Analysis, Hazard & Operability Analysis (Hazop), Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis, Event Tree Analysis, Cause – Consequence Analysis, Human Reliability Analysis, and Layer of Protection Analysis (LOPA) as shown in Figure 44 from CCPS (2001).

These methods each help the operator to make a systematic assessment of potential hazards associated with a particular process involving dangerous substances. The output of the process often relies substantially on expert judgement. Often methods may be used in combination to produce independent outcomes that can then be compared. Some methods, such as Hazop and LOPA, require substantial input from a multidisciplinary team of experts. The operator will ideally choose hazard identification methods that are suited for the processes and substances present on the site.

A hazard identification produces a list of possible undesirable scenarios. From these scenarios, a subset of scenarios will be selected as the subject of the risk assessment.

### 18.5.2 Selecting the accident scenarios (How likely is it that it will happen and if it does happen, what are the consequences?)

The selection of the accident scenario(s) for the risk assessment depends on the risk assessment approach selected.

#### Deterministic approach

The selection of scenarios may be based on a qualitative estimate of the consequences only, which means an expert judgment of the expected damage (severe, medium, low). But the main problem is the definition of the

scenarios before this step. The selection is not based on a numeric evaluation of the risk, but selects incidents judged by experts to be undesirable events. Selection criteria often include one or more of the following:

- An assumption of a release, or loss of containment (LOC) of all the contents of the equipment (vessel or pipe)
- Assumption of a specific type of LOC (e.g., leak from a pipe of 25cm diameter)
- Expectation that preventive measures could avoid the LOC (so that the scenario is no longer considered for the risk assessment)
- Qualitative criteria to accept or exclude certain preventive measures for a scenario (e.g., based on the expected reliability of a measure) For example, automated protections, such as pressure relief valves, are often considered more reliable than prevention measures that rely solely on human intervention

Applying the criteria will generally result on some accident scenarios ranked higher in severity than others and on the basis of this ranking, the operator will select scenarios for the risk assessment.

### Probabilistic approach

This approach requires sufficient data on the likelihood of plant' system failures. The frequency data may refer to the so-called "top event", i. e., the LOC or Loss of Containment, or to the sequence of events leading to the top event, on the left-hand side of the bow tie, or to the performance of any preventive measures (left-hand side) or mitigation measures (right-hand side). Despite the fact that specific data referring to the individual case is always the most favourable option, generic data are widely used in order to avoid extensive research to identify numbers, especially when complete datasets from past events occurring on the site may not be available.

The so-called Dutch "Purple Book"<sup>145</sup>, the FRED database of the HSE<sup>146 147</sup>, the so-called "Taylor-Study"<sup>148</sup>, NS the "AMINAL-Study"<sup>149</sup> are all well-known sources of generic frequency data for chemical accident risk analysis. An example of the values for a pipe leak is shown in **Table 12**. Example of pipe failure frequencies below.

**Table 12.** Example of pipe failure frequencies

	Small leak (effective diameter of 10% of the nominal diameter)	Leak (effective diameter of 22% of the nominal diameter)	Leak (effective diameter of 44% of the nominal diameter) (Large leak)	Full bore rupture
Nominal diameter < 75 mm	$1.18 \cdot 10^{-5}$	$7.93 \cdot 10^{-6}$	$3.3 \cdot 10^{-6}$	$1.22 \cdot 10^{-6}$
75 mm ≤ nominal diameter ≤ 150 mm	$2.5 \cdot 10^{-6}$	$1.11 \cdot 10^{-6}$	$4.62 \cdot 10^{-7}$	$3.5 \cdot 10^{-7}$
Nominal diameter > 150 mm	$1.75 \cdot 10^{-6}$	$6.5 \cdot 10^{-7}$	$2.7 \cdot 10^{-7}$	$1.18 \cdot 10^{-7}$

Source: Basta et al., 2008

<sup>145</sup> Committee for the Prevention Disasters (CPR), 1999, "Guideline for Quantitative Risk Assessment-"Purple Book" CPR18E, SDU, The Hague

<sup>146</sup> UK Health and Safety Executive. 1999. Failure rate and event data for use in risk assessment (FRED). Issue 1. Nov 99 (RAS/99/20).

<sup>147</sup> UK Health and Safety Executive. 2003. New failure rates for land use planning QRA Update. Chapter 6K: Failure rate and event data for use within risk assessments. 2/09/2003. RAS/00/22.

<sup>148</sup> Taylor, J. R. 2006. Hazardous Materials Release and Accident Frequencies for Process Plant. Volume II Process Unit Release Frequencies. Version 1 Issue 7. [http://efcog.org/wp-content/uploads/Wgs/Safety%20Working%20Group/\\_Nuclear%20and%20Facility%20Safety%20Subgroup/Documents/Reidat%20II%207.pdf](http://efcog.org/wp-content/uploads/Wgs/Safety%20Working%20Group/_Nuclear%20and%20Facility%20Safety%20Subgroup/Documents/Reidat%20II%207.pdf)

<sup>149</sup> Handboek Kanscijfers voor het opstellen van een Veiligheidsrapport 1/10/2004, AMINAL – Afdeling Algemeen Milieu- en Natuurbeleid.

The second main element of the scenario selection in probabilistic assessment is the application of reliability figures for control measures that may prevent the accident from occurring or reduce its severity. Similar to the deterministic approach, measures may be grouped into the following categories:

- “Avoid Measures”: the scenario will not occur (example: burying a vessel will prevent a BLEVE)
- “Prevention Measures”: the frequency of a scenario is reduced (example: automated systems to prevent overfilling)
- “Control Measures”: the size, severity or extent of the scenario is reduced (example: gas detectors operating block valves)
- “Mitigate Measures”: the size, severity or extent of the effects is reduced (example: firewalls) The necessary steps at this stage are

It is up to the individual user or the national system to determine which types of measures are taken into account and what and how the efficiency is assessed. Some approaches may only consider passive measures (no human intervention or measurement of parameters necessary).

The third part of the quantitative selection of accident scenarios is the definition of “cut – off”. The cut-off is a set of numerical values that are fixed and indicate the threshold of selection, that is, which scenarios have likelihood that is too low for the risk assessment.

## 18.6 Evaluating the consequence analysis

The outcome of the risk assessment, regardless of approach is an estimate of the risk in terms of likelihood and severity. The likelihood measure may be expressed either numerically, e. g., yearly occurrence of an undesirable event in the range of  $10^{-3}$  –  $10^{-9}$ , or qualitatively (e. g. very likely to very unlikely). The severity may be expressed quantitatively by numerical effect (e.g., how many deaths), or qualitatively from “low” to “high”.

### 18.6.1 Evaluating impacts and severity

Dangerous phenomena produced by a chemical accident scenario

The risk assessment will identify phenomena that can be produced from the accident scenario. The main types of potential dangerous phenomena that may be generated by a chemical accident are shown in **Table 13**. The consequence analysis will identify which phenomena are produced by the accident scenario.

**Table 13.** Effects related to different kind of scenarios

Dangerous phenomenon	Scenario types		
	Thermal Radiation	Overpressure	Toxic Effects
Fireball	x	x	
Flashfire	x		
Jetfire	x		
Poolfire	x		
VCE	x	x	
Toxic Clouds			x
Solids Fire	x		

Source: Basta et al., 2008



### 18.6.2 Human health effect evaluation

The risk assessment will identify potential human health effects from dangerous phenomenon, mainly a fire (thermal radiation), explosion (overpressure) or toxic release. **Table 14** below is an example of severity classifications for human health effects.

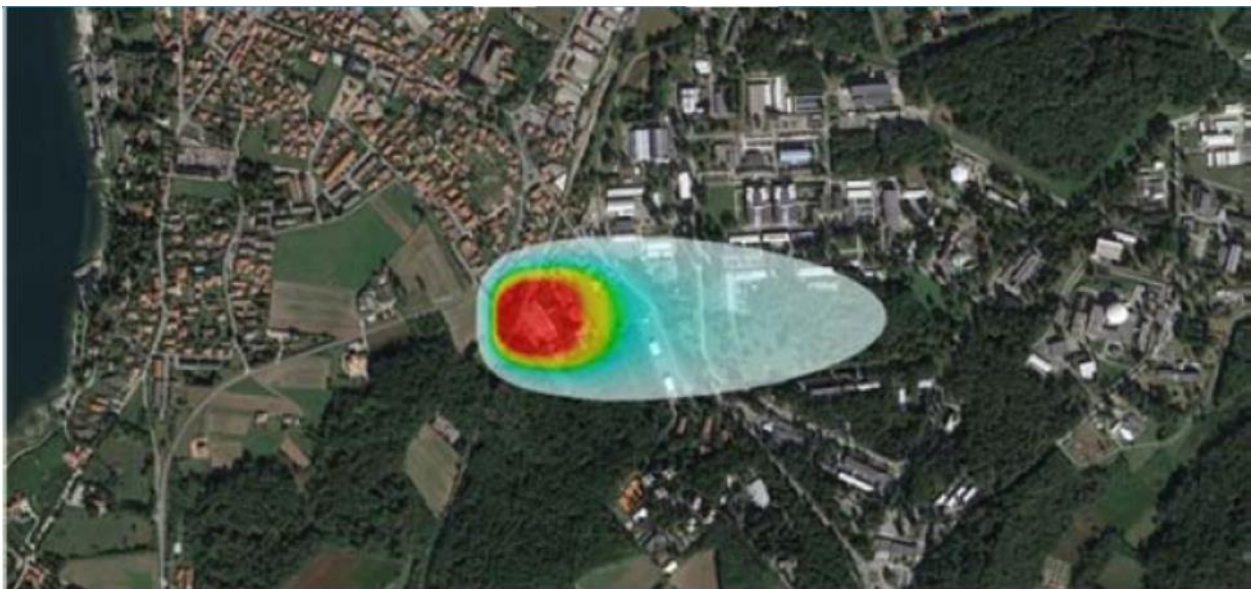
**Table 14.** Consequence classification for human and environmental impacts

Consequence Classification	
Effects on human health	Effects on the environment
No injury or slight injuries without sick leave	No action needed but surveillance
Injuries leading to an hospitalization	Serious effects on the environment inside the establishment
Irreversible injuries or death inside the establishment, reversible injuries outside the establishment	Reversible effects on the environment outside the establishment
Irreversible injuries or death outside the establishment	Irreversible effects on the environment outside the establishment

Source: JRC, 2018

The severity level is determined by reviewing the expected intensity of the impact (heat, overpressure, lethality and concentration of the toxic substance) and the spatial area over which each level of intensity is sustained. Impacts of consequences are usually expressed in terms of spatial distribution and number of people affected, often displayed as a map as in **Figure 45**.

**Figure 45.** Toxic dispersion from a catastrophic rupture of a tank wagon containing sulphur dioxide



Source: JRC, 2018

### Physical effects of fire and explosions

The definition of physical hazards is comparatively easy. The divergence of accepted thresholds is not wide and the main difference lies in the decision which levels of effects should be taken into account. For thermal radiation and overpressure the values in **Table 15** and **Table 16** may serve as default figures.

**Table 15.** Endpoints values of fires and explosions for different severity levels

Level	Stationary Radiation	Non – stationary Radiation	Overpressure
No effect	1,6 kW/m <sup>2</sup>		
Small effects	< 3 – < 5 kW/m <sup>2</sup>	< 125 kJ/m <sup>2</sup>	< 30 mbar
Reversible effects	< 3 – < 5 kW/m <sup>2</sup>	125 – < 200 kJ/m <sup>2</sup>	30 - < 50 mbar
Irreversible effects	5 – 7 kW/m <sup>2</sup>	200 - 350 kJ/m <sup>2</sup>	50 – 140 mbar
Lethality	> 7 kW/m <sup>2</sup>	> 350 kJ/m <sup>2</sup>	> 140 mbar

Source: Basta et al., 2008

Another distinction concerns the duration of the effect, as shown in **Table 16**:

**Table 16.** Stationary, non-stationary and fixed effects

Dangerous phenomenon	Effect type		
	Stationary Radiation	Non – stationary radiation	Overpressure (fixed value)
Fireball		x	x
Flashfire		x	
Jetfire	x		
Poolfire	x		
VCE		x	x
Solids Fire	x		

"Non – stationary" means that the effect is calculated on the basis of an equation that takes into account the actual time of exposure which may be very short in the case of certain scenarios.

Source: Basta et al., 2008

### **Toxic effects**

For toxic effects the situation is more complex than for physical hazards, taking into account the following limitations:

- Countries with existing concepts only agree one threshold, which is the level corresponding to the start of the certain effects (for example irreversible health effect).
- There are various exposure guidelines; the selection of one of them based on scientific expertise is difficult (finding evidence of the effects of a given toxic substance in humans is often unmanageable, so the experimentation is usually done in animals and the values obtained extrapolated to humans).
- Each source guideline (e.g., American Institute of Industrial Hygienists Emergency Response Planning Guidelines – ERPGs) covers only a limited number of substances.
- The effects of toxic substances on humans are in some cases related to the dose and not to a given concentration.

- The dose may depend not only on the concentration value and the exposure time but also on other parameters which depend on the substance and may be unknown.
- The effects on exposed persons is greatly affected by their health condition, age etc, Currently three databases for toxic effects are widely used: IDLH, ERPG and AEGL
- Immediately Dangerous for Life and Health (IDLH) Threshold Levels<sup>150</sup>
- Emergency Response Planning Guidelines (ERPG) Threshold Levels<sup>151</sup>

### 18.6.3 Consequence and risk assessment modelling tools

Given the complex nature of consequence and risk assessment of chemical accidents, various organisations have developed tools. The following tools are the most well-known, but other tools are also available:

- The JRC ADAM (Accident Damage Assessment Model) Tool. The JRC created this versatile application for competent authorities implementing the EU Seveso Directive. It models consequences for a wide range of substances and scenarios and also can incorporate frequency data and produce a risk assessment figure. It is available for free to competent authorities. For more information, go to the website <https://adam.jrc.ec.europa.eu/en/adam/content>
- The ALOHA software tool created by the U.S. Environmental Protection Agency is used widely to plan for and respond to chemical emergencies. ALOHA allows users to enter details about a real or potential chemical release, and then it will generate threat zone estimates for various types of hazards. ALOHA can model toxic gas clouds, flammable gas clouds, BLEVEs (Boiling Liquid Expanding Vapor Explosions), jet fires, pool fires, and vapor cloud explosions. It is available for free at <https://www.epa.gov/cameo/aloha-software>
- EFFECTS is a commercial software developed by TNO and available at cost for safety professionals to calculate and analyse the effects of accident scenarios. More information is available at: <https://www.tno.nl/en/foccus-areas/circular-economy-environment/roadmaps/environment-sustainability/public-safety/effects-advanced-easy-to-use-consequence-analysis/>
- PHAST is DNV's commercial software for modeling releases and dispersions including modelling of pool spreading and evaporation, and flammable and toxic effects. More information is available at: <https://www.dnvgl.com/services/process-hazard-analysis-software-phast-1675>

## 18.7 Presenting the risk assessment outcome for decision-making

The final result of the risk assessment combines the impact analysis with likelihood of the event for each accident scenario. This product gives the necessary information for decision-makers. Some common mechanisms for communicating the results of the risk assessment are as follows:

A risk matrix, representing the compatibility between defined level of risk and urban/environmental development (see Figure 46 below)

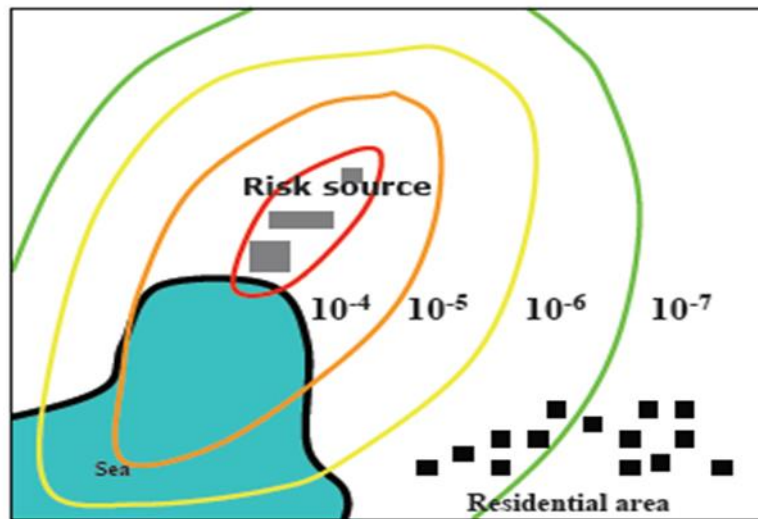
A spatial distribution of the consequences expressed on a geographic map of the area (as in **Figure 45**).

A chart that shows different zones of risk of any individual being harmed by an accident scenario. The individual risk curves are associated with impact areas with different frequency endpoints. The numeric frequencies in **Figure 46** can only be produced through a probabilistic risk assessment. However, similar charts can also be produced from a deterministic risk assessment, with the zones described qualitatively (e.g., likelihood of fatalities or irreversible injury, likelihood of reversible injury, etc.). Such charts may be used to create land-use planning zones or emergency response intervention zones. For example, 10<sup>-6</sup> irreversible damage area where only limited residential developments are allowed. The societal risk graph (F/N-curve), is a single measure of the chance that an accident (or accidents) could harm a number of people. It can only be produced through a probabilistic risk assessment.

<sup>150</sup> National Institute for Occupational Safety and Health, USA. Online: <http://www.cdc.gov/niosh>

<sup>151</sup> Online: <http://www.aiha.org>

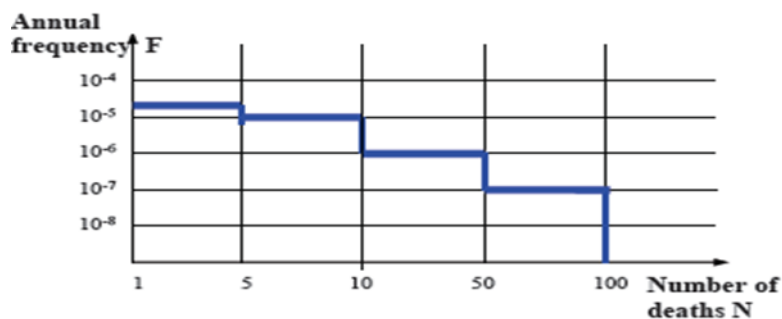
**Figure 46.** Example of an individual risk curve.



Source: Basta et al., 2008

These outputs can be used directly by decision makers to determine whether the site has achieved an acceptable level of risk. The risk assessment of each accident scenario must be within the range of acceptable risk. When probabilistic risk assessment is used, acceptable risk is defined as a numeric risk, e.g.,  $10^{-5}$ , established by the operator, or sometimes by national legislation (**Figure 47**). The F/N curve usually represents the collective risk of the entire range of critical accident scenarios at a site. It can generally only be produced through a probabilistic approach.

**Figure 47.** Example of an F/N diagramme



Source: Basta et al., 2008

These outputs can also be used by governments to create standardised distances. The matrices shown in **Figure 48** and **Table 17** are examples of tools that can be used to evaluate risks for decision-making in this regard.

**Figure 48.** Example of risk matrix

RISK ASSESSMENT MATRIX				
SEVERITY \ PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Source: Department of Defense, 2012

**Table 17.** Example of a risk matrix with quantified likelihood

Frequency/ Likelihood		Single fatality	2-10 fatalities	11-50 fatalities	50-100 fatalities	100+ fatalities
Likely	>10-2/yr	Intolerable	Intolerable	Intolerable	Intolerable	Intolerable
Unlikely	10-4/yr – 10-2/yr	Tolerable (Intolerable if individual risk of fatality >10-3/yr)	Intolerable (Intolerable if individual risk of fatality >10-3/yr)	Intolerable	Intolerable	Intolerable
Very unlikely	10-6/yr – 10-4/yr	Tolerable	Tolerable	Tolerable	Tolerable	Intolerable
Remote	10-8/yr – 10-6/yr	Broadly Acceptable	Broadly Acceptable	Tolerable	Tolerable	Tolerable

Source: Derived from findings presented in HSE (2001) and HSE (2009)

## 18.8 Making decisions based on the risk assessment

The output of any risk assessment provides an indicator of the magnitude of the risk associated with the hazard. Organisations can use this output in numerous ways, depending on their role in the process. Operators will use the risk assessment to make decisions about strengthening risk management and where to invest resources in a way that reduces risk most effectively. Inspectors may make decisions about whether the site is safe and can continue operations without significant changes. Land-use planners will use the outputs to make rules about where certain uses can be developed, and also to impose restrictions on certain development when necessary. Emergency planners will use the information to determine the types of equipment, knowledge, and training that emergency personnel will require. They may make decisions about

when and how to evacuate certain populations, setting up medical services around the site, and other intervention components.

The outputs of risk assessment of chemical incidents have a high degree of uncertainty that can make them difficult to communicate to politicians and the public. They are complicated to explain and the fact that they are not entirely certain, may undermine their importance. In the case of numeric estimates, there can be tendency to underestimate the need to prevent and prepare for low frequency high severity events. On the other hand, the public may see these numbers as frightening. Nonetheless, the advantage of having more knowledge about chemical accident risk far exceeds some of the challenges it creates.

## 18.9 References

<https://minerva.jrc.ec.europa.eu/en/shorturl/minerva/publications>

Basta, C., M. Christou and M. Struckl. 2008. Overview of Roadmaps for Land-Use Planning in Selected Member States. European Commission Joint Research Centre. EUR 23519 EN.

Center for Chemical Process Safety. 2001. Layer of protection Analysis – Simplified Process Risk Assessment. ISBN 0-8169-0811-7

Christou, M. D., M. Struckl and T. Biermann. 2006. Land-use planning guidelines in the context of Article 12 of the Seveso II Directive 96/82/EC as amended by Directive 105/2003/EC. European Commission Joint Research Centre. EUR 22634 EN

Department of Defense (United States of America). 2012. MIL-STD-882E. Standard Practice. System Safety.

Gyenes, Z., M. Wood and M. Struckl. 2017. Handbook of Scenarios for Assessing Major Chemical Accident Risks. European Commission Joint Research Centre. EUR 28518 EN

Health and Safety Executive (United Kingdom), 2001. Reducing risks, protecting people. Norwich, United Kingdom. ISBN 0 7176 2151 0

Health and Safety Executive (United Kingdom), 2009. Safety and environmental standards for fuel storage sites. Process Safety Leadership Group. Final report. Published in the United Kingdom. ISBN 978 0 7176 6386 6

## 19 Nuclear accidents

MIGUEL ANGEL HERNANDEZ CEBALLOS, CRISTINA TRUEBA ALONSO, MILAGROS MONTERO PRIETO, GIORGIA IURLARO, MARCO SANGIORGI, BLANCA GARCÍA PUERTA,

The objective of this contribution is to present the steps to follow in order to carry an analysis of a single hazard (nuclear accident), stressing the limitations of the methods and the opportunities to link them with other hazards. Focus is made on the methodologies and tools existing to assess the hazards, exposure and vulnerability to ionising radiation, pointing out the requirements of data and expertise, the assumptions made and the limitations of the results.

### 19.1 Context

It is generally recognized the dichotomy between the advantages and disadvantages provided by facilities and activities dealing with ionising radiation. Among the benefits, they range from power generation to medicine, industry and agriculture uses. In addition, nuclear power can make an important contribution to the problems of climate change, and play a key role in the transition to a clean energy future (IAEA, 2018; NEA, 1998), as a dispatchable low carbon source of electricity. On the contrary, the radiation risks to workers, public and environment that may arise from a potential accident generate its rejection.

The radioactive material once released, dispersed and deposited on different environments, causes a situation of exposure to the population through different pathways that can lead to doses and health risks. It creates that ionising radiation have to assessed and, if necessary, controlled. The EU has radiation protection legislation in place to protect human health against the dangers arising from ionising radiation. This includes the Basic Safety Standards (Council Directive 2013/59/EURATOM), which is supplemented by a number of acts ensuring a high level of protection for the public, workers, and patients. In addition, the EU requires member states to monitor radioactivity in the air, water, soil and foodstuffs. A full text of all EU-level provisions currently valid in radiation protection can be consulted in the following link<sup>152</sup>.

### 19.2 Risk identification

A nuclear accident is when the accident occurs in a nuclear power plant or in any other establishment using nuclear technology. In safety analyses and the IAEA safety standards, the term 'accident' has been used much more generally to mean "Any unintended event, including operating errors, equipment failures or other mishaps, the consequences or potential consequences of which are not negligible from the point of view of protection or safety" (EC/FAO/IAEA, 2014). Specifically, in the context of the reporting and analysis of events, it is the event that has led to significant consequences to people, the environment or the facility (IAEA, 2009). In this last context, the International Nuclear and Radiological Event Scale (INES) (IAEA, 2009) facilitates consistent communication on the safety significance of nuclear and radiological events. Based on a numerical rating, from one to seven, the scale rates events into incidents (levels 1-3) or accidents (levels 4-7), while events without safety significance are rated as level 0.

Events are considered in terms of their impact on three different areas:

1. **People and the Environment:** It considers the radiation doses to people close to the location of the event and the widespread, and unplanned release of radioactive material from an installation;
2. **Radiological Barriers and Control:** It covers events without any direct impact on people or the environment and only applies inside major facilities. It covers unplanned high radiation levels and spread of significant quantities of radioactive materials confined within the installation;
3. **Defence-in-Depth:** It also covers events without any direct impact on people or the environment, but for which the range of measures put in place to prevent accidents did not function as intended.

The event is rating against each impact area and the highest level is selected as the actual rating of the event.

As an example of the INES scale application, nuclear power plant (NPPs) accidents at Chernobyl and Fukushima Daiichi were rated 7 due the highest impact on the People and the Environment area. On the contrary, the event in the Three Mile Island NPP was categorized as level 5 attending the maximum impact on the Radiological Barriers and Control area. Successfully response arrangement has often turned out to be a

---

<sup>152</sup> <https://ec.europa.eu/energy/en/overview-eu-radiation-protection-legislation>

major challenge – if not impossible – where no prior risk assessment and proper preparedness planning had taken place. The main target of nuclear risk assessment is to improve safety and minimize risks related to nuclear energy. Risk assessment denotes the total process, and the results, of assessing the radiation risks and other risks associated with normal operation and possible accidents involving facilities and activities, from which a release of radioactive material occurs or is likely to occur (IAEA, 2016). This process normally includes consequence assessment, together with some assessment of the probability of those consequences arising.

#### **Box 11: The NERIS platform**

The NERIS platform (European Platform on Preparedness for Nuclear and Radiological Emergency Response and Recovery)<sup>153</sup>, was established in 2010, to be a forum where joint European arrangements for nuclear and radiological emergencies can be developed and improved. The Platform addresses all notable trends, arrangements and capabilities in the area of response to and recovery from nuclear and radiological emergencies. The activities supported and developed under the umbrella of the NERIS platform include training courses, workshops, working groups and user groups of J-RODOS. NERIS is also linked to research projects under the European Research Programmes, such as NERIS-TP (Towards a self-sustaining European technology platform (NERIS-TP) on preparedness for nuclear and radiological emergency response and recovery, 2011-2014), PREPARE (Innovative integrative tools and platforms to be prepared for radiological emergencies and post-accident response in Europe, 2013-2016), OPERRA-project CATHyMara (Child and Adult Thyroid Monitoring after Reactor Accident, 2015-2017), OPERRA-project HARMONE (Harmonising Modelling Strategies of European Decision Support Systems for Nuclear Emergencies, 2015-2017), OPERRA-project SHAMISEN (Nuclear energy situations – Improvement of medical health surveillance, 2015-2017), and more recently, the CONCERT-European Joint Programme for the Integration of Radiation Protection Research (2015-2020), structure for the research initiatives jointly launched by the radiation protection research platforms, and their associated projects, as CONFIDENCE (Coping with uncertainties for improved modelling and decision making in nuclear emergencies, 2016-2020), TERRITORIES (To Enhance uncertainties Reduction and stakeholders Involvement TOwards integrated and graded Risk management of humans and wildlife In long-lasting radiological Exposure Situations, 2016-2019), ENGAGE (ENhancinG stAkeholder participation in the GovernancE of radiological risks for improved radiation protection and informed decision-making, 2017-2019) and SHAMISEN-SINGS (Stakeholder INvolvement in Generating Science after Nuclear Emergencies, 2017-2019)<sup>154</sup>. Through these projects, methodological aspects and computational models have been developed to be consistent with recommendations from international bodies such as the ICRP (International Commission for Radiological Protection), and can be coupling to decision support systems, improvements in atmospheric and aquatic modelling, data mining, information gathering and providing information to stakeholders and mass media, stakeholder engagement and dialogue and social media/networking technology studies. For instance, the CONFIDENCE Project (2017-2019) improved decision making for the protection of the population affected by nuclear emergencies and to minimize disruption of normal living conditions. A multidisciplinary approach dealing with all aspects regarding the radiological situation following an accidental release has been followed, from the prognosis of dispersion and its spatial-temporal evolution, to the offsite consequences and the decision making to select, implement and evaluate recovery strategies, including the viewpoints of stakeholders. Their goals have been to understand, reduce and cope with the uncertainty, including social and ethical aspects, in both the threat and early release and transition phase of an accident, engagement of all relevant stakeholders from lay people to decision makers in planning and recovery strategy development and final decision making<sup>155</sup>.

### **19.3 Risk Analysis**

Targets of risk assessment are the people and the ecological systems close to the location of the event, as well as those potentially under the influence of the radioactive material released due to its transport. With this in mind, the final product should be the information to determine appropriate defense-in-depth strategies, to develop policies by decision makers and public information at global, regional and national levels, as well as list of corrective measures that are feasible, rational and in line with environmental, social and economic objectives.

In general, risk assessment is included within the scope of safety assessment, which covers all aspects of facilities and activities that are relevant to protection and safety of technological systems (IAEA, 2016). The evaluation of safety can be addressed by a bottom-up approach, i.e., it starts with postulated failures and proceeds to identify their consequences, or by a top-down approach, i.e. it starts with postulated end states (adverse consequences) and proceeds to identify a set of disturbances to normal operation which can lead to the end state (initiating events) (Apostolakis, 2003). While the Probabilistic Safety Assessment (PSA) follows the bottom-up approach, the Quantitative Risk Assessment (QRA) applies the top-down approach.

<sup>153</sup> <https://www.eu-neris.net/>

<sup>154</sup> <https://www.eu-neris.net/projects/concert.html>

<sup>155</sup> <https://portal.iket.kit.edu/CONFIDENCE/index.php>



The evaluation of the nuclear infrastructure vulnerability against, for example, human errors, terrorist attacks and natural disasters, as well as preparation of emergency response plans is vital to assurance safety nuclear operations and national security (Kostadinov, 2011). The international community has agreed to strengthen the Convention on the Physical Protection of Nuclear Material, and in establishing nuclear security guidance (IAEA, 2011). In this line, to prevent any risk growth beyond acceptable levels, the climate change effects must be also accounted for into risk assessment (Vagnoli, 2017). The majority of nuclear facilities commenced operation between thirty and forty-eight years ago, before climate change was considered in plant design or construction, and hence, the impact of, for instance, intensifying storms, droughts, extreme precipitation, wildfires, higher temperatures, and sea-level rise, should be considered and analysed on already existing and/or the design of planned nuclear facilities (Jordaan et al., 2019).

The role and importance of PSA as a technique to numerically quantify risk measures in NPP is defined and emphasised in many national and international safety standards (e.g., IAEA, 2010a, 2010b, 2012). PSA is a comprehensive and structured approach to identifying failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk (IAEA, 2016). PSA makes possible to examine a complex system's potential risk and to study the new design features and evaluate which of the safety improvements brings the required safety upgrading in NPP. Therefore, PSA provides insights into the strengths and weaknesses of the design and operation of a NPP. In all European countries, PSA methodology is used to confirm and enhance the safety of NPPs in complement to the deterministic approach. As an example of this use, the Nordic project "The Validity of Safety Goals" (2006-2010) (Bengtsson et al., 2011) had the aim to provide a general description of the issue of probabilistic safety goals for NPPs, of important concepts related to the definition and application of safety goals in Finland and Sweden.

PSA estimates the final measure of risk by combining the consequences with their respective frequencies. To this purpose, NPP's PSAs deal with "internal events" – those that start inside the power plant or the electric system it serves – and "external events" such as earthquakes, tsunamis, floods, hurricanes, fires and malicious events. The technique in this kind of probabilistic studies is to work with many hypothetical events covering a large range of possible outcomes. This allows assessing the probabilities and severity of loss. PSA combines estimations of three levels of risk<sup>156</sup>:

- Level 1 PSA estimates the frequency of accidents that causes damage to the nuclear reactor core, commonly called core damage frequency (CDF). This Level models from the various plant responses, called "accident sequences", to an "initiating event" that challenge the plant operation. Therefore, this level models all of a reactor's protective and accident mitigation systems.

#### **Box 12: The ASAMPSA\_E project**

The ASAMPSA\_E project (2013-2016)<sup>157</sup>, aims at promoting good practices for the identification of initiating events (e.g. earthquakes, tsunamis, etc) and external hazards with the help of PSAs and for the definition of appropriate criteria for decision-making in the European context. The project gathered experts from 28 organisations in 18 European countries and tried to cover the consequences associated with extreme external events, in particular flooding, that went beyond what those considered in the initial NPP design.

- Level 2 PSA, which starts with the Level 1 core damage accidents, estimates the frequency of accidents that release radioactivity from the nuclear power plant. Such core damage sequences are typically referred to as severe accidents. This Level analyses the progression of an accident by considering how the containment structures and systems respond to it. Once the containment response is characterized (timing and location parameters, thermal energy release rate and quantities of radionuclides releases), the analyst can determine the amount and type of radioactivity released from the containment.

#### **Box 13: SOURCE TERM**

SOURCE TERM is an international research programme carried out by IRSN (L'Institut de Radioprotection et de Sûreté Nucléaire) and CEA (Commissariat à l'Energie Atomique). This programme sets out to reduce uncertainties when evaluating the environmental release of radioactive products such as iodine or ruthenium following a core meltdown accident in a pressurised water reactor (PWR). The experimental data gained from this programme are used to develop and validate numerical simulation tools needed to assess the consequences of such an accident and to evaluate the efficiency of the prevention means.

<sup>156</sup> <https://www.nrc.gov>

<sup>157</sup> <http://asampsa.eu/context/>

- Level 3 PSA, which starts with the Level 2 radioactivity release accidents, estimates the consequences that might result in terms of health effects resulting from the radiation doses to the population around the plant such as short-term injuries or long-term cancers and economic losses that may result when radioactive material reaches the environment. Consequences are estimated based on the characteristics of the radioactivity release calculated previously, conditioned by several factors such as the dispersion of the plume, the deposition pattern, the land contamination and land use, the exposure of population and the early countermeasures applied.

Therefore, only the Level 3 PSA estimates the health and economic impact in terms of different offsite consequence measures. U.S. NRC 2013 provides guidance to develop a technical analysis approach plan for Level 3 PSA to be used in performing the full-scope site Level 3 PSA. However, integrated assessments of the risk emanating from the operation of facilities from which a release of radioactive material occurs (e.g. NPPs) is scarce, and there is not a state-of-the-art guidance material to address this Level 3 PSA. Performance of the full-scope site Level 3 PSA study involves an extensive number of technical tasks, and, consequently, the need to obtain or develop numerous models and substantial data. The level of effort to accomplish this work is a function of the amount of information and models. In general, it is required careful selection of suitable models for description of natural phenomena and effects of pollution exposure.

## 19.4 Risk Evaluation

Two examples of approaches to the Level 3 PSA are the flexRisk (Arnold et al., 2012; Seibert et al., 2013) and the ANURE project (ANURE, 2017)). Both activities are performed with the purpose of estimating the contamination risk from the atmospheric dispersion of radionuclides released by NPPs accidents. The common characteristic of this kind of analysis is the consideration of many events to cover a large range of possible outcomes, and to assess the probabilities and to create a distribution of exceedance probability.

The flexRISK project studies the geographical distribution of the risk due to severe accidents in nuclear facilities, especially NPP in Europe. Starting with source terms and accident frequencies, the large-scale dispersion of radionuclides in the atmosphere were simulated for about 2800 meteorological situations (ten years period). The transport and dispersion model FLEXPART simulated the dispersion in the atmosphere and produce the contamination patterns of the ground and near-surface concentrations of relevant radionuclides. Radiation doses derived from the dispersion calculation are calculated to assess the consequences of severe accidents. Maps and diagrams indicate, e.g., where in Europe the risk to be affected by a severe accident is especially high, or which contribution is incurred by the NPPs of a specific country.

The ANURE project aims at developing a methodology to elaborate nuclear risk maps, considering local factors, to be used by decision-makers in the preparedness and management of a nuclear post-accident exposure situation. The Almaraz NPP in Spain is taken as reference in this feasibility study. The methodology and the ANURE's results are based on 1825 numerical dispersion calculations from 5 consecutive years (2012-2016) using the Lagrangian mesoscale atmospheric dispersion model RIMPUFF, which is implemented in the JRODOS Decision Support System. For this period, the dispersion of two different source terms has been simulated, 1) severe accident with relative large release and 2) severe accident with small release. The outputs of each dispersion calculation, among others, consist of ground contamination on an irregular geographical grid. This information is useful to establish the affected area and the probability of exceedance of thresholds of contamination. This deposit probability combined with detailed information of soil vulnerability and the food chain impact provides an estimation of the risk distribution associated with both kinds of nuclear releases.

The global climate change is an element to consider in the analysis of this results and its medium and long-term application. The possibility to increase the occurrence of extreme climate and weather events (Schar et al., 2004), could have impact on atmospheric circulation and regional wind patterns, which can lead large changes in net precipitation. Beniston et al., 2007, for instance, found that intensity and frequency of heat waves will increase in Europe, and extreme wind speeds will increase between 45N and 55N by the end of 2100. Changes in wind and precipitation patterns influence the transport, dispersion and deposition patterns of the radioactive material, and hence, the risk evaluation results. This fact suggests that it is important to understand how atmospheric phenomenon will change in the future if we are ever to accurately predict how winds and precipitation in different regions will respond to climate change (Yan 2016).

## 19.5 Risk Treatment

Here, and as case study, it is explained the elaboration of a risk map for rainfed cereals and  $^{137}\text{Cs}$  deposit based on offsite radionuclide release from the Almaraz NPP. Rainfed cereals is one of the most widely produced crops in Spain, and therefore, it has large health, social and economic impact. The methodology applied to achieve this purpose is the one suggested under the ANURE project (ANURE, 2017) which is deeply developed in García Puerta, 2020. The methodology combines the predicted deposition patterns of the release obtained from a large amount of numerical dispersion simulations (deposition map) with the knowledge of factors that influence the behavior of radionuclides in soils and its transfer to food chain (vulnerability map).

Following the general recommendation for this kind of analysis of working with many hypothetical meteorological scenarios, the base of this case study is the  $^{137}\text{Cs}$  ground contamination predicted on a geographical grid spacing by 1383 numerical dispersion calculations (2012–2016 period) for 35 hours of offsite radionuclide release. The simulations were carried out by the Lagrangian mesoscale atmospheric dispersion puff model RIMPUFF of JRODOS System (in the below box is explained the needed steps to carry out a JRodos emergency model chain simulation).

Once performed the set of simulations, the predicted values in each grid cell were grouped into six contamination levels taken as reference the contamination levels predefined in the Nordic Guidelines and Recommendations (NGR, 2014), according to the activity concentration deposited on the ground. The probability of occurrence of each category in each cell is obtained and they are weighted by their corresponding factor. The contamination levels and the weight factor associated are shown in **Table 18**. The results of each weighted contamination level are added in each output grid cell. The 8056 resulting values (one per cell) are used to calculate the percentiles  $P_{25}$ ,  $P_{50}$ ,  $P_{75}$  and  $P_{95}$  which are used as the thresholds of the named "Deposition Index". This index is, hence, distributed in five classes ranging from 1, representing the minimum probability of having a high activity concentration deposition (less than  $P_{25}$ , to 5, which represents the maximum weighted probability (more than  $P_{95}$ ). The Deposition Index is assigned to each cell of the calculation grid by using a GIS to obtain the deposition map which, in this case study, is limited to the Iberian Peninsula. The spatial variability of this index identifies those areas largely and continuously affected by high depositions of  $^{137}\text{Cs}$  among the 1383 deposition simulations.

**Table 18.** Contamination levels modified from NGR, 2014, referred to the activity concentration deposited on the ground for gamma and beta emitters. Contribution of the  $^{137}\text{Cs}$  to the total activity concentration and Deposition weighting factor corresponding to each level.

Contamination level	Activity concentration deposited (kBq m <sup>-2</sup> )	$^{137}\text{Cs}$ Activity concentration deposited (kBq m <sup>-2</sup> )	Deposition Weighting Factor
No affected area*	0	0	1
Non-contaminated	<10*	0.01	1·10 <sup>1</sup>
Slightly contaminated	10-100*	0.01-0.1	1·10 <sup>2</sup>
Contaminated	100-1000	0.1-1.0	1·10 <sup>3</sup>
Heavily contaminated	1000-10000	1.0-10.0	1·10 <sup>4</sup>
Extremely contaminated	>10000	>10.0	1·10 <sup>5</sup>

\*NGR, 2014 define the lower contaminated category as "Non-contaminated" for activity concentration levels under 100 kBq m<sup>-2</sup>. A 10 kBq m<sup>-2</sup> threshold has been included, as well as another contamination level: "No affected area", to distinguish those cases where there is no deposition at all, from the cases affected with the considered lower activity concentration.  
Source: NGR, 2014

Having the deposition map, the radiological vulnerability map, is obtained. It represents the capacity of the soil-plant system to transfer the  $^{137}\text{Cs}$  contamination from the soil to the cereal crops. The factors taken into account are empirical values of the soil properties and the soil type distribution, the land use, and the soil-to-plant transfer factors.

The potassium and the clay contents are used to create the Caesium Bioavailability Index (see **Table 19**). Both parameters are key in the radiocaesium transfer from soil to plant, since they reflect the nutrient holding capacity of the soil. Therefore, this index reflects the potential capacity of the soil to store the  $^{137}\text{Cs}$ , which may become bioavailable for crops over time and, therefore, contaminate the foodstuff.

**Table 19.** Caesium Bioavailability Index ( $I_{Cs}$ ) definition, considering clay and K soil content.

Bioavailable K content in Soil (cmol Kg <sup>-1</sup> ) depending on clay content				Caesium Bioavailability Index
Clay 0-10 %	Clay >10-20 %	Clay >20-30 %	Clay >30 %	$I_{Cs}$
>0,5	>0,8	>0,9	>1	1
>0,4-0,5	>0,6-0,8	>0,7-0,9	>0,9-1	2
>0,2-0,4	>0,5-0,6	>0,6-0,7	>0,7-0,9	3
>0,1-0,2	>0,3-0,5	>0,4-0,6	>0,5-0,7	4
<=0,1	<=0,3	<=0,4	<=0,5	5

Source: Domínguez Vivancos, 1997

The parameters assumed to represent the transfer of <sup>137</sup>Cs from soil to plant are the transfer factors compiled in IAEA, 2010 for this crop. A tree-category Transfer Factor Index, ranged from 1 to 3, shows that transfer for the corresponding topsoil texture, as it can be seen in **Table 20**. This index is assigned to the Iberian agricultural systems where rainfed cereals may be grown according to the land use (EEA, 2016).

**Table 20.** Transfer Factor Index associated to each transfer factor value, corresponding to the soil texture, for the grain of cereals in temperate climates.

Soil texture	Mean	Soil-to-Crop Transfer Index ( $I_{TF}$ )
Sand	$3,90 \times 10^{-2}$	3: High
Loam	$2,00 \times 10^{-2}$	2: Medium
Clay	$1,10 \times 10^{-2}$	1: Minimum

Source: IAEA, 2010c

According to the topsoil properties throughout the Iberian Peninsula, the Caesium Bioavailability Index and the Transfer Factor Index are assessed. Then, both are combined by multiplying them as shown in **Figure 49**, to obtain the Radiological Vulnerability Index. The resultant values are reclassified into five radiological vulnerability classes: from 1 for minimum vulnerability to 5 for the maximum.

**Figure 49.** Risk matrix to combine the Caesium Bioavailability Index and the Transfer Factor Index to obtain the Radiological Vulnerability Index.

Combination matrix to obtain the Radiological Vulnerability Index:

Cs-137 Bioavailability Index \ TF Index	Min. TF	Low TF	High TF
	1	2	3
Very Low Bioavailability   1	1	2	3
Low Bioavailability   2	2	4	6
Medium Bioavailability   3	3	6	9
High Bioavailability   4	4	8	12
Very High Bioavailability   5	5	10	15

Radiological Vulnerability Index values:

1	1: Minimum Vulnerability
2 - 3	2: Low Vulnerability
4 - 6	3: Medium Vulnerability
8 - 12	4: High Vulnerability
15	5: Maximum Vulnerability

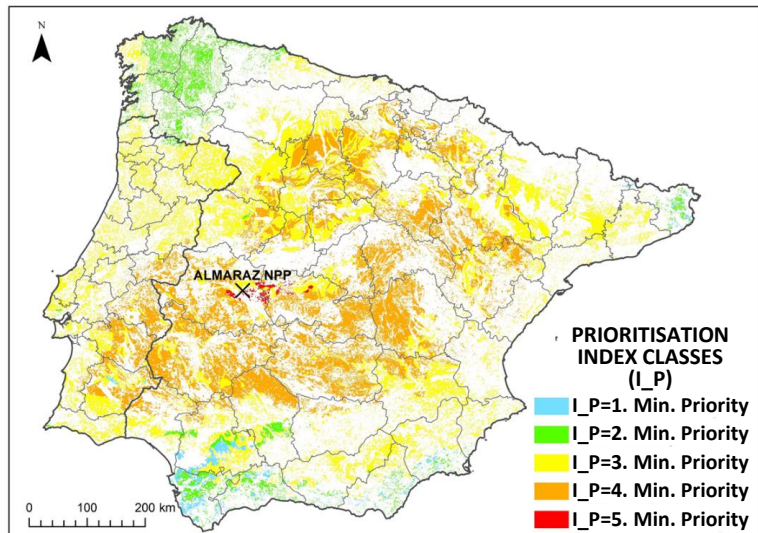
Source: ANURE, 2017

Finally, a Prioritisation Index is obtained. This index results from the reclassification of the results obtained from the multiplication of the corresponding Deposition Index and the Radiological Vulnerability index for cereals (**Figure 50**). To perform this combination, previously the deposition map and the radiological vulnerability map must be overlapped by means of a GIS. The spatial distribution of this Priority Index is a risk map for prioritising recovery actions, considering the rainfed cereals affected by <sup>137</sup>Cs ground contamination from Almaraz NPP releases. The higher the prioritisation index is, the higher the risk posed to the food chain for the long-term is. This map raises the overall risk categorization and allows identifying priority areas for actions to be undertaken and making decisions on recovery investment. For instance, in areas with the highest

priority indexes (4-5), remediation actions should be applied with the aim to minimize the root Cs uptake for the next year harvested cereals.

**Figure 50.** Priorisation map of the Iberian Peninsula for cereals and <sup>137</sup>Cs deposit

Rad. Vulnerability Index	Min. R.V.	Low R.V.	Med. R.V.	High R.V.	Max. R.V.
<b>Deposition Index</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
<b>Minimum Dep. I.</b>	1	2	3	4	5
<b>Low Dep. I.</b>	2	4	6	8	10
<b>Medium Dep. I.</b>	3	6	9	12	15
<b>High Dep. I.</b>	4	8	12	16	20
<b>Maximum Dep. I.</b>	5	10	15	20	25



Source: ANURE, 2017

**Box 14: An example application of the JRodos Emergency model chain**

The redesigned Java-based version of the EU nuclear emergency response system RODOS<sup>158</sup> is a decision support system for accident management, in continuous updating. The system is free and open source, and available upon request. JRODOS is a synthesis of many innovative methods and techniques, being suitable for real-time decision-making and for probabilistic analysis, by mean the statistical analysis tool for countermeasure planning available. JRODOS has been developed within several European research projects and is currently being used in more than 20 countries worldwide (Raskob 2010).

JRODOS operates on modern information technology platforms and it is fully supported by the platforms Microsoft Windows and Linux, and partly Mac OS. For straightforward applications, it is sufficient to use a quad core 64 bit laptop with 4 gigabyte RAM and 200 gigabyte hard drive. The system consists of a Server part for computations and system management, a Client part for interactions with the user, and a Data Base (PostgreSQL) (KIT, 2017). JRODOS shows good performance and operational stability and is user friendly in operation and administration. In addition, inherent features and tools allow adapting models, databases, and the user interface to national conditions and user preferences.

In the following, the JRODOS user interface is explained by means of an example application of the so-called EmergencyLite chain (KIT, 2017). To this aim, we assume a hypothetical accident taking place at the Almaraz nuclear power plant, sited in Spain, and the use of re-analysis Grib2 NOMADS data:

1. Create a new project: When the User Interface be open, the operator just needs to click on File ☐ "new project" or in the "create a new project" icon. A pop-up window appears to define the project name, project description and model chain. In this case, the EmergencyLite chain project is named "Almaraz". Click [confirm].
2. Tab "Site" (Define the scenario – location of the incident): All European operating NPP are already available in JRODOS database. The user can choose the country (e.g. Spain) from the list of countries, and the site/unit (e.g. Almaraz/Amaraz 1) from the list of available reactors. Click [confirm]

<sup>158</sup> www.rodos.fzk.de

3. Tab "Source term" (Define the characteristics of the source term): The first step is to setup the release time (day and hour) (e.g.02.08.2018 09:35). The second one is to define the source term. In an emergency, when the actual emissions may be difficult to obtain quickly and a first assessment of the emergency situation is needed, source terms already stored in JRODOS ("system public" or in "user public"), or previously imported by ourselves ("user defined or imported/loaded run") (e.g. Chernobyl (Waight et al., 1995), Fukushima (Stohl et al., 2012)) are usually used. In this case, the user public source term "F6.Tracer\_24Hrs\_Cs137" is selected. Click [confirm]

4. Tab "Weather" (Specify the meteorological information to run the calculation). In the "Prognosis time setup", the prognosis coverage after the starting release time, and the time step of the outputs are defined (e.g. 24 hours and 60 min respectively). Meteorological data can be from provider, or defined by the user ("user input"). While the latter can be collected on site or from an existing nearby sites, the prognostic meteorological data needed to perform atmospheric dispersion and deposition calculations, can be obtained from different sources.

a) NOAA National Operational Model Archive and Distribution System (NOMADS) project; JRODOS is usually pre-configured to automatically download NOMADS data, e.g. free global meteorological data from the Global Forecasting System (GFS) of NCEP (GRIB1 and GRIB2 files)<sup>159</sup>.

b) National meteorological offices or weather services (e.g. HIRLAM<sup>160</sup>, ALADIN<sup>161</sup>). They are non-free for most organizations.

c) European Centre for Medium-Range Weather Forecasts (ECMWF) NWP data<sup>162</sup> o In-house Numerical Weather Prediction data: higher spatial and temporal resolution (e.g. WRF, Andronopoulos et al., 2014). Better spatial and temporal resolution. In case of not having files for the simulating period, nothing appears on the data provider label. Click [confirm]

5. Tab "Run" (select the grid type and the distance to which the calculation shall be performed). In this tab, the pre-setting is "Exercise". The spatial coverage of the prognosis is defined in this tab. By default JRODOS used 5 rings of the grids, and JRODOS offers the option of playing with distance and grid type in order to cover the purposes and needs of the calculation (e.g. if the chosen radius of calculation is 800 km, it corresponds to a minimum grid cell size of 2 km. This means that the grid cell size is 2 km around the point of release, and it becomes progressively coarser with the distance). Once selected the grid cell size (e.g. 800 (2)), click [confirm].

6. Tab "Summary". This tab reports a summary of the defined inputs. At this stage, the user can go back to any tab for inspection or corrections, as well as, all input made is saved and can be re-used for future projects. Click [confirm].

7. "Prognostic calculations". By using the defined inputs, JRODOS uses the near range Atmospheric Transport and Deposition Model, the Emergency Action Simulation model and the Terrestrial Food Chain and Dose Module, to carry out the prognosis calculations one after the other, without further user interference. Time consuming depends on the temporal duration of the simulation. In this specific case, the calculation lasts 5 min.

8. "Visualization" (JRodos User Interface). JRODOS illustrates the presentation of map-type results. The central "Map" tab consists of one or more result and map

## 19.6 Gaps and challenges

In radiation protection, the International Commission on Radiological Protection quantified the risk of stochastic effects of radiation and proposed a system of dose limitation based on three principles, justification, optimisation of protection, and individual dose limitation (ICRP, 1977).

Lessons learned from past nuclear events, such as Three Mile Island (1979), Chernobyl (1986), and the most recent of Fukushima have influenced the nuclear industry significantly. The nuclear industry has still to have challenges to maintain and improve the safety regarding nuclear activities. We would like to highlight the importance of the multiform activities conducted to prevent any accident or to limit its consequences should one occur. For instance, the events at Fukushima clearly demonstrate the potential risk significance of accidents involving release of radionuclides from multiple sources. The link between natural hazards and its impact on nuclear facilities is a topic of wide interest for which knowledge should be improved and developed.

PSA results have positive implications for the day-to-day operation of existing nuclear power plants. On top of this, research and development activities should be aimed at improving PSA codes, for instance in order to model all the dependencies between systems and to properly account for human actions. A greater understanding of how to interpret, utilise and communicate probabilistic information is also required. This is

<sup>159</sup> <https://www.ncdc.noaa.gov/dataaccess/model-data/model-datasets/global-forecast-system-gfs>

<sup>160</sup> <http://hirlam.org/>

<sup>161</sup> <http://www.umr-cnrm.fr/aladin-old/>

<sup>162</sup> <https://www.ecmwf.int/>



particularly important, since future development in forecasting systems, lead to forecast that are inherently probabilistic.

PSA results are complex and it cannot be reduced to a single number. Instead, PSAs provide a wide spectrum of possible outcomes associated with a frequency distribution. It is clear that from the beginning of its use, there have been a change both in quality and in maturity of the PSA technique. The level of detail of PSA has changed considerably. Mosleh 2014 presented a perspective of strengths, current limitations and possible improvements of the PSA methodology. This author reaches several interesting conclusions, as current PSA methods can remain adequate for certain problems, but there is a need for improving stakeholder confidence and engagement in risk-informed decisions through improving and demonstrating credibility of PSAs.

PSA applications are becoming more and more important. Due to its own nature, PSA methods have revealed significant differences in results when the same risk problem is analysed by different methods and/or different analysts. The justification of this fact is because most of the factors influencing the PSA results can only be determined with a high level of uncertainty. Seibert et al., 2013 indicates the following major factors of uncertainty to assess the risk in the framework of the FlexRisk project: 1) the accident frequency to different NPP, 2) the risk parameter considered, 3) the release fraction (source term definition), and 4) the dispersion calculations. Among them, the definition of the source term is pointed out as the most important uncertainty factor. Analysts try to reduce uncertainty by a) improving and evaluating their models; b) more precise parameterizations of physical processes; and c) collecting additional data to improve model accuracy.

A comprehensive risk assessment is necessary to mitigate risks for new and existing plants, which needs adequately evaluate the climate vulnerabilities of nuclear power and the subsequent threats to international energy security, the environment, and human health (Jordaan, 2019). Level 3 PSA is the least precise level as consequences depend on several factors affecting the transport and impact of the radioactive material. For example, health effects depend on the population in the plant vicinity, evacuation conditions, and the path of the radioactive plume. The plume, in turn, is affected by meteorological conditions, e.g. wind speed and direction, as well as rainfall or snowfall. Similarly, land contamination depends on the characteristics of the radioactivity release and the land use. In this context, an important issue to consider at Level 3 PSA studies is the need to take into account local and specific data to reduce the uncertainties in the assessment of consequences.

## 19.7 References

- Andronopoulos, A., Kovalets, I., Ievdin, Y., Anulich, S., and Trybushnyi, D., 2014. Operation of Decision Support Systems for Nuclear Emergencies based on freely available meteorological data – New functionalities developed in the NERIS- TP project. NERIS-TP dissemination workshop, 22-24/01/2014 Oslo, Norway [https://euneris.net/images/activities/workshops/2014-01/04Andronopoulos\\_23\\_Jan\\_RODOS-WRF1.pdf](https://euneris.net/images/activities/workshops/2014-01/04Andronopoulos_23_Jan_RODOS-WRF1.pdf)
- Apostolakis, G., 2003. How useful is quantitative risk assessment? Massachusetts Institute of Technology, Engineering Systems Division. ESD-WP-2003-05.
- Arnold, D., Gufler, K., Kromp-Kolb, H., Mraz, G., Seibert, P., Sholly, S., Sutter, P., Wensch, A., 2012. FlexRISK- Flexible tools for Assessment of Nuclear Risk in Europe. In Air Pollution Modeling and its Application XXI; Springer, Dordrecht. The Netherlands. pp 737-740.
- Bengtsson, L., Holmberg, J-E., Rossi, J., Knochenhauer, M., 2011. Probabilistic Safety Goals for Nuclear Power Plants; Phases 2-4 / Final Report. 2010:35.
- Beniston, M., et al., 2007. Future extreme events in European climate: an exploration of regional climate model projections. *Clim. Change* 81, 71–95. <https://doi.org/10.1007/s10584-006-9226-z>.
- European Environment Agency (EEA) 2016. *Corine Land Cover 2012 seamless vector data. 2016. Version 18\_5*. [Online] Available at: <http://land.copernicus.eu/pan-european/corine-land-cover/clc-2012> [Accessed 6 2 2017].
- European Commission, Food And Agriculture Organization of the United Nations, International Atomic Energy Agency, International Labour Organization, OECD Nuclear Energy Agency, Pan American Health Organization, United Nations Environment Programme, World Health Organization. 2014. Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards, IAEA Safety Standards Series No. GSR Part 3, IAEA, Vienna.
- ANURE, 2017. Specific Agreement between JRC-CIEMAT. Joint Project ANURE “Assessment of the Nuclear Risk in Europe. A Case Study in the Almaraz Nuclear Power Plant (Spain)” Ref. CIEMAT 7551/2016.

- García Puerta, B., 2020. The use of Geographic Information Systems in creating tools to improve nuclear emergency and response plans and as an aid in the decision-making process for agricultural áreas. (Defense date: November 19th of 2020. To be published in TESEO database). [Doctoral dissertation, Complutense University of Madrid].
- IAEA-INSAG, 1999. Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev.1.
- IAEA, 2006. Fundamental Safety Principles. IAEA safety Standards for protecting people and the environment. No SF-1.
- IAEA, 2009. INES - The International Nuclear and Radiological Event Scale. User's Manual (2008 Edition), IAEA, Vienna. 206 pp.
- IAEA 2010a. Development and application of level 1 Probabilistic Safety assessment for nuclear power plants. Specific Safety Guidelines. IAEA safety standards series No. SSG-3.
- IAEA 2010b. Development and application of level 2 Probabilistic Safety assessment for nuclear power plants. Specific Safety Guidelines. IAEA safety standards series No. SSG-4.
- IAEA, 2010c. Handbook of parameter values for the prediction of radionuclide transfer in terrestrial and freshwater environments. IAEA, Technical reports series nº 472.
- IAEA, 2011. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)
- IAEA, 2012. Technical meeting on Level 3 Probabilistic Safety Assessment. IAEA Headquarters, Vienna, Austria.
- IAEA, 2016. IAEA Safety Glossary. Terminology Used in Nuclear Safety and Radiation Protection (2016 Revision), 219 pp.
- IAEA, 2018. Climate change and nuclear power 2018. IAEA, Vienna.
- ICRP, 1977. Recommendations of the ICRP. ICRP Publication 26. Ann. ICRP 1 (3).
- Jordaan, S.M., Siddiqi, A., Kakenmaster, W., Hill, A.C., 2019. The Climate Vulnerabilities of Global Nuclear Power. Global Environmental Politics, Vol. 19, No. 4: 3-13.
- U.S NRC 2013. Technical Analysis Approach Plan for Level 3 PSA Project (Rev 0a, Working Draft).
- Karlsruhe Institute of Technology (KIT), 2017. JRodos: An off-site emergency management system for nuclear accidents. [https://resy5.iiket.kit.edu/JRODOS/documents/JRodos\\_Report\\_forHomepage.pdf](https://resy5.iiket.kit.edu/JRODOS/documents/JRodos_Report_forHomepage.pdf)
- Kostadinov V., 2011. Developing new methodology for nuclear power plants vulnerability assessment, Nuclear Engineering and Design 241 (2011) 950–956
- Mosleh, A., 2014. PSA: A perspective on strengths, current limitations and possible improvements. Nuclear Engineering and Technology, 46, 1-10.
- NEA, 1998. Nuclear Power and Climate Change. <http://www.oecd-nea.org/ndd/climate/climate.pdf>
- Nordic Guidelines and Recommendations (NGR), 2014. Protective Measures in Early and Intermediate Phases of a Nuclear Or Radiological Emergency. Beredskabsstyrelsen (Denmark), Sundhedsstyrelsen (Denmark), Geislavarnir Ríkisins (Iceland), Stuk (Finland), Statens Stralevern (Norway), Stral Sakerhets Myndigheten (Sweden).
- Raskob, W. and Hugon, M. (Eds.) (2010). Enhancing nuclear and radiological emergency management and rehabilitation: Key Results of the EURANOS European Project. Radioprotection Vol. 45, No. 5 Supplément 2010.
- Raskob, W., Schneider, T., Gering, F., Charron, S., Zheleznyak, M., Andronopoulos, S., Heriard-Dubreuil, G., Camps, J., 2016. Innovative integrative tools and platforms. Key results of the PREPARE European Project. Radioprotection 51(HS2), S59-S61.
- Seibert, P., Arnold, D., Arnold, A., Gufler, K., Kromp-Kolb, H., Mraz, G., Sholly, S., Wenisch, A., 2013. FlexRISK- Flexible tools for Assessment of Nuclear Risk in Europe. BOKU-Met Report 23. ISSN 1994-4179.
- Schar, C., Vidale, P.L., Luthi, D., Frei, C., Harberli, C., Liniger, M.A., Appenzeller, C., 2004. The role of increasing temperature variability in European summer heatwaves. Nature 427, 322. <https://doi.org/10.1038/nature02300>.



Stohl, A., Seibert, P., Wotawa, G., Arnold, D., Bukhart, J.F., Eckhardt, S., Tapia, C., Vargas, A., Yasunari, T.J. (2012) Xenon-133 and caesium-137 releases into the atmosphere from the Fukushima Dai-ichi nuclear power plant: determination of the source term, atmospheric dispersion, and deposition, *Atmospheric Chemistry and Physics*, Vol. 12, 2313–2343.

Vagnoli M. et al., 2017, Ensembles of climate change models for risk assessment of nuclear power plants, *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*.  
<https://doi.org/10.1177/1748006X17734946>.

Waight, P., Metivier, H., Jacob, P., Soulchkevitch, G., Viktorsson, C., Bennett, B., Hance, R., Yumazawa, S., Kusumi, S., Bouville, A., Sinnaeve, J., Ilari, O., and Lazo, E.: Chernobyl – Ten Years on: Radiological and Health Impact, OECD Nuclear Energy Agency and OECD Nuclear Energy Agency, Committee on Radiation Protection and Public Health, 1995.

Yan, W. (2016), How regional wind patterns will influence climate change, *Eos*, 97,  
<https://doi.org/10.1029/2016E0053209>. Published on 06 June 2016.

## 20 Terrorist attacks

VASILIS KARLOS, MARTIN LARCHER

### 20.1 Introduction

Over the last years, the fear of terrorism is steadily one of the main concerns of Europeans, as can be witnessed by the latest Eurobarometer surveys (Standard Eurobarometer 92, 2019). This is mainly attributed to its unique characteristics, unpredictable nature and the extensive coverage of attack incidents by the media. Even though terrorist events are of low frequency, a comprehensive understanding of the parameters that influence their likelihood is required for establishing a robust risk assessment and management framework. Independent of their rarity, their psychological, economic and political impact on society can be disproportionately high, as for example after the bombing attacks in Brussels and the vehicle-ramming attack in Nice in 2016. As a result, the European Commission has issued an 'Action Plan to support the Protection of Public Spaces' (European Commission, 2017) that Member States, regions and cities are advised to incorporate into their infrastructure investment program.

As mentioned in the Commission Staff Working Document (European Commission, 2017) developed through the results of the National Risk Assessments (NRAs) of Member States, the global terror threat is uncertain due to its complex and fragmented nature, that includes both structured groups and individual (lone wolves) aggressors. In particular, scenarios concerning individual terrorist actions aiming public spaces and critical infrastructures have been developed with links to political and religious extremism. A terrorist attack could potentially have cascading effects and cross-sectorial consequences, e.g. pandemics after an attack with a toxic agent or environmental disaster after a substance release.

Terrorist events can be defined as intentional violent acts performed under the pretext of political, religious or social motives, whereas crime is usually driven by economic or retaliation intentions. The borderline between terrorism and military conflicts (encounters in which armed combat among military forces takes place either at international or national level) might be hard to be distinguished, since both rely on the extensive use of violence and could be guided by similar motives. Weapons (firearms, knives etc.), vehicles, CBRN (Chemical, Biological, Radiological and Nuclear) devices and improvised explosive devices (IEDs) that are either homemade or purchased in the black market are the preferred attack methods of terrorist groups and lone actors. However, it is important to consider that the modus operandi of the aggressors (in both terrorist acts and military conflicts) can rapidly transform, as has been demonstrated in the recent past. This transformation depends on a number of factors, such as the current political, economic and religious status that are driving the motives, the skills and capabilities of the perpetrators, the availability of financial and human resources, the instructions and guidance available in terrorist propaganda sites and magazines. A tendency has recently appeared to target unprotected public spaces of mass congregation (also known as soft targets) by using easily obtained weapons like knives, axes or vehicles. Such attacks may generate cascading effects on the societal level as the objectives of the terrorists include, but not limited to, causing casualties, gaining media attention, spreading fear and inflicting a sense of insecurity in the public's daily life.

The risk of terrorism exists in both developed and developing countries and it still poses a major concern in certain regions that are mainly located in Africa, the Middle East and Asia. Nevertheless, the recent attacks in the Western world have clearly demonstrated that terrorism is a worldwide phenomenon, featuring complex direct (e.g. victims, injuries, loss of property) and indirect (e.g. psychological) consequences on the society. Unfortunately, the unique characteristics of terrorism risk are often neglected, resulting in a lack of dedicated guidance material for assessing and managing the relevant risk. Therefore, the establishment of a national terrorism risk assessment plan is crucial for identifying critical zones and tactics and get the overall picture regarding the economic, social and political consequences in case of a successful attack.

The varied, cross-border and cross-sectorial nature of terrorist attacks is addressed at the EU level in the European Agenda on Security (2015), which aims at assisting Member States in ensuring security through coordinated and effective response at the European level. As a result, several operational measures have been proposed to significantly reduce the number of inherent vulnerabilities that were exposed in previous terrorist attacks and enhance the overall security of potential targets.

The development of a risk assessment and risk management procedure in the field of terrorism is an overwhelming task and presents a challenge for every Member State in terms of complexity, time and resources. Providing answers to terrorism-related issues (e.g. how to prioritize the assets to be protected, how to strike the right balance between effective and cost-efficient countermeasures etc.) is more difficult than the ones concerning natural hazards, since the terrorism risk incorporates numerous attack scenarios (e.g.

blast, vehicle, UAS, active-shooter, knives), resulting in approaches that may differ greatly depending on both the examined asset and the attack type. Risk assessment aims at estimating the potential impacts of terrorist acts, their severity and their probability of occurrence. As different assets require very different analysis of their risk, questions usually arise concerning how to establish a terrorism risk management plan, how to initiate a terrorism risk assessment process, what are the best mitigation/deterrence strategies and how to prioritize the allocation of resources. As has already been demonstrated in the management strategies of other risks (e.g. drought, earthquakes, floods, biological disasters, chemical and nuclear accidents), the proposed scheme should incorporate an orderly approach for identifying and tackling the threat of terrorism.

In the current chapter, the definition of risk assessment according to the ISO 31010 (ISO, 2018) will be employed, even though the steps that are described in the standard concerning the risk assessment process are generic, in order to include both natural and human-induced hazards. Certain shortcomings in the risk assessment methodology have already been pointed out by preceding documents (ISO 31000:2009), such as the difficulties in estimating the likelihood of rare events and the quantification of consequences in the human/social domain. The approach that is proposed herein, is based on a collection of best practices related to the risk assessment of various hazards/threats, while certain techniques that can assist national authorities in their risk assessment and management process are introduced. Finally, light is shed on substantial gaps and challenges that generate obstacles in the calculation of the risk from terrorist attacks.

## **20.2 Lessons learned from prior terrorist attacks**

The deadliest terrorist attacks have been usually carefully planned (or at least to a certain degree) to maximize the number of casualties, increase the generated damage and draw the attention of the media. Targets are usually selected according to their vulnerability and past experience has shown that unprotected sites have higher chances of being attacked. Predicting locations and type of a potential attack is a challenging task, since there exist many different factors that affect the reaction of the aggressors. In this section, a selection of indicative cases of terrorism incidents, which resulted in a large number of victims and injuries, is presented, emphasizing on their common characteristics and underlining lessons-learned that have influenced the selection of protection measures against terrorism acts, serving as useful examples for future risk assessments.

- One of the most notorious terrorist acts resulting in a great death toll is the attack against the World Trade Centre in New York, USA on 11th September 2001, which took place in parallel to other attacks in the USA. The attack included sophisticated and detailed planning, aiming at structures of symbolic value, while guaranteeing a great number of victims and provoking panic and fear to the population. The use of asymmetric warfare techniques led to the realization that both public spaces and critical infrastructures could be potential targets of terrorist attacks and that different strategies need to be adopted for resisting the aggressors. The business and economic activities at the affected sites were disrupted for many weeks due to the widespread destruction causing severe consequences at the financial sector. The 19 terrorists who hijacked four airplanes, were members of the Al-Qaeda network and four of them had received specific pilot training in the USA without raising any suspicion to the secret services.
- On 19th April 1995 in Oklahoma City, USA a vehicle borne explosive device was detonated in front of the A. P. Murrah building resulting in the collapse of approximately one third of the structure. The attack was performed by two US citizens that had undergone military training, though not belonging to a terrorist group, and was extensively planned while it targeted a structure that housed several state facilities, since the aggressors wanted to disapprove several governmental actions. Bomb ingredients were acquired from local stores and the bomb was placed in a rental truck that was parked on the curb outside the nine-storey building. After the attack, the remaining standing structure was demolished due to safety reasons and several years were required for the construction of a new facility that would substitute the old one.
- On 13th November 2015, Paris experienced a series of coordinated terrorist attacks that resulted in a great number of victims and injuries. The aggressors used person-borne improvised explosive devices (suicide bombers) and assault rifles attacking a sport stadium, a music theatre and several restaurants and bars. The perpetrators belonged to the ISIL group and claimed that the motives behind the attacks were the ideological objections to the western lifestyle. Clearly, the simultaneous attacks against multiple targets, reveal the existence of a sophisticated plan against places of mass congregation that would guarantee maximizing the number of victims and drawing the attention of the media.

- One of the deadliest vehicle-ramming attacks took place at the city of Nice against the thousands of people gathered at the city's waterfront during the Bastille Day celebrations. On 14th July 2016 a 20-ton rented cargo truck attacked the public by managing to attain a speed of 70-80km/h, as the promenade leading to the pedestrian zone was an almost straight path. Because of its mass and speed, the truck managed to force its way through the existing light protection measures (crowd control portable barriers, lane dividers etc.) and covered a total distance of approximately 1.7km before being stopped by the police. In order to increase the number of victims, the terrorist, who had not been involved in major crimes before, was driving the truck in a zigzag fashion boarding the crowded sidewalks whenever possible. Police investigation revealed that the aggressor had been planning the attack for over a year and that he had surveyed the site while driving the rented truck on numerous occasions before the assault date. He was born in Tunisia and had been living in France for more than 10 years, while he had been previously involved in minor crimes and was radicalized, sharing the views of the Islamic State, shortly before the vehicle-ramming incident.

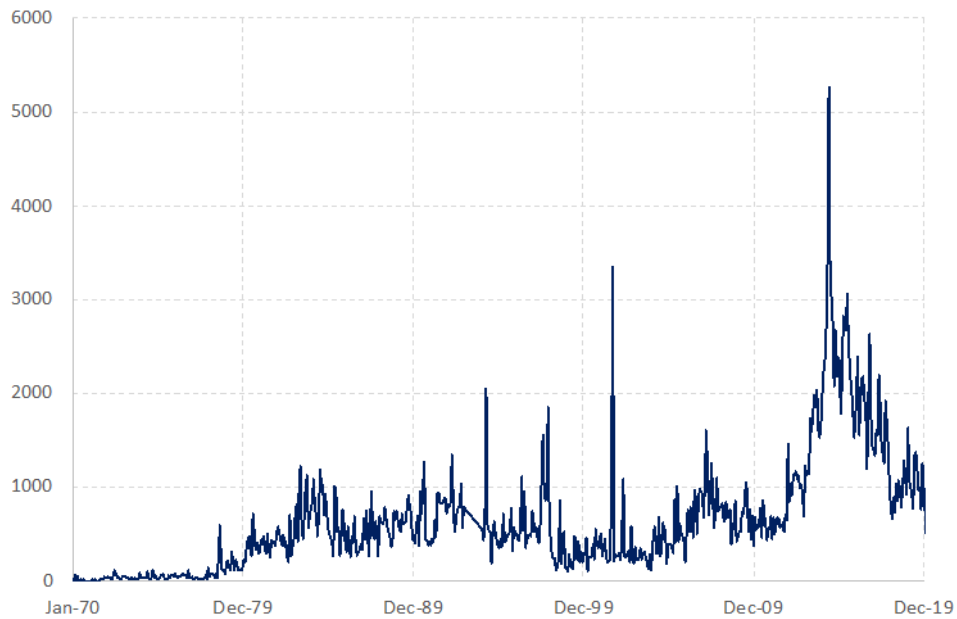
The above-mentioned events are only a small fraction of the number of terrorist attacks that have been performed over the last years, but constitute a sample of different scenarios (including the use of airplanes, explosives, weapons and vehicles as the preferred attack methodology) that shares a substantial number of characteristics. It is clear, that the majority of the described incidents were carefully planned in advance, as the aggressors had examined the attack sites beforehand to mark their vulnerabilities. The targets were iconic structures and places of mass congregation that would cause mass casualties, gain media attention and spread terror and fear at the population. The sites were characterized by the absence of (or the presence of insufficient) protective measures that would be able to deter or mitigate the consequences of the assaults. The outcome of the attacks resulted in a great number of victims, damages on infrastructures, economic losses that lasted for a long period and psychological impacts on the society. Moreover, the majority of the aggressors were not considered a threat by the local intelligence agencies, as they had never been arrested before, even though in some occasions their planning communications were unencrypted.

A common feature among the majority of the attacks was the role of radicalisation (especially for Jihadist related attacks), as many of the aggressors had adopted violent extremism after being inspired from radicalised preachers and online propaganda. Tackling radicalization is a major challenge that requires the collaboration of different stakeholders at both national and local level. There are various reasons and paths that push individuals to violent extremism but since most of them have roots in the local community, detection and prevention activities need to mainly focus at the local level. Clearly, the most effective prevention is to deter people from performing acts of terrorism in the first place, which is why the European Commission has set up the Radicalisation Awareness Network (Migration and Home Affairs-RAN, 2018) working on the fight against terrorism that has provided guidance material on assessing the relevant risk and suggested actions that guarantee resilience against violent radicalisation.

It has already been highlighted that aggressor tactics and targets may quickly change introducing attack techniques that were not considered before. For instance, Radiological Dispersion Devices (RDD's, also known as "dirty bombs") are feared to be of interest to terrorist groups as they can be constructed by combining conventional explosives with radioactive material normally used in nuclear medicine and industrial applications. The aim of such an attack is generating a panic reaction in the public and inflicting high economic damage due to the required cleaning actions and the consequences from the disruption of affected services. As the immediate number of casualties from such attacks is small, a target may be selected not because of its high concentration of people, but depending on the favourable dispersion conditions for the radioactive particles. Moreover, as drone technology has proliferated over the last years, there are growing concerns regarding the security threat they pose, as they have already been used for terrorist attacks outside Europe.

However, not all terrorist attacks are extensively planned and may be of opportunistic character resulting in smaller number of fatalities. The impact of an attack on the society is not necessarily related only to the number of fatalities and injuries, since even a failed attack may have significant psychological implications for the public. Depending on the information source, the worldwide number of terrorist attacks in the last years is approximately 20,000 per year and the number of yearly casualties about 25,000 (**Figure 51**).

**Figure 51.** Fatalities per month from global terrorism database 1970-2017 (year 1994 is missing in the recordings) and Control Risks (2018-2019).



Source: University of Maryland, 2018

### 20.3 Risk assessment

ISO 31010 provides a generic approach to managing various risk types, since it is not directly correlated to a specific hazard or asset, while EN 1991-1-7 (EN 1991-1-7, 2006) provides a risk assessment process against accidental loads in the field of buildings and civil engineering structures. The most common approach for assessing the risk of a certain site can be divided in three distinct steps that can help decision-makers in prioritizing their security needs: risk identification, risk analysis and risk evaluation. If the risk assessment process within a terrorism context follows the same format, it could be categorized into the following stages (**Figure 52**):

- Identification of potential terrorist threats by gathering all available information on the risk components and development of relevant attack scenarios.
- Risk analysis (qualitative, semi-quantitative or quantitative) to estimate the likelihood of occurrence and the potential consequences for the exposed assets, while taking into account the vulnerabilities of each potential target.
- Evaluation of the relevant risks for each attack scenario and asset in order to decide whether further action is required and which is the best tailor-made strategy for reducing the risk to an acceptable level.

The risk assessment concerning terrorist threats can be performed at various levels, depending on the asset that is examined. It may be performed at the local level if a stand-alone, specific asset is considered or at a city, regional or national level if a whole sector is analysed. The decision for initiating a risk assessment lies in the hands of the relevant stakeholders (building/site owners, venue organizers, state organizations, security and/or law enforcement officials etc.) and their engagement is crucial for tackling the far-reaching consequences of a potential attack. Clearly, the analysis results may differ substantially depending on the stakeholder performing the risk assessment, as their views on risk maybe differentiate depending on their experience and goals.

**Figure 52.** Risk assessment process.



Source: Authors

### **20.3.1 Threat identification**

The first step in the risk assessment process is the identification of potential terrorist threats that are relevant for the region and the target under consideration. Threat identification focuses on pinpointing potential terrorist tactics and providing the framework for determining effective prevention and/or mitigation measures. For estimating the likelihood of occurrence of a terrorist attack and formulate possible attack scenarios, one has to resort to available statistical data from recent incidents and investigate information that is available from counterterrorism units, intelligence services, state and emergency agencies and the internet. Attack scenarios should be rated according to their feasibility and probability. For example, the probability of vehicle ramming incidents is usually higher compared to attacks with the use of explosives due to the terrorists' direct accessibility to a variety of vehicles, the minimal required expertise and the easy planning. In general, during assessing terrorist threats, decision makers and assessors tend to put more emphasis on past events failing to "think the unthinkable". New tactics may emerge that, even though they might be characterized by a smaller probability, could result in higher societal, economic or political impact. A scenario-based approach at potential targets is bound to simplify the complexity of the risk assessment process and assist in the evaluation of the different targets in terms of criticality (i.e. consequences severity).

#### **20.3.1.1 Threat identification on national level**

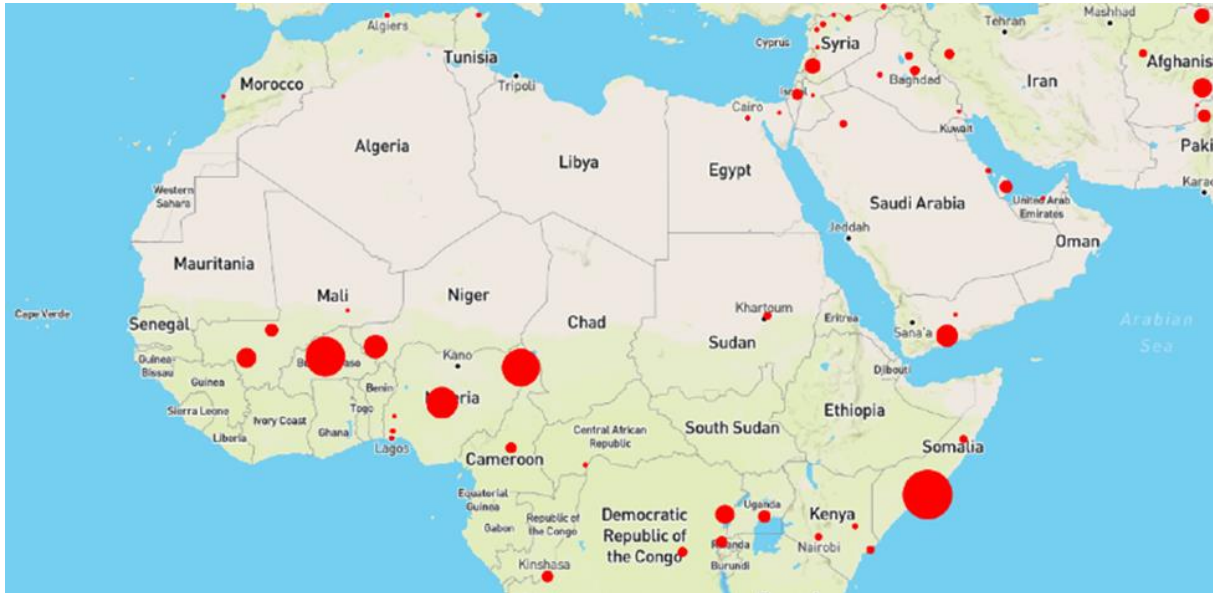
The nature of extreme manmade events with malicious intent, such as terrorist attacks, differentiates them from other natural hazards. Their intentional character means that they are not as common events as, for example small scale earthquakes, floods or droughts. Classical statistical approaches may provide an indication for calculating future risk, even if in some cases the statistical basis might not be enough. Detailed data from additional sources, such as intelligence agencies, could be required for a more rigorous analysis. Information included in propaganda sites and magazines can greatly contribute in identifying potential attack scenarios against specific targets. Nevertheless, information concerning potential terrorist threats is not always readily available due to its sensitive nature and access may be granted only to authorized individuals and not to private stakeholders. Moreover, the risk needs to be re-assessed in regular intervals to analyse any new security-related information and relevant threats, especially since a major part of malicious events is politically or religiously motivated and can rapidly transform, as has been demonstrated in the recent past.

Potential attack scenarios can be estimated by examining any observed criminal activity in the area of interest and possible recorded incidents or security breaches over a certain time period. Possible data sources are:

- Global terrorism database (University of Maryland, 2018), which is freely available but updated on an annual basis, which means that latest data are not readily available.
- Commercial security risk providers like Jane's (IHS Markit, 2019) or Control Risks (Control Risks Group Holdings Ltd, 2019) databases.

- European Media Monitor (European Commission-EMM, 2020) system that analyses information from both traditional and social media. The usability of the provided data to create a terrorism tool by using machine learning approaches is currently tested by the JRC. A first result of that approach is shown in Figure 53.

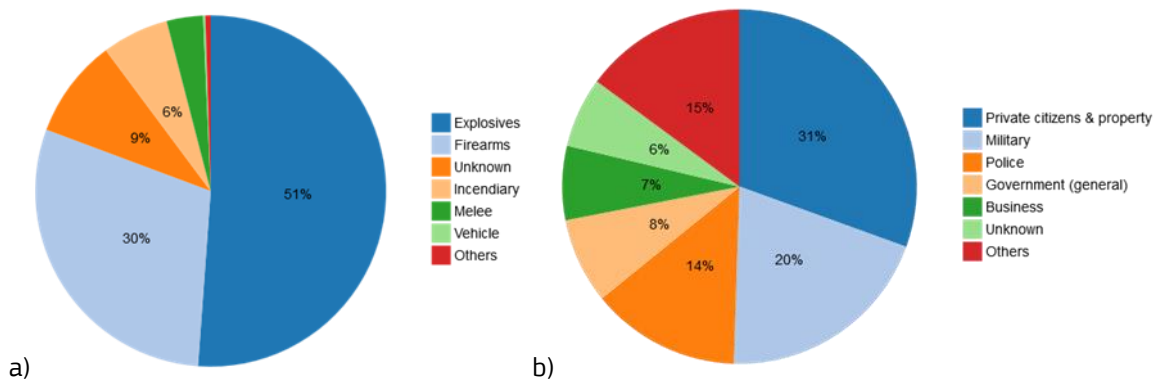
**Figure 53.** Threat level from terrorist attacks in central Africa and Middle East in 12/2019-03/2020 by JRC terrorism database using EMM.



Source: Background map © Mapbox, © OpenStreetMap

Since terrorism threats can completely change over time, special attention should be paid on very recent events, thus it is advised that higher statistical weighing factors are assigned to such events during the threat identification process compared to older ones. Supporting information that can prove valuable during this threat identification process may be located in organized crime databases, such as the number of firearms in circulation, the terrorism funds obtained via drug trafficking etc. For example, the pie charts presented in **Figure 54** highlight the worldwide predominant assault types and targets over a four-year period (2014-2017).

**Figure 54.** Worldwide terrorist attacks by a) utilized modus operandi and b) target.



Source?

Assessing the risk of terrorism on a country level, can prove useful in identifying critical countries, yet the results are usually too general for recommending and implementing specific actions. A breakdown of risk to smaller regions is even more questionable, since the statistical significance of available data might not be adequate for performing a reliable assessment. The development of worldwide critical terrorism-affected

zone maps (e.g. Niger, Afghanistan, Yemen) that demonstrate terrorist incidents, like the one presented in Figure 53, can assist in classifying hot spots and issuing travel advices, but are impractical if the introduction of specialized protective plans is of interest.

**20.3.1.2 Threat identification on local level**

Carrying out a threat identification on a local level is a challenging process, as a definite “yes or no” answer concerning imminent attack types cannot be provided. Quantifying the probability of a terrorist attack against a specific target may seem futile, as by nature it contains many uncertainties. Examining statistical data from previous similar events at the region and potential target of interest using the databases that have been described in the previous section, can provide valuable indications concerning its threat rating. Nevertheless, usually there are not adequate data (especially in Europe) to support the assessment and expert judgement is required to identify the specific threats that are of interest to the examined asset.

**20.3.2 Risk analysis**

To determine the risk level, a dedicated risk analysis has to be performed, where the various risk components and drivers are combined, such as the specific threat, the exposure (including attendance) and the asset’s vulnerabilities. Each risk analysis may greatly vary in degree of detail as it depends on the availability of data and the way the uncertainties and vulnerabilities are addressed. The risk analysis needs to provide the likelihood of an attack and the consequences, should such an attack materialize. Within this process the assets that are exposed to such an attack need to be identified, pinpointing their vulnerabilities and evaluating their influence on the probability of an attack.

**20.3.2.1 Exposed asset identification**

A crucial step in the risk assessment process is the identification of the assets that have to be considered in the analysis, if they have not been expressly preselected by the relevant stakeholder. Recent terrorist attacks have shown that there is a recurrent targeting of unprotected public spaces of mass congregation of various gathering purpose, as shown in Table 21. These are also known as soft targets, meaning targets characterized with high concentration of people and absence of specific security measures. They are the opposite of “hard targets” that indicate grounds equipped with heightened protection and surveillance. Target attractiveness depends on many different factors that are associated with both the terrorist group and its motivation, and the characteristics of the target. For instance, aggressors may choose a target that is against their political, social or religious ideology, while the selection may be also influenced by the availability of funds and the number of terrorist members. This means that religious or cultural symbols that are considered to be promoting the Western lifestyle, capitalism and/or democracy may become the target of Jihadist terrorists. Iconic and recognizable locations have higher chances of being attacked, especially if they are mentioned in terrorist propagandist magazines. Popular tourist locations, open-air festivals, sport events, landmarks and areas that are typically characterized with high people presence and lack of security guards are also appealing to terrorists.

**Table 21.** Soft target categories.



Target category	Places of people congregation
Recreational	Stadiums, concert halls, entertainment venues, festivals, parks, markets, shopping malls, theatres, cinemas, clubs, restaurants, bars, cultural events, parades, pedestrian areas etc.
Commercial	Hotels, apartment buildings, office complexes, shops etc.
Public	Hospitals, medical centres, universities, schools, museums, libraries, etc.



Religious	Churches, religious events, places of worship, etc.
Transportation	Train and subway stations, airports, bus and port terminals, transportations sites, etc.
Governmental	Town halls, ministries, official residences, monuments, landmarks governmental office complexes, etc.

Source: Authors

The weighing factors for evaluating the criticality of each exposed target may be different among the various countries, but some common indicators (e.g. people attendance, site symbolism, facility size and importance) may be used for identifying the sites where potential consequences have the greatest impact. Such a process guarantees improved, custom-made security and mitigation actions, though differences may appear depending on the stakeholder responsible for performing the identification. For instance, the criticality of a certain target from the building/site owners' perspective is usually related to its operation, whereas state organizations and policymakers may be more attentive to the public's security and needs. Consequently, during the design of an effective physical security strategy the harmonic collaboration of all relevant stakeholders is crucial for effectively tackling the interdependencies between the different assets.

### **20.3.2.2 Vulnerability identification**

Vulnerabilities are the inherent weaknesses of a potential target that may render it susceptible to the destructive consequences of a terrorist attack and are directly related to its risk level. These vulnerabilities can be exploited by perpetrators in their effort to strike, thus effective mitigation measures and identification of optimal strategies are required for minimizing exposure and enhancing resilience. A detailed examination of the asset under consideration can disclose deficiencies and flaws that may encourage the formulation of an attack plan, as, for instance, the lighter the security measures, the more attractive a target is deemed to the eyes of terrorists. An objective assessment of the vulnerability degree of a public space or infrastructure is a challenging task, as there are many different factors that should be taken into account, such as the target's accessibility, its significance, its location, its shape and protective measures that may be present (entry checks, video surveillance, security guards, perimeter protection etc.). DG HOME has developed a vulnerability assessment checklist that considers the following attack modes:

- Firearms – Small calibre pistols or semi/fully automatic rifles
- Bladed Weapon – Knives, machete or other sharp and blunt objects
- Vehicle Ramming – Use of vehicle for ramming crowded places
- Improvised Explosive Devices (IED) – Carried or concealed in objects or goods
- Person Borne Improvised Explosive Devices – Concealed on a person
- Vehicle Borne Improvised Explosive Devices – Concealed inside a vehicle
- Unmanned Aerial Vehicles (UAV) as a weapon and UAV borne IED or agents (CBRN-E)
- Biological Agent – Concealed in goods or carried items
- Radiological Agent – Concealed in goods or carried items

Even though these threats are unlikely to take place simultaneously, they emphasize the complexity and plethora of different attack scenarios. This generated tool provides a series of suggestions and questions the assessor should make in order to identify the vulnerabilities of the examined asset and combine them with people attendance so as to arrive in a preliminary evaluation of the potential target's risk level. An example of a vulnerability assessment categorization is shown accordingly:

- Low vulnerability: The examined asset (infrastructure or public space) is equipped with adequate security countermeasures (controlled access, safeguards, perimeter protection etc.) to drive away potential aggressors and is unattractive as a potential target.
- Moderate vulnerability: The examined asset (infrastructure or public space) may be equipped with some security countermeasures (no controlled access, some safeguards, partial perimeter protection etc.) and is well-known only at a local scale.

- High vulnerability: The examined asset (infrastructure or public space) is characterized by inadequate security countermeasures, while it is well-known at a national scale.
- Very high vulnerability: The examined asset (infrastructure or public space) is characterized by inadequate security countermeasures, while it is well-known at a global scale.

### **20.3.2.3 Likelihood and consequences assessment**

The introduction of a universally applicable method for calculating the likelihood of a specific attack type against a certain target is problematic due to the frequently opportunistic character of attack planning and the absence of sufficient data. Moreover, due to the nature of the terrorist threat, the majority of the required information is possessed by various intelligence services and is of restricted nature, which makes the assessment of the probability of an attack a challenging task. Despite the fact that no concrete conclusions can be drawn from analysing the potential modus operandi of the aggressors (attack scenarios), some valuable information regarding the likelihood of an attack can be deduced by responding to several questions that may arise during the assessment process including, but not limited to:

- Are there any indications of an imminent terrorist attack at a local, regional, national or international level?
- Does the potential target represent a religious/ethno-nationalist ideology that is against the political or religious agendas of active terrorist groups?
- Is the target of symbolic or historical value?
- Which is the maximum attendance?
- Are there any high-profile events hosted that are attended by famous people and covered by the media?
- Are there any trained security officials present?
- Are there any security measures already deployed (access control, CCTV, security barriers, perimeter protection, UAV countermeasures etc.)?
- How easily accessible are the target's premises and by what means (vehicles, motorcycles, on foot etc.)?

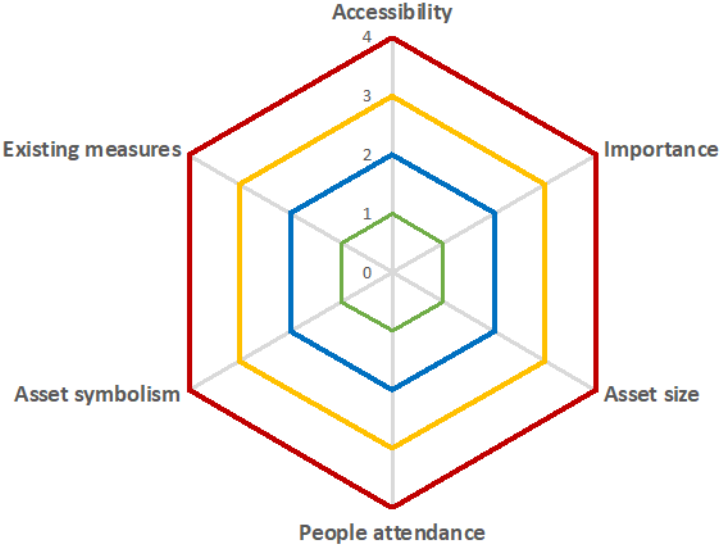
To provide a certain value on the criticality of an asset/building structure and the likelihood of an attack, a number of indicators may be used following a similar approach to the one proposed by the US Interagency Security Committee (ISC, 2013) may be followed. According to this method, a point system is introduced that may be used to provide an estimate of the facility's criticality. Herein, six different factors with equal weights are evaluated and after their scores are summated, the examined asset/site is categorized according to its criticality. The main characteristics of each indicator are:

- Accessibility: Is a measure of the openness of the examined asset to the public, of any reported previous threats (to the asset or the users) and the crime rate at the surrounding area.
- Importance: Depends on the asset's tasks, its interdependencies with other facilities and the consequences to the state and the society after a potential attack.
- Asset size: Demonstrates the space (in square meters) that is occupied by the asset.
- People attendance: Shows the maximum number of people (personnel and visitors) that are present in the asset during peak hours.
- Asset symbolism: Is linked to the attractiveness of an asset as a potential target and on the probability of being considered to be promoting a lifestyle that is against the political, social or religious ideology of aggressors. It also includes popular tourist locations, landmarks and cultural sites.
- Existing measures: Considers security measures that are already present in the examined facility and may render it less attractive in the eyes of possible aggressors.

Figure 55 presents the examined indicators and the points that have to be allocated (1 to 4) to each of them, while Table 22 shows in detail the scoring criteria to be followed when assigning the points. It is underlined that these scoring criteria do not cover all the different cases that may be used for characterizing an asset.

Thus, the scope of the current process is to provide a simplified process for conducting a preliminary assessment regarding an asset’s criticality.

**Figure 55.** Indicator point system for assessing criticality of exposed assets.



Source: Authors

**Table 22.** Scoring criteria per indicator

	Allocated points	1	2	3	4
Indicators	Accessibility	-No public contact -No previous threats -Minor-crime area	-Little public contact -Some previous threats in the surrounding area -Low-crime area	-Normal public contact -Previous threats against the facility -Moderate-crime area	-High public contact -Usual presence of protests -Usual threats against the facility -High-crime area
	Importance	-Insignificant impact at national level in case of an incident -Activities only at local level	-Some impact at national level in case of an incident -Activities only at regional level	-Significant impact at national level in case of an incident -Activities at national level	-Very big impact at national level in case of an incident (e.g. critical infrastructures) -Activities at national level
	Facility size (A)	$A < 1000m^2$	$1000 < A < 10000m^2$	$1000 < A < 25000m^2$	$A > 25000m^2$
	People attendance (N)	$N < 100$	$101 < N < 250$	$251 < N < 750$	$N > 751$
	Site symbolism	-Not well-known facility	-Well-known at a local level -Symbolic only at a local level	-Well-known at a regional level -Symbolic only at a regional level	-Well-known at a national level -Symbolic only at a national level (tourist attraction)
	Existing measures	-Elevated physical security measures	-Some physical security measures	-Basic physical security measures	-Absence of physical security measures

		-Presence of multiple security guards	-Presence of limited security guards	-Absence of security guards	-Absence of security guards
--	--	---------------------------------------	--------------------------------------	-----------------------------	-----------------------------

Source: Authors

After assigning the relevant points to the abovementioned indicators, the points are added together and the criticality of the asset may be defined, as shown in **Table 23**. The criticality level of an asset (low, medium, high or very high) is directly linked to the required protection level and the specific security measures (additional or not) that have to be adopted. The type of measures depends on the asset that has to be protected and need to be decided by both stakeholders and experienced professionals, as will be discussed in the risk evaluation section.

**Table 23.** Assessment of an asset's criticality

Asset criticality	LOW	MEDIUM	HIGH	VERY HIGH
Asset score (points sum)	6-9	10-15	16-21	22-24
Required protection level	LOW	MEDIUM	HIGH	VERY HIGH

Source: Authors

The consequences of an attack are directly linked to the type of target selected by the terrorists and the conditions at the time of the assault. For instance, an attack against a city square will have a completely different aftermath if it is performed during peak hours or during social events when the crowd attendance is at its highest. The impacts of past attacks, such as the effects on human life (injuries, fatalities etc.) and the economy (repair cost, disruption of services etc.), can be used as input for assessing the repercussions of potential future events. Indirect consequences from a terrorist attack are more difficult to be assessed, as they include the social and (indirect) economic costs, such as the effects on the population's psychology and the impact on the tourism industry (Larcher, 2018). Cascading phenomena may also appear through the interconnections among infrastructure systems, such as for instance after a terrorist attack against a power plant which, apart from the immediate life losses, would also result in disruptions in many other sectors and the public.

Consequence assessments serve as a tool for estimating the outcome of different attack scenarios at various sites and categorize them in terms of severity. However, many of the components of terrorist risk and their impact are not quantifiable (especially the ones related to the psychological consequences) and entail a very large degree of uncertainty. Since specialized quantitative approaches for measuring the consequences of an attack are still missing, qualitative methods and expert judgement may provide valuable insight at the dependencies among the different affected elements. Part of the indicators included in the (Sendai Framework for Action on Disaster Risk Reduction 2015-2030) may also be used for analysing the consequences and eventually reducing disaster loss in terms of lives and other types of damage. For example, Global Target A aims at reducing disaster mortality (A-2 compound), while Global Target B is devoted to reducing the number of affected people by an attack. In detail, the framework addresses the 'number of deaths attributed to disasters' (target A-2 compound) and 'number of injured people attributed to disasters' (target compound B-2). Moreover, the objective of Global Target D is to reduce disaster damage to critical infrastructure and disruption of main services, as is specifically indicated in Target Compound D-1 (damage to critical infrastructure attributed to disasters) and Target Compound D-5 (number of disruptions to basic services attributed to disasters).

### 20.3.3 Risk evaluation

During the risk evaluation stage, the results of the risk analysis are evaluated and an appropriate response is selected, indicating and prioritizing the attack scenarios that have an increased likelihood or greater consequences and should be tackled first. Different response alternatives have to be considered, depending on the desired outcome and the availability of resources. The risk can be either deemed acceptable/tolerable, so no further action is needed, or may be considered unacceptable, which means that an intervention is required. The criteria under which the risk is evaluated are based on a mixture of socio-economic-political factors, that can be very different among Member States, local authorities or private stakeholders. In other

words, before arriving at a decision, certain components are considered, including the cost of an intervention, the existing legislation/codes, the presence of physical obstacles, the potential effects on the daily life of the public, the social perception and the political cost.

The decision makers, who are usually different from the expert group responsible for the risk analysis, are frequently required to make a 'judgement call' concerning the action that should be followed, due to the large degree of uncertainties a terrorist attack risk analysis entail. One of the main concerns during these evaluation procedures, is the definition of an acceptable risk level, since providing protection against all possible terrorist threats is not feasible in both economic and practical terms. Clearly, it is difficult to describe the severity of potential consequences by using a single parameter, as it is extremely challenging to assign a value on human life and compare it with lifeless objects. Nevertheless, the results of the risk analysis can provide useful information that can facilitate the employment of the most effective actions and the prioritization of the exposed assets in terms of criticality.

The task of deciding the specific action that needs to be undertaken requires close collaboration between the decision-makers, that evaluate whether the action is required, and experts, that can facilitate the selection of the most efficient solution. For instance, in case of the protection of the built infrastructure against explosive events, specialized engineers are required to intervene on the aspects of engineering design, such as:

- Resistance against progressive collapse. Increasing structural robustness by employing methodologies similar to the ones designed for resisting the effects of severe earthquakes.
- Resistance of glazing material. Increasing the performance of glass under blast loads. Its presence in nearly every building's façade and instant failure, due to its extreme fragility creating glazed fragments is responsible for a large fraction of the injuries and fatalities during explosive events. The use of laminated glass panels or anti-shatter films guarantees a higher resistance to blast loads and reduces the relevant risk.
- Protection of soft targets/people. Decrease the mortality rate for the public by enforcing a stand-off perimeter through the introduction of a combination of tailor-made active (access control, security guards, video surveillance etc.) and passive (stiff protective elements and barriers that are harmonically integrated into the surrounding urban environment) protection measures.

## 20.4 Key messages and challenges

Given the diverse targets and tactics selected by terrorists in their effort to cause victims and draw public attention, a multidimensional response is needed, one that includes innovative new approaches in the assessment of the relevant risk. A holistic and individualised risk evaluation approach is crucial for drawing together all terrorism-related data and providing tailor-made suggestions for effectively reducing and/or mitigating the risk of a terrorist attack. Past incidents may provide valuable information concerning the vulnerability of various sites, the potential consequences should an attack materialize, and common tactics used by the aggressors. Clearly, protection of all public spaces is impractical in both economic and technical terms, so a cost and benefit analysis needs to be followed for the zones that have to be protected and introduce an efficient protection plan with reduced installation and running costs.

Since a universally accepted risk assessment methodology for terrorism is still missing, efforts should focus on identifying potential threats utilizing available terrorism databases, evaluating the impact of potential attacks and assessing the vulnerability of targets. Terrorism-affected zone maps are available at country level, but breaking down the information to smaller regions is questionable, as the samples usually lack the statistical significance for drawing concrete conclusions. In high terrorist risk countries where many events have occurred in the past there may exist enough data, but in countries with hardly any attacks, as commonly observed in the western world, this approach leads to unreliable results. However, these zone maps may provide hints regarding the preferred terrorist tactics and potential targets, which are essential inputs for the vulnerability and consequences assessment procedure.

Using the number of fatalities and injuries for assessing the consequences of an attack is a rather straightforward process, as they can be easily measured from prior attacks or even calculated in certain cases (e.g. mortality rate after the explosion of an IED in a crowded place). The use of other parameters, such as the effect of assaults on public morale or the economic damage due to the disruption of services are hard to be measured since they do not constitute quantitative values. Nevertheless, the global targets set out by the Sendai Framework for the disaster risk management include indicators, some of which (e.g. economic loss, disruption of basic services etc.) may be employed during the impact assessment of a terrorist attack.

Finally, NRA strategies should be updated on a regular basis, since threat types and terrorist tactics alter with time. When reviewing terrorism risks different factors, such as the global and local political scene, religious tensions and the availability of potential weapons (explosives, vehicles, guns, biological agents etc.), should be considered. The various attack scenarios that may be examined during the risk evaluation process should be regularly reassessed and updated to be in line with the latest threat developments. Furthermore, the implementation of mitigation and protective measures need to follow, whenever possible, a security-by-design approach, so that the selected solutions may be harmonically integrated in the surrounding environment, reaching a proper balance between security and the protected asset's characteristics. These measures should focus on increasing the redundancy of the potential target in order to be effective for a variety of different threats and be also adequate for emerging risks.

## 20.5 References

- Control Risks Group Holdings Ltd, 2018, < <https://www.controlrisks.com/>>
- European Commission, 2017, Commission Staff Working Document, Overview of Natural and Man-made Disaster Risks the European Union may face, SWD (2017), Brussels, doi: 10.2795/861482, 2017.
- European Commission, 2015, The European Agenda on Security, COM(2015) 185.
- European Commission, 2017, Action Plan to support the protection of public spaces, COM(2017) 0612.
- European Commission Joint Research Centre, 2020, Europe Media Monitor, < <http://emm.newsbrief.eu/overview.html>>
- European Committee for Standardization (CEN) Eurocode 1: Actions on structures, Part 1-7: prEN 1991-1-7: "General actions-Accidental actions", 2006.
- IHS Markit, 2018, Jane's 360- Defence & Security Intelligence & Analysis, < <https://www.janes.com/>>
- Interagency Security Committee (ISC), The Risk Management Process for Federal Facilities, Department of Homeland Security, USA, 2016.
- ISO, 2009. ISO 31000: Risk management – Principles and guidelines
- ISO, 2018. ISO 31010: Risk management – Risk assessment techniques
- Larcher M., 2018, Security in Public Spaces, < <https://www.mrrb.bg/en/pts-security-in-public-spaces-martin-larcher-soft-target-public-spaces-vulnerability-assessment-and-protection/>>
- Migration and Home Affairs, 2018, Radicalisation Awareness Network-RAN, < [https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation\\_awareness\\_network\\_en](https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en)>
- Prevention Web, 2018, Sendai Framework for Action on Disaster Risk Reduction 2015-2030 < <https://www.preventionweb.net/drr-framework/sendai-framework-monitor/indicators>>
- University of Maryland, 2018, Global Terrorism Database, < <https://www.start.umd.edu/gtd/>>

## 21 Critical infrastructure disruptions

MARIANTHI THEOCHARIDOU, LUCA GALBUSERA, GEORGIOS GIANNOPOULOS

### 21.1 Introduction

In Council Directive 2008/114/EC, a Critical Infrastructure (CI) is defined as “an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions”<sup>163</sup>. In time, various characterizations and categorizations have been proposed for CIs, especially to promote their protection and resilience<sup>164</sup>.

When discussing risk assessment and related good practices in this context, we have to consider that both exogenous (e.g. natural, man-made) and endogenous (e.g. aging) factors may lead CIs to failure. Moreover, generally CIs play multiple roles during disasters and crises. In particular,

- they may be directly affected by critical events;
- the failure of a CI may provoke consequences and trigger emergencies;
- a CI may mediate response and mitigation actions<sup>165</sup>.

It is then interesting to evaluate how these three aspects are taken into account in current risk assessment practices.

Based on the latest Commission Staff Working Document on National Risk Assessment (NRA) results<sup>166</sup>, CI-related risk scenarios assessed by the majority of Member States (MSs) focus predominantly on the first two aspects. In particular, such scenarios refer to either: (a) major accidents or energy shortages or (b) infrastructure failures induced by other kinds of hazards. Several NRAs also assess potential infrastructure-to-infrastructure cascading effects, including cross-sectoral consequences. Besides, correlated hazards such as the loss of CIs or nuclear and industrial accidents have been linked to increased exposures to terrorism and cyber-risks. In this regard, a recent JRC report<sup>167</sup> identified some gaps in the way CIs are addressed during risk assessment processes performed by MSs. These findings were based on the NRA report published in 2015<sup>168</sup>, but similar observations can be made for recent NRAs, as reported in 2017<sup>169</sup>.

Since CIs mediate the flow of goods and allow the provision of essential services to the society, bolstering their resilience against critical events requires a comprehensive analysis of the failure-recovery cycle. To this end, it is often inadequate to evaluate the coping capabilities of an infrastructure in isolation. Exposures, for instance, may emerge from the accumulation of those specific to each asset, or be inherent to the way systems are interconnected. Global supply chains are one of the clearest examples in this sense, and they demonstrate how systemic vulnerabilities may enable cascading effects and amplify losses.

Interdependencies and associated risks are often complex to assess, due to the articulated geospatial layouts of CIs, their many mutual interactions, the integration of technological sectors and many other factors. Traditional asset-based, hazard-specific risk assessment methodologies are sometimes ineffective in coping with this challenge. On the other side, new trends emerge in this area, such as the so-called service-based approaches. These, instead of focusing on damages to specific assets, capture interdependencies on the basis of exchange of services between infrastructures of the same or different sectors.

---

<sup>163</sup> Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. URL: <https://eur-lex.europa.eu/eli/dir/2008/114/oj>.

<sup>164</sup> See [www.cipedia.eu](http://www.cipedia.eu).

<sup>165</sup> Rome E., Doll T., Rilling S., Sojeva B., Voß N., Xie J., The Use of What-If Analysis to Improve the Management of Crisis Situations Chapter 10 in: Setola R., Rosato V., Kyriakides E., Rome E. (Eds.): *Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach*, Springer, DOI 10.1007/978-3-319-51043-9\_10.

<sup>166</sup> Commission Staff Working Document on Overview of Natural and Man-made Disaster Risks the European Union may face, SWD(2017) 176 final, Brussels, 23.5.2017.

<sup>167</sup> Theocharidou M, Giannopoulos G, Risk assessment methodologies for critical infrastructure protection. Part II: A new approach, EUR 27332 EN, 2015.

<sup>168</sup> Commission Staff Working Document on Overview of Natural and Man-made Disaster Risks in the EU, SWD(2014) 134 final, Brussels, 8.4.2014.

<sup>169</sup> Commission Staff Working Document on Overview of Natural and Man-made Disaster Risks the European Union may face, SWD(2017) 176 final, Brussels, 23.5.2017.

In this sense, moving from the definition of risk proposed in standard ISO 31000:2009 (“effect of uncertainty in objectives”)<sup>170</sup> discusses the concepts of systemic risk (“the risk of having not just statistically independent failures, but interdependent”) and hyper-risk (“implied by networks of networks”). The same reference also points out some key shortcomings of current risk-assessment methods. These include poor estimates of probability distributions and parameters for rare events, underestimation of likelihoods of coincidence of multiple rare events, scarce accounting for feedback loops in fault/event tree analysis, insufficient consideration for joint probabilistic analysis and complex dynamics analysis, human/social factors, lack of questioning about established ways of thinking, economic/political/personal incentives.

Awareness about the aspect of interdependency and direct/indirect effects is also clear in standard ISO 31000:2018, which we will reference for our discussion on risk assessment phases<sup>171</sup> and, throughout most of this document, for risk-related terminology. In the standard’s definitions, for instance, term “consequences” receives a comprehensive interpretation, which includes both direct and indirect effects.

In the rest of this chapter, we will first overview some recent policy background relevant to CI risk, starting from the Sendai Framework for Disaster Risk Reduction 2015-2030, the European Union framework and some other significant experiences on a global scale. Secondly, we will introduce aspects of interest and good practices related to risk assessment for CIs, notably in risk identification, analysis and evaluation. Emerging trends interpret risk assessment as part of a broader, circular risk management process. We will, therefore, introduce techniques (frameworks, methodologies and tools) supporting this process in the case of CIs, also including the concept of resilience and the implementation of related strategies. Finally, we will discuss risk treatment and some important gaps and challenges that both policymakers and CI operators are facing today.

## 21.2 Policy background

The multi-dimensional aspect of disaster risk reduction in the case of CIs is taken into account with increasing emphasis in international policies and agreements. A notable example is found in the Sendai Framework for Action on Disaster Risk Reduction 2015-2030, which promotes actions devoted to reducing disaster losses in various areas and expressed in terms of lives as well as material/non-material damages. As part of the framework, Global Target D proposes to “substantially reduce disaster damage to critical infrastructure and disruption of basic services, among them health and educational facilities, including through developing their resilience by 2030”. More in details, the target articulates the aspect of “damage to critical infrastructures attributed to disasters” (target D1-compound) and “number of disruptions to basic services attributed to disasters” (target D5-compound). Interestingly, the latter conceptualization equally stresses the aspect of damage/disruption to assets and to services, which clearly binds with the discussion on interdependencies proposed above.

Observe that CIs are also mentioned in other portions of the Sendai Framework, notably in Global Target C. There, within the general framework of economic losses reduction (“reduce direct disaster economic loss in relation to global gross domestic product (GDP) by 2030”), target C5 refers to “direct economic loss resulting from damaged or destroyed CI attributed to disaster”. This is a case where consequences emerging from CI failing are taken into account, emphasizing once more the multiplicity of roles played by CIs in disaster scenarios.

At the EU level, the designation of CIs is accompanied by the attention to their protection and ability to withstand and overcome crises. However, the landscape within the EU remains diverse<sup>172</sup>. Indeed, the MSs follow different approaches with respect to CI designation, with the notable exception of the Energy and Transport sectors<sup>173</sup>, which are commonly accepted due to Council Directive 2008/114/EC. This diversity is also reflected in the associated best practices, such as the Operator Security Plan for designated infrastructures. Risk assessment is the cornerstone for the design of such plans at the CI level or at a sectoral level, and can be performed either by the CI operator, the sector regulator, or in a collaboration involving local or national authorities.

---

<sup>170</sup> Helbing, Dirk. “Globally networked risks and how to respond.” *Nature* 497.7447 (2013): 51.

<sup>171</sup> For further discussion on terminology, see also:

Theocharidou M., Giannopoulos G. 2015. Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. Report EUR 27332 EN, Luxembourg: European Union — Publications Office.

<sup>172</sup> Lazari, A. & Simoncini, M. (2016). Critical Infrastructure Protection beyond Compliance. An Analysis of National Variations in the Implementation of Directive 114/08/EC. *Global Jurist*, 16(3), pp. 267-289, doi:10.1515/gj-2015-0014.

<sup>173</sup> See [www.cipedia.eu](http://www.cipedia.eu) for the ‘Critical Infrastructure Sector’ per country.



Beyond the EU, USA's 'National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience'<sup>174</sup>, includes a CI risk management approach which can be applied to all threats and hazards, including cyber incidents, natural disasters, manmade safety hazards, and acts of terrorism. It is designed in a way that complements and supports the Threat and Hazard Identification and Risk Assessment (THIRA) process conducted by regional, State, and urban area jurisdictions. Similarly, the Canadian government recognizes that the impacts of disruptions can cross sectors and jurisdictions, and provides practical guidance for implementing a coordinated, all-hazards approach to CI risk management<sup>175</sup>.

As observed in <sup>176</sup>, "complementing traditional risk management, security, and protection practices, resilience gains a prominent role as the 'umbrella' term to cover all stages of crisis management. This aspect is also prominent in emerging EU policy trends, wherein CI resilience acquires increasing importance and links to a number of strategic priorities". Selected key policy documents at the EU level related to the topic include:

- Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism<sup>177</sup>;
- Green Paper on a European programme for critical infrastructure protection<sup>178</sup>;
- Communication from the Commission on a European Programme for Critical Infrastructure Protection<sup>179</sup>;
- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance)<sup>180</sup>;
- Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure<sup>181</sup>;
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union<sup>182</sup>;
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - An EU Strategy on adaptation to climate change<sup>183</sup>;
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - The European Agenda on Security<sup>184</sup>;
- Joint Communication to the European Parliament and the Council - Joint Framework on countering hybrid threats a European Union response<sup>185</sup>;
- Joint Communication to the European Parliament, the European Council and the Council - Increasing resilience and bolstering capabilities to address hybrid threats<sup>186</sup>;
- Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU<sup>187</sup>.

<sup>174</sup> <https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience#>

<sup>175</sup> Risk Management Guide for Critical Infrastructure Sectors, Public Safety Canada, July 2010. Available at: <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/rsk-mngmnt-gd/index-en.aspx>

<sup>176</sup> Theocharidou M., Galbusera L., Giannopoulos G. Resilience of critical infrastructure systems: Policy, research projects and tools. In Linkov I., Trump B., Florin M.V. (Eds.) IRGC Resource Guide on Resilience (volume 2) Domains of Resilience for Complex Interconnected Systems in Transition, to appear, 2018.

<sup>177</sup> [COM/2004/0702 final](#)

<sup>178</sup> [COM/2005/0576 final](#)

<sup>179</sup> [COM/2006/0786 final](#)

<sup>180</sup> [Directive \(EU\) 2016/1148](#)

<sup>181</sup> [SWD\(2013\) 318 final](#)

<sup>182</sup> [Directive \(EU\) 2016/1148](#)

<sup>183</sup> [COM/2013/0216 final](#)

<sup>184</sup> [COM/2015/0185 final](#)

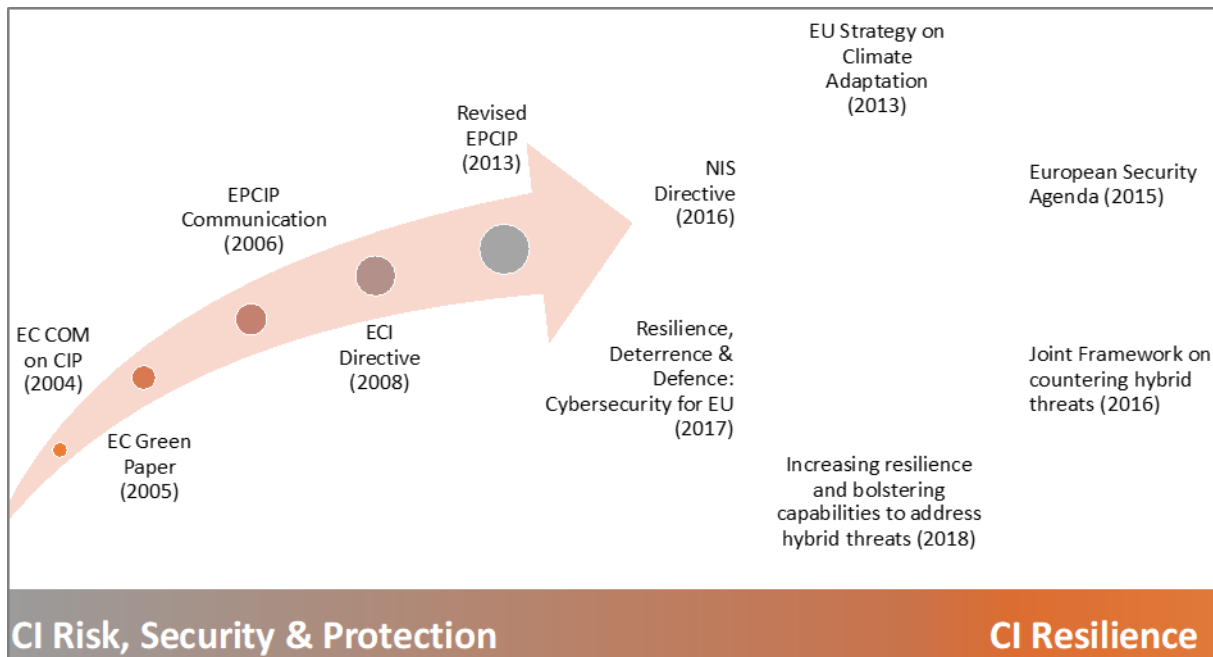
<sup>185</sup> [JOIN/2016/018 final](#)

<sup>186</sup> [JOIN/2018/16 final](#)

<sup>187</sup> [JOIN/2017/0450 final](#)

**Figure 56** illustrates the conceptual evolution of the emerging policies from the context of CI risk, security and protection to that of CI resilience. The EU-funded H2020 IMPROVER project<sup>188</sup> uses the following definition of CI resilience: “the ability of a CI system exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, for the preservation and restoration of essential societal services.”<sup>189</sup> However, through six interactive workshops with infrastructure operators organized by the IMPROVER project, what has become apparent is that the definition of resilience isn’t what matters; what does matter is the way resilience changes the outlook of operators<sup>190</sup>. Indeed, resilience is an optimistic approach when compared to current risk management practices, allowing operators to be actors in responding to crises, as opposed to simply being subjects exposed to risks.

**Figure 56:** EU policy milestones towards the resilience of CIS.



Source: Theocharidou et al, 2018<sup>191</sup>.

From the perspective of CI protection, there are main two schools of thought regarding the relationships between risk management and resilience management<sup>192</sup>. Some see resilience management as part of risk management; others interpret resilience management as a separate process. Regardless of the most correct interpretation, considering the relationships between these two concepts is unavoidable when discussing CI resilience. Indeed, in many respects both approaches find justification. Resilience management can be a separate process with respect to risk management, while it can also be performed in a way such that the two processes enrich and support each other. At the time of writing, a proposal for a new ISO resilience standard is being prepared under the ISO 31000 family of standards on risk management, exploring the potential benefits of a resilience-based approach. Moreover, many of the methods, frameworks and tools described below in this chapter implement risk approaches which comprise resilience elements as well.

<sup>188</sup> [www.improverproject.eu](http://www.improverproject.eu)

<sup>189</sup> The definition has been adapted from: 2009 UNISDR Terminology on Disaster Risk Reduction, United Nations International Strategy for Disaster Reduction (UNISDR), Geneva, Switzerland, May 2009.

<sup>190</sup> Petersen L., Theocharidou M., Lange D., & Bossu R. (2018). Who cares what it means? Practical reasons for using the word resilience with critical infrastructure operators. The Third Northern European Conference on Emergency and Disaster Studies (NEEDS 2018).

<sup>191</sup> Theocharidou M., Galbusera L., Giannopoulos G. Resilience of critical infrastructure systems: Policy, research projects and tools. In Linkov I., Trump B., Florin M.V. (Eds.) IRGC Resource Guide on Resilience (volume 2) Domains of Resilience for Complex Interconnected Systems in Transition, to appear, 2018.

<sup>192</sup> Theocharidou M., Lange D., Storesund K. (2018). Guideline on implementation of organisational, societal and technological resilience concepts to critical infrastructure, IMPROVER D5.2, September 2018.

## 21.3 Risk assessment

According to ISO 31000:2018, risk assessment is the overall process comprising risk identification, risk analysis and risk evaluation. However, when applying such a standard to the case of CIs, there are some issues that pose challenges or require particular consideration.

### 21.3.1 Defining the scope

A risk assessment related to CIs can be performed at various levels:

- at the level of specific infrastructures, typically conducted by the CI operator;
- at the sector level, conducted by governmental authorities or the sector's regulator with input by the CI operators; or
- at local (e.g. for a city) or national (e.g. as part of the NRA) level, where the process should involve all relevant authorities and stakeholders.

#### Goal definition

In general, the goal of the assessment could be to identify those critical components where potential consequences would be highest and where security and resilience enhancement activities can be mainly focused. It is clear that, depending on the level of analysis, such goals are likely to vary across sectors, organizations, and policymakers. CI operators may view criticality or risk differently, as their goals relate to their operations, while a policymaker's goals may relate more to public needs and priorities.

#### Stakeholder identification

In all cases, when focusing on infrastructures, the consequences to the society and the presence of interdependencies are parameters that highlight the importance of collaboration. An important step is, therefore, to identify and engage all stakeholders relevant to the assessment.

#### CI identification

Another key step is the identification of the CIs to be included in the analysis. As we briefly mentioned in the previous section, different countries have different interpretations about what is considered to be critical. Some practices in this domain include<sup>193</sup>:

- adopting definitions of CI sectors and services from other countries;
- introducing methodologies to identify CI sectors and services systematically;
- performing (national and cross-border) dependency analysis.

#### Data collection challenges

One of the early questions to be faced, even in defining the scope of the assessment, is whether or not adequate data support can be provided. A number of actions have been completed or are ongoing in order to address the availability of data relevant to risk assessment, for instance through initiatives such as the OFDA/CRED International Disaster Database EM-DAT<sup>194</sup> and JRC's Risk Data Hub<sup>195</sup>.

Risk analysis data requirements vary depending on the situation and the tasks to be completed, spanning from prevention measures to real-time status assessment and decision making just after a critical event has hit a region. Different information sources may complement each other in order to address the various situations more comprehensively (e.g. institutional information, crowd-sourced crisis information).

---

<sup>193</sup> The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers, Luijif E. (Ed.), 2017. Available at: <https://www.thegfce.com/documents/reports/2017/10/22/the-gfce-meridian-good-practice-guide-on-critical-information-infrastructure-protection-for-governmental-policy-makers>.

<sup>194</sup> This resource provides disaster information for an extensive and increasing number of disasters. In particular, "the main objective of the database is to serve the purposes of humanitarian action at national and international levels. The initiative aims to rationalise decision making for disaster preparedness, as well as provide an objective base for vulnerability assessment and priority setting". URL: <https://www.emdat.be/>.

<sup>195</sup> This platform "adopts the comprehensive framework of policies and guidelines, data sharing initiatives and spatial data infrastructure with the purpose of setting the bases for knowledge for DRM at local, national, regional and EU-wide level". The platform also comes with a collection of good practices to the development of risk web-platforms and risk data. Data are available at different levels of aggregation, while country corners allow MS to manage their own risk assessment, covering both the prevention and preparedness assessment and the response and recovery assessment. URL: <https://drmkc.jrc.ec.europa.eu/risk-data-hub>.

Moreover, best practices in the area of risk data management are also developed in the private sector. Often, these also manifest a need for smoother interaction with regulatory bodies and partnering entities. Indeed, guidelines for the creation of sound infrastructure risk data and management methods can be found in the experience of CI operators. For example, four aspects are identified in <sup>196</sup> for achieving effective risk data infrastructures in the financial sector:

- efficiency, which may be affected by siloed and incompatible data, while suffering from the more time is spent on data management than on risk treatment;
- flexibility, needed in order to provide quick response with limited manual work, when non-standard scenario analysis and reports are needed, or when regulators request information;
- quality, which can be compromised by incompatible definitions, inconsistency, incompleteness, and duplication;
- ownership, which expresses the need for risk governance, accountability and commitment to quality, especially when data are collected by multiple stakeholders.

Finally, observe that concerns have also been raised about the public availability of CI data, which in some cases might represent a threat in itself<sup>197</sup>.

### **21.3.2 Risk Identification**

The purpose of this stage is to identify and describe the risks that may or are expected to affect a CI or a CI sector. Sources for the selection of scenarios of interest include:

- events that may affect the functionality of the CI;
- vulnerabilities of the CI (e.g. its age or location);
- indicators of emerging risks;
- intelligence information for man-made threats;
- time-related factors, etc.

An all-hazards approach to risk management does not mean that all hazards will be assessed, evaluated and treated, rather that all hazards will be considered. When analysts are developing scenarios to identify potential risks for an assessment, these should be selected in such a way as to cover the full scope of the assessment.

It is important to observe that service loss for a CI can result from:

- causes inherent to the infrastructure (e.g. technical failures, accidents, aging),
- external causes (hazards, man-made threats), or
- the service loss of another infrastructure.

In some cases, relevant scenarios can be driven not only by service loss but also by increased demand for service provision, as in the case of an emergency.

### **21.3.3 Risk Analysis**

At a minimum, risk analysis should determine:

- the likelihood of the threat or hazard; and
- the consequences of the threat or hazard, taking into account the disruption of critical services and products.

---

<sup>196</sup> KPMG, Rebuilding and reinforcing risk data infrastructure. An extract from KPMG's Frontiers in Finance. April 2014. Available at: <http://kpmg.com/frontiersinfinance>.

<sup>197</sup> Abbas, R, The Threat of Public Data Availability on Critical Infrastructure Protection (CIP), and the Level of Awareness Amongst Security Experts in Australia, Bachelor of Information and Communication Technology (Honours), University of Wollongong, 2006, 129p.

For CIs, risk often includes the frequency of service loss and the resulting consequences for the concerned people<sup>198</sup>. Important factors to consider include complexity (CI interdependency), time-related factors and the effectiveness of existing controls. By definition, CIs provide essential services to the public, and their disruption is associated with significant consequences. The emphasis of an assessment is often placed more on the consequences when CIs fail to some degree, with a lack for precise definitions about the cause and the associated probabilities. Regardless of the initiating factor, CI operators often mostly focus, for their planning or training, on the consequences of service loss. This allows them to plan and exercise against disruptions of unknown probability and to focus more on the effects to the service provision.

When assessing the consequences of CI loss or failure, one should not only consider economic aspects such as the reconstruction costs or the expenses for building or system recovery, but also the effects of service inoperability on the population or a country. For example, FP7 project Casceff considers various types of consequences from infrastructure failures<sup>199</sup>. In particular,

- technical consequences encompass the damage and loss of technical components and physical assets, loss of production etc.;
- organizational consequences relate to the organisations and institutions that manage the systems (CI owners or operators), encompassing impacts on organisational capacity, coordination, and information management, etc.;
- social consequences encompass impacts on the community, such as political instability and civil unrest;
- human consequences are about impacts on population such as health-issues, reduced well-being, casualties and injuries;
- economic consequences encompass impacts in terms of direct costs;
- environmental consequences relate to the effects on natural resources, flora and fauna.

Secondly, as we mentioned above, CIs can be affected by a hazard. As an example of direct effects caused by a flood scenario, FP7 project CIPRNet considers and identifies the following possible disruptions<sup>200</sup>:

- transport disruptions due to flood-related accidents (derailment, collision of road vehicles);
- collision of maritime vehicles, structural elements collapse or overflow, e.g. tunnels, bridges, airports etc.;
- transport disruptions due to large-scale evacuation of civilian causing traffic congestion;
- disruptions of water supply or contamination of drinking water or other health hazards;
- hazardous substances (CBRN) incidents due to structural damages/flooding on facilities;
- hazardous substances (CBRN) incidents due to accidents to transporting vehicles;
- collapse of sewage systems;
- electrical power supply disruptions;
- telecommunications disruptions;
- medical care facilities disruptions, due to power shortage, flooding, increased number of patients or inability of the personnel or supplies to reach the location;
- industrial or business disruptions, due to power or communication disruptions.

Here observe that a flood can cause multiple damages to CIs of various sectors (e.g. transport, ICT, energy), beyond the direct consequences to the population. These may refer to damages to a specific building or infrastructure element, and they are calculated based on exposure of the element to the hazard and its vulnerability level. While the list is not exhaustive and these disruptions are unlikely to happen all simultaneously, they highlight the complexity of mapping the direct and indirect effects of a scenario to

---

<sup>198</sup> E. Zio, Challenges in the vulnerability and risk analysis of critical infrastructures, *Reliability Engineering and System Safety* 152 (2016) 137–150.

<sup>199</sup> [http://casceff.eu/media2/2016/02/D2.1-Deliverable\\_Final\\_Ver2\\_PU.pdf](http://casceff.eu/media2/2016/02/D2.1-Deliverable_Final_Ver2_PU.pdf)

<sup>200</sup> Y. Barbarin, M. Theocharidou, and E. Rome, "CIPRNet deliverable D6.2: Application scenario," CEA, JRC, Fraunhofer IAIS, Tech. Rep., May 2014. [Online]. Available at: <https://www.ciprnet.eu/>.

national CIs. An additional parameter to consider is whether the disruptions described above can hinder the emergency response capabilities. For example, the disruption of transportation nodes can delay assistance in reaching affected areas, and potentially amplify the consequences to the population.

Calculating the overall societal impact of a scenario is a difficult process, especially in cases when parallel disruptions take place or double counting of losses is difficult to avoid, likely leading to poor quality impact estimations. The case of previous incidents may allow for more realistic assessments, but this is not always the case when examining unknown or rare events.

As a third point, cascading effects between infrastructures need to be considered<sup>201</sup>. The impact of a disruption, or failure, may spread both geographically and across multiple sectors. The 2017 World Economic Forum's Global Risks Report<sup>202</sup> observes that *"greater interdependence among different infrastructure networks is increasing the scope for systemic failures – whether from cyberattacks, software glitches, natural disasters or other causes – to cascade across networks and affect society in unanticipated ways"*. This observation highlights a key parameter with respect to CIs that should be considered when performing a NRA.

Identifying dependencies is, therefore, an important task<sup>203</sup>. While various classifications of dependencies can be found in the literature<sup>204</sup>, such as physical, geographical, cyber, social, etc., a more recent empirical study<sup>205</sup>, shows that events can be classified as cascade-initiating (i.e., an event that causes an event in another CI), cascade-resulting (i.e., an event that results from an event in another CI), and independent (i.e., an event that is neither a cascade-initiating nor a cascade-resulting event). The empirical findings indicate that:

- cascade-resulting events are more frequent than generally believed, and that cascade initiators are about half as frequent;
- dependencies are more focused and directional than often thought;
- energy and telecommunications are very frequent cascading initiating sectors.

A JRC report observed the lack of CI dependency modelling and analysis in most NRAs<sup>206</sup>. This is also highlighted by<sup>207</sup>, which includes *"dependencies and interdependences identification and modelling"* and *"dynamic analysis (including cascading failures)"* as two of the steps required in CI vulnerability and risk analysis (*"hazards and threats identification"* and *"physical and logical structure identification"* are also part of the approach). If MSs select to perform a risk assessment method that considers both dependencies among CIs and the direct or indirect consequences of hazards, then the method for analysing a risk scenario needs to include more steps and iterations, as illustrated in **Figure 57**.

Such an approach would allow to establish closer links between Disaster Management or Civil Protection and Critical Infrastructure Protection within a MS or across MSs, when examining hazards of cross-border scale.

### 21.3.4 Risk evaluation

The purpose of risk evaluation is to support decisions. In general, the output of this step includes a prioritized list of risks, information gaps, and lessons learned. The outcome of risk evaluation should be recorded, communicated and then validated by the decision-makers. In the case of CIs, this step allows to focus on critical assets or services, and amend plans for their protection and resilience. It is the basis to create a plan with short-term and long-term actions that need to be taken to mitigate risk. It can also be the input for national funding or the trigger for a new regulation.

---

<sup>201</sup> L. Franchina, M. Carbonelli, L. Gratta, M. Crisci and D. Perucchini, An impact-based approach for the analysis of cascading effects in critical infrastructures, *International Journal of Critical Infrastructures*, vol. 7(1), pp. 73–90, 2011.

<sup>202</sup> <https://www.weforum.org/reports/the-global-risks-report-2017>

<sup>203</sup> Setola, R., Theocharidou, M. (2016). Modelling Dependencies Between Critical Infrastructures. In: R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures*, *Studies in Systems, Decision and Control* 90, DOI 10.1007/978-3-319-51043-9\_2.

<sup>204</sup> Rinaldi SM, Peerenboom JP, Kelly TK (2001) Critical infrastructure interdependencies. *IEEE Control Syst Mag*, 11–25.

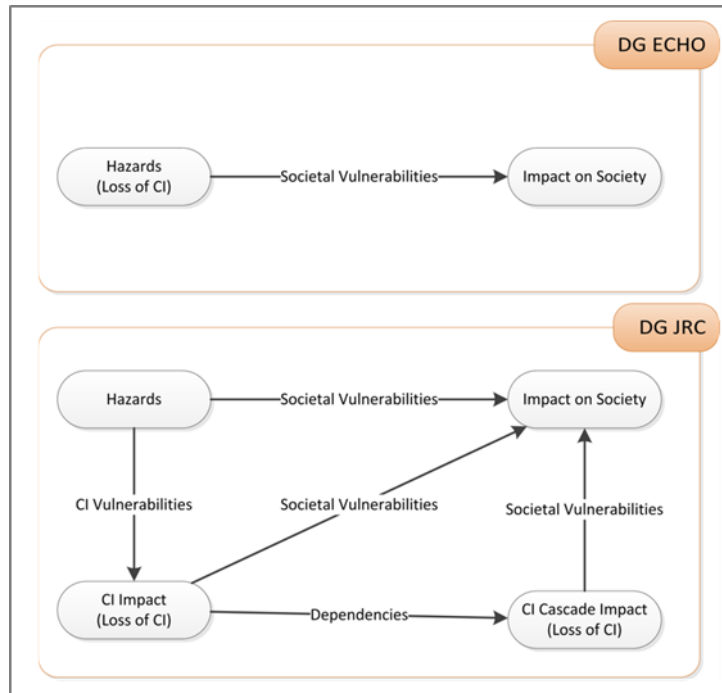
De Porcellinis S, Panzieri S, Setola R (2009) Modelling critical infrastructure via a mixed holistic reductionistic approach. *Int J Crit Infrastruct* 5(1–2):86–99.

<sup>205</sup> Van Eeten M, Nieuwenhuijs A, Luijff E, Klaver M, Cruz E (2011) The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports. *Public Adm* 89(2):381–400.

<sup>206</sup> Theocharidou M, Giannopoulos G, Risk assessment methodologies for critical infrastructure protection. Part II: A new approach, EUR 27332 EN, 2015. Available at: <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96623/lbna27332enn.pdf>.

<sup>207</sup> Zio, Enrico. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety*. 152. 137–150. 10.1016/j.ress.2016.02.009.

**Figure 57: Risk Assessment for CI Loss.**



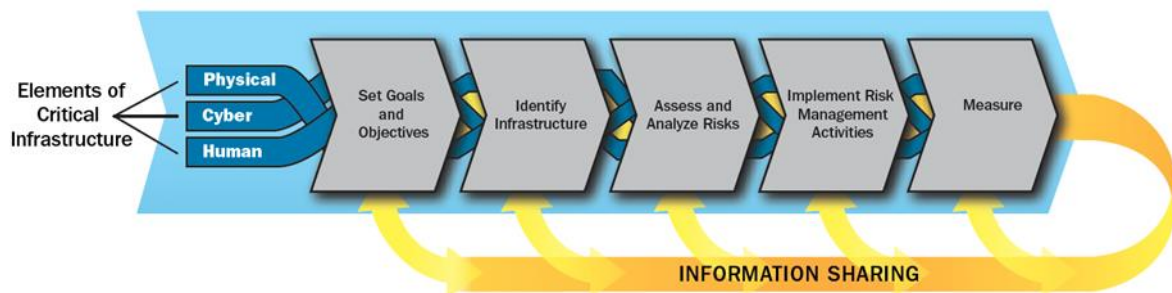
Source: Theocharidou and Giannopoulos, 2015 <sup>208</sup>.

See also reference<sup>209</sup> for a comparative analysis of risk assessment methods for CIs, with an emphasis on security. Therein, the authors discuss both institutional risk assessment standards (NIST risk assessment framework SP800-30/30rev1, ISO/IEC 27 005:2008 and BS-7799-2006) and enterprise models (OCTAVE, Fair, Microsoft).

## 21.4 Frameworks, methodologies and tools

In the previous section, referring to the ISO 31000:2018 standard's risk assessment framework, we discussed some key elements that contextualize this process to CI risk assessment. Similar aspects can be traced in other risk management frameworks, including those specifically devoted to CIs. For instance, in **Figure 58** we report a representation of the NIPP's Critical Infrastructure Risk Management Framework.

**Figure 58: NIPP's Critical Infrastructure Risk Management Framework**



Source: US Department of Homeland Security, 2013 <sup>210</sup>

<sup>208</sup> Theocharidou M, Giannopoulos G, Risk assessment methodologies for critical infrastructure protection. Part II: A new approach, EUR 27332 EN, 2015. Available at: <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96623/lbna27332enn.pdf>.

<sup>209</sup> Tweneboah-Koduah, Samuel, and William J. Buchanan. "Security Risk Assessment of Critical Infrastructure Systems: A Comparative Study." *The Computer Journal* (2018).

<sup>210</sup> NIPP 2013 Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach, US Department of Homeland Security, 2013.



In many of the merging contributions about CI risk management, there is an attempt to cope with the diversity of perspectives and to offer support all along the failure/recovery processes, through a circular process striving for improved response to risk. In this sense, as mentioned above in this chapter, emerging policies, methodologies and studies in the CI domain stress the importance of the overall risk management process and the aspect of resilience<sup>211</sup>.

Therefore, in the rest of this section, we discuss methodologies, frameworks and tools significant to risk management and resilience enhancement processes for CIs<sup>212</sup>. It has to be observed that some of the tools in place are not limited to the risk assessment step, but instead reach the full extent of the risk management process.

### 21.4.1 Frameworks

A number of frameworks are in place to tackle the broader risk management process and, to some extent, resilience enhancement. Many of the existing methodologies emphasize the convergence of competences, the cyclic nature of assessment and the implementation of multistep evaluation procedures. In a number of cases, the scope of such frameworks also includes the provision of practical guidance, to support the formulation and actuation of risk and resilience assessment initiatives relative to either specific CIs or the same in a broader context, such as at regional levels.

While an exhaustive review of the existing frameworks is out of the scope of this chapter, next we describe some instances of recent proposals in this domain. Our examples are partly drawn from ongoing research projects and partly from institutional initiatives.

#### **National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience**

The 2013 NIPP<sup>213</sup> “elevates security and resilience as the primary aim of critical infrastructure homeland security planning efforts”. It “focuses on establishing a process to set critical infrastructure national priorities determined jointly by the public and private sectors”. In formulating the framework, reference is made to the DHS Risk Lexicon – 2010 Edition<sup>214</sup>. Additional documents that aim at facilitating the implementation of the plan are:

- supplement “*Executing a Critical Infrastructure Risk Management Approach*”, which offers practical guidance towards the construction of CI risk management approaches comprising the following activities: set goals and objectives; identify infrastructure (including the cyberinfrastructure); assess and analyse risks (through documented, reproducible and defensible assessments); implement risk management activities; measure effectiveness (also towards continuous improvement);
- supplement “*Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community*”, which outlines a “multidirectional, decentralized network of formal and informal channels through which government entities and the private sector share information”.

An important aspect of NIPP 2013 is the collaborative dimension of CI security and resilience, which calls for a “*partnership-based collective action*”. As such, it involves the delivery of training courses and other initiatives, such the security and resilience challenges issued to foster the cohesion and the capabilities of the CI community<sup>215</sup>.

#### **NIST Community Resilience Planning Guide for Buildings and Infrastructure Systems**

The guide<sup>216</sup> has been created with the objective “to help communities address these challenges through a practical approach that takes into account community social goals and their dependencies on the ‘built environment’ – buildings and infrastructure systems”. The proposed six-step process to planning for

<sup>211</sup> See also the Resource Guide on Resilience (available at <https://irgc.org/risk-governance/resilience>) by the International Risk Governance Council, whose first volume has been issued in 2016 and whose second volume is in preparation. This is “*an edited collection of authored pieces comparing, contrasting and integrating risk and resilience with an emphasis on ways to measure resilience*”, and it contains various resources relevant to the case of CIs.

<sup>212</sup> See also <https://www.dhs.gov/critical-infrastructure-resources> for a list of further CI resources.

<sup>213</sup> <https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience>

<sup>214</sup> <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>

<sup>215</sup> <https://www.dhs.gov/nipp-challenge>

<sup>216</sup> <https://www.nist.gov/topics/community-resilience>



community resilience comprises the following aspects: form a collaborative planning team; understand the situation; determine goal and objectives; plan development; plan preparation, review, and approval; plan implementation and maintenance.

The planning guide is organized into two volumes, wherein the first volume addresses the steps of the process in details and including practical examples, while the second volume contains support information and deals with the social dimension of resilience, as well as the aspect of buildings/CI interdependencies.

### NIST Framework for Improving Critical Infrastructure Cybersecurity

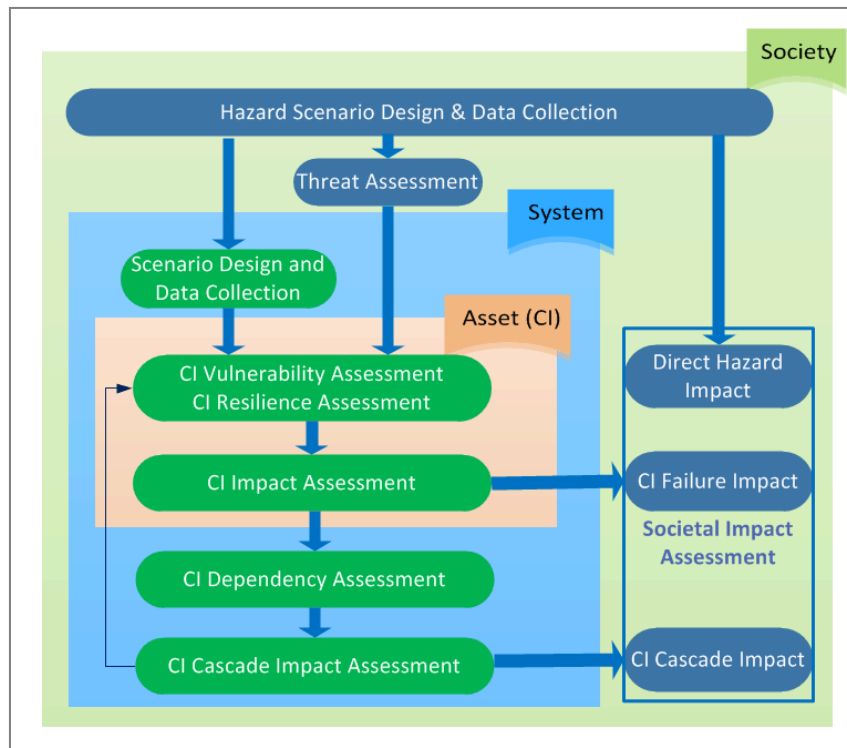
The Cybersecurity Framework<sup>217</sup> (v.1.1, April 2018) “focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes”. A joint related document is the NIST Roadmap for Improving Critical Infrastructure Cybersecurity.

Based on the NIPP Risk Management Framework and the NIST Framework for Improving Critical Infrastructure Cybersecurity, Department of Homeland Security (DHS) risk assessments have been issued<sup>218</sup> for the assessment of threat-vulnerability-consequence triads relative to selected CI sectors. These operations see the involvement of multiple DHS offices and take into account sector-specific regulatory environments.

JRC’s CRITICAL Infrastructures & Systems Risk and Resilience Assessment Methodology (CRISRRAM)

The CRISRRAM methodology developed at the JRC<sup>219</sup> proposes a generic approach that could be applied by MSs for their NRA scenarios. As illustrated in **Figure 59**, it involves the asset, system and society levels and it designs a multistep, cyclic assessment procedure leading to the evaluation of impacts of various nature.

**Figure 59:** Critical Infrastructures & Systems Risk and Resilience Assessment Methodology.



Source: based on Theocharidou and Giannopoulos, 2015<sup>220</sup>

The first step is to define a hazard scenario that may directly have an impact on the society (e.g. flooding, earthquake) but, at the same time, may impact a CI (Society Layer). As described in the NRA guidelines, risk is

<sup>217</sup> <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

<sup>218</sup> <https://www.gao.gov/assets/690/688028.pdf>

<sup>219</sup> Theocharidou M, Giannopoulos G, Risk assessment methodologies for critical infrastructure protection. Part II: A new approach, EUR 27332 EN, 2015.

<sup>220</sup> Theocharidou M, Giannopoulos G, Risk assessment methodologies for critical infrastructure protection. Part II: A new approach, EUR 27332 EN, 2015.

calculated according to a risk matrix, based on threat likelihood and (societal) impact assessment. However, this approach also considers impacts due to the failure of a CI or other dependent ones (cascade impact). These are assessed based on the direct impact of the threat on a CI (Asset Layer) or due to the indirect impact of the hazard to other CIs (System Layer).

Direct impact on one or more directly affected CI (Asset Layer), can be calculated on the basis of historical data, the results of vulnerability assessment of the CI or the presence of resilience mechanisms, in collaboration with CI operators or owners. This is usually assessed in terms of inoperability level or economic loss per asset. This direct effect to each CI – i.e. service degradation, disruption or failure – is related to an impact at the societal level. If this is not the case, then this infrastructure should not be considered as a CI at first hand. This approach to assessment links asset level disruptions with societal impact. In the System Layer, dependency assessment is introduced in the risk assessment framework. Identifying and assessing dependencies can allow a MS to take into account the additional impact from the cascading failure relative to other CI/sectors. However, one limitation to consider is the presence of cyclic dependencies among infrastructures, which may lead to a limited-quality estimation of impacts at the societal level.

### **IMPROVER project's Critical Infrastructure Resilience Framework (ICI-REF)**

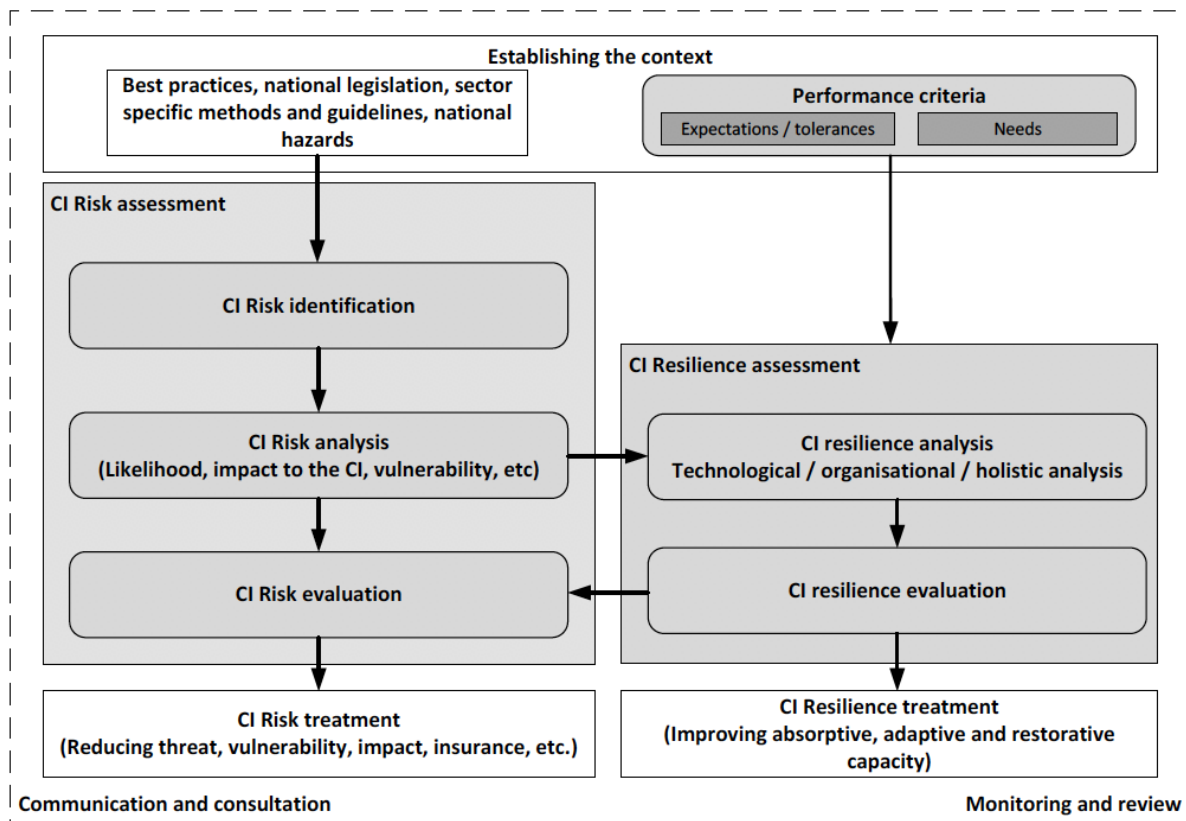
H2020 project IMPROVER (*“Improved risk evaluation and implementation of resilience concepts to Critical Infrastructure”*) considers the relationship between a CI risk analysis and a CI resilience analysis and tries to link the two aspects, proposing an approach that could also inform NRAs<sup>221</sup>. This framework, ICI-REF, aims at addressing *“the integrated process of risk and resilience management”*<sup>222</sup>. In particular, it maps resilience management to the risk management process from ISO 31000:2018 discussed above in this chapter. See **Figure 60** for an illustration.

---

<sup>221</sup> Lange, D. et al. (2017b). Incorporation of resilience assessment in Critical Infrastructure risk assessment frameworks, In: Safety and Reliability – Theory and Applications, ISBN 978-1-138-62937-0, p. 1031-1038.

<sup>222</sup> Lange et al. IMPROVER Deliverable 5.1 Framework for implementation of resilience concepts to Critical Infrastructure, 2017. Available at: [www.improverproject.eu](http://www.improverproject.eu).

**Figure 60:** ICI-REF: integration of resilience management in risk management



Source: Lange et al, 2017 <sup>223</sup>

Establishing the context is the first stage in both risk and resilience management, and this includes the identification of best practices as well as national or sector-specific legislations and methods of interest. It also comprises the identification of any nationally identified hazards which may be relevant for the considered infrastructure. While establishing the context, it is also needed to identify the evaluation criteria to be applied. These could be based, for instance, on land use planning curves in the case of risk evaluation. For resilience evaluation, assessment criteria might be based on societal tolerances, past performance, or minimum quality/quantity of service for a community to survive. Establishing the context acts as input to both the risk assessment process and the resilience assessment process, regardless of whether these processes are undertaken independently of one another or not. Risk identification only needs to be done as part of the risk assessment process, as some resilience assessment methodologies are independent of hazards and, thus, the risk assessment phase does not actually contribute here.

Typically, a risk evaluation would determine whether or not the assessed risk is below an acceptable threshold or if remedial action is necessary. While risk assessment has a focus on the consequences of an incident, resilience goes beyond, to include the recovery phase. Resilience evaluation, therefore, can be used to enrich the risk evaluation process. Risk treatment and resilience treatment are independent processes achieving different objectives. In the case of risk treatment, the objective is the reduction of threat, vulnerability, impact and, indeed, it can affect associated costs such as insurance premiums. In the case of resilience treatment, the objective is to improve the absorptive, adaptive or restorative capacity of the infrastructure. The implementation of this framework can be done by selecting appropriate tools or methodologies for the different stages.

<sup>223</sup> Lange et al. IMPROVER Deliverable 5.1 Framework for implementation of resilience concepts to Critical Infrastructure, 2017. Available at: [www.improverproject.eu](http://www.improverproject.eu).

## 21.4.2 Methodologies

A number of risk assessment methodologies relevant to CIs have been thoroughly reviewed in <sup>224</sup>. Moreover, a recent classification was proposed in<sup>225</sup>, where the following aspects were taken into consideration:

- purpose: risk identification, risk assessment, risk prioritization, risk mitigation planning, and effectiveness evaluation (following the phases of the NIPP framework);
- technical modelling approach: empirical approaches, system dynamics based approaches, agent based approaches, network based approaches, and other approaches<sup>226</sup>.

We will now briefly make reference to some key methodologies addressing the various areas of the risk and resilience management process. The presentation is articulated in accordance with the stages of the CRISRRAM framework discussed above; see also <sup>227</sup> for further details and references about many of the mentioned projects and methodologies.

### Scenario Design and Data Collection

We observe that only a limited number of existing methods and tools focus on designing scenarios. One such example is the Risk and Vulnerability analysis (RVA) by DEMA<sup>228</sup>, which dedicates a specific step to scenario design. Most methods usually address particular, predefined threat scenarios or apply the same methodology for selected case scenarios. Only in limited cases threat likelihood assessment is included (e.g. COUNTERACT, DECRIS, EURACOM, BMI, CIPDSS, etc.). A scenario-based approach to NRA was both recommended by DG-ECHO and applied by several MSs. It is also supported by the DHS guidelines for National CI Risk Management<sup>229</sup>. A clever definition of scenarios is considered a means to tackle the complexity of the problem; a key objective is to *“divide the identified risks into separate pieces that can be assessed and analysed individually”*. The use of such scenarios should identify which infrastructures are more critical (potential consequences would be highest) and also where security and resilience activities should be focused more<sup>230</sup>.

### CI Vulnerability assessment

Regarding vulnerability assessment, the BIRR method introduces the concept of Vulnerability Index (VI) and Protective Measures Index (PMI), CARVER assesses the accessibility to a physical location, COUNTERACT evaluates the safeguards in place for the corresponding risks for the various assets, DECRIS uses a vulnerability analysis step to identify which threats should be examined further, and RVA follows a qualitative five-levels scale for vulnerability assessment. The Sandia Risk Assessment Methodology takes into account the protection system effectiveness, expressed in terms of its ability to reduce the threat success probabilities.

### CI Resilience Assessment

---

<sup>224</sup> Giannopoulos G., Filippini R., Schimmer M., “Risk assessment methodologies for critical infrastructure protection. part I: A state of the art,” European Commission, Tech. Rep. EUR 25286, 2012.

<sup>225</sup> Stergiopoulos G., Vasilellis E., Lykou G., Kotzanikolaou P. and Gritzalis D. Classification and Comparison of Critical Infrastructure Protection Tools. M. Rice and S. Shenoi (Eds.): Critical Infrastructure Protection X, IFIP AICT 485, pp. 239–255, 2016. doi: 10.1007/978-3-319-48737-3\_14

<sup>226</sup> This is based on a classification by:

Ouyang, M.: Review on modeling and simulation of interdependent critical infrastructure systems, Reliability Engineering and System Safety, vol. 121, pp. 43–60 (2014).

Empirical approaches analyse interdependencies *“according to historical accident or disaster data and expert experience”*; system dynamics approaches *“take a top-down method to manage and analyse complex adaptive systems involving interdependencies”*; agent-based approaches *“adopt a bottom-up method and assume the complex behaviour or phenomenon emerge from many individual and relatively simple interactions of autonomous agents”*; network based approaches *“describe the interdependencies by interlinks”*, with the associated possibility to portray connectivity and flows. Finally, the other approaches mentioned in (Stergiopoulos et al., 2016) summon a number of additional techniques, including economic interdependency models and various other methods.

<sup>227</sup> Giannopoulos G., Filippini R., Schimmer M., “Risk assessment methodologies for critical infrastructure protection. part I: A state of the art,” European Commission, Tech. Rep. EUR 25286, 2012.

<sup>228</sup> [http://brs.dk/eng/inspection/contingency\\_planning/rva/Pages/vulnerability\\_analysis\\_model.aspx](http://brs.dk/eng/inspection/contingency_planning/rva/Pages/vulnerability_analysis_model.aspx)

<sup>229</sup> “Supplemental tool: Executing a critical infrastructure risk management approach,” U.S. Department of Homeland Security, Tech. Rep., 2013. [Online]. Available at: <http://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf>.

<sup>230</sup> Haimes YY, Jiang P (2001) Leontief-based model of risk in complex interconnected infrastructures. J Infrastruct Syst 1–12.

In terms of CI resilience assessment<sup>231</sup>, BIRR introduces a Resilience Index (RI) to provide an evaluation of how resilient an asset is, based on Robustness, Resourcefulness and Recovery mechanisms. CARVER2 similarly considers the presence of redundancy mechanisms, even if resilience is not explicitly mentioned. RAMCAP-Plus includes a Risk and Resilience Management step, highlighting how central this aspect is in the methodology.

### CI Consequence Assessment/CI dependency assessment

Interdependencies are covered by most methods being proposed, as this is a key feature for CIs. At the same time, the techniques involved and the level of detail varies significantly from case to case. Indirect consequences needing to be assessed include the social and economic costs inflicted to the society by the unavailability (or scarce availability) of essential services. One way to assess consequences is based on Service Availability Wealth (SAW) Indexes, which are implemented in CIPRNet's Decision Support System<sup>232</sup>. These indexes refer to perceived societal consequences expressed in terms of "*reduction of wealth*" in various societal domains: citizens, availability of primary services, economic sectors and the environment. SAW indexes indicate the relevance of a specific service supplied by a CI to a given societal domain. The consequences estimation enables to weigh the different disaster scenarios and to compare their severity<sup>233</sup>. An improvement to the model also takes into consideration the mobility of people, to allow for a more dynamic and accurate assessment of consequences<sup>234</sup>.

Another approach used to assess spreading consequences is through the application of input-output inoperability models (IIMs). These are based on the input-output approach proposed by Wassily Leontief, which is regarded as a key tool for the quantitative representation of interdependencies between different sectors within an economy. Input-output models are also supported by a number of publicly available economic datasets that portray dependencies between different economic sectors at regional, national and international levels. In IIMs, the concept of inoperability refers to the inability of a sector to perform its prescribed functions, and it can be caused by internal failures as well as external perturbations affecting the delivery of a system's intended output. IIMs have been applied to quantify the economic losses triggered by terrorism and other disruptive events to economic systems (or industry sectors). In recent years, extensions have been proposed in order to dynamically assess resilience to critical events, such as a disruption affecting some sectors and propagating through the economy depending on mutual dependencies, the centrality of the trigger points, and the response capabilities to the overall economy. In this context, a key factor towards the mitigation of monetary losses is represented by preparedness, which can be fostered by factors such as the availability of inventories able to ensure business continuity despite the temporary unavailability of some upstream services. In this perspective, IIMs can support the choice and prioritization of actions devoted to enhancing operability levels during and after crises.

#### 21.4.3 Tools

Next, we provide some examples of tools that can offer support to risk assessment and resilience enhancement of CIs. The first three tools focus on this issue of dependency modelling, while the fourth one assists policy makers to define performance goals for infrastructures.

#### JRC's Geospatial Risk and Resilience Assessment platform (GRRASP)

---

<sup>231</sup> G. Giannopoulos, R. Filippini, and M. Schimmer, "Risk assessment methodologies for critical infrastructure protection. part i: A state of the art," European Commission, Tech. Rep. EUR 25286, 2012.

<sup>232</sup> Di Pietro A., Lavalle L., La Porta L., Pollino M., Tofani A., Rosato V. (2016) Design of DSS for Supporting Preparedness to and Management of Anomalous Situations in Complex Scenarios. In: Setola R., Rosato V., Kyriakides E., Rome E. (eds) Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control, vol 90. Springer.

<sup>233</sup> This "*reduction or loss of well-being*" indicator is composed of four terms: (a) reduction of well-being of the most vulnerable population (categories concern old, young, disabled people and others), (b) reduction of primary services that affect the wealth and the well-being of the population; (c) economic losses due to services outages; (d) direct and indirect environmental damages (if any) caused by the outages (release of pollutants in the environment etc.). The previous criteria are affected directly by the event, but also by the lack of primary technological and energy services on different territories, over different time frames. The consequences of the scenario on each criterion are calculated on the basis of: (i) the quality of the considered services which contribute to wealth (electricity, telecommunication, gas, water and mobility), i.e. their level of availability during the event (this is a function of time), (ii) the relevance of each service to the achievement of the maximum level of the wealth quantity for a given aspect of the criteria, and (iii) the reduction of well being of people (for example the number of people affected, in a population segment, during a considered time period).

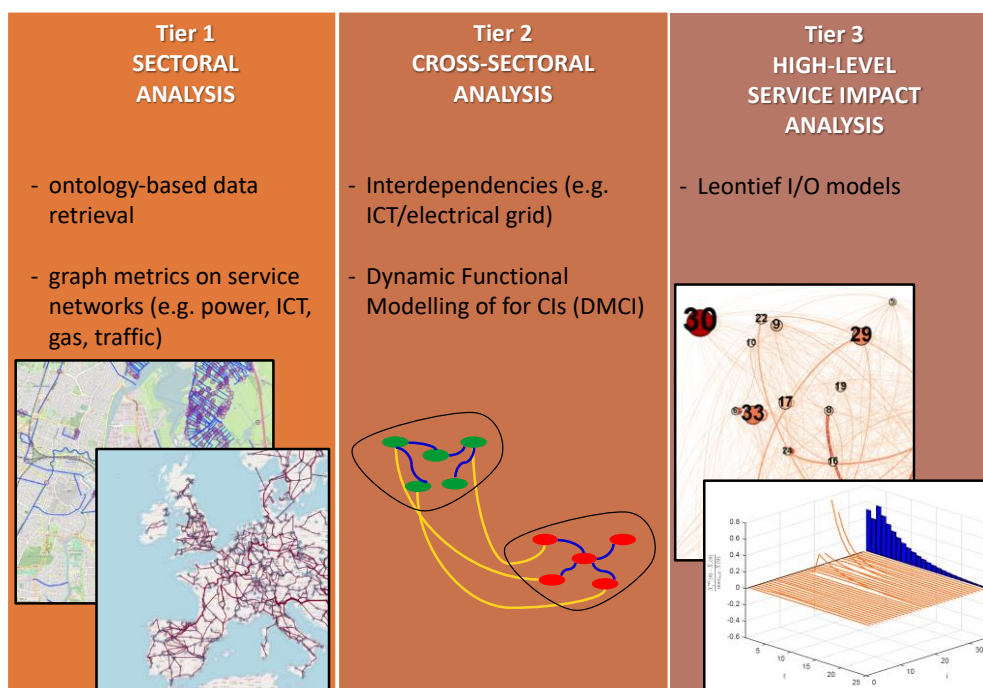
<sup>234</sup> Grangeat A., Sina J., Rosato V., Bony A., Theocharidou M. (2017) Human Vulnerability Mapping Facing Critical Service Disruptions for Crisis Managers. In: Havarneanu G., Setola R., Nassopoulos H., Wolthusen S. (eds) Critical Information Infrastructures Security. CRITIS 2016. Lecture Notes in Computer Science, vol 10242. Springer.

JRC has developed the Geospatial Risk and Resilience Assessment Platform (GRRASP)<sup>235</sup>. This is a World Wide Web-oriented architecture bringing together geospatial technologies and computational tools for the analysis and simulation of CIs. It allows information sharing and constitutes a basis for future developments in the direction of collaborative analysis and federated simulation. Moreover, it takes on board security concerns in the information sharing process, in terms of users, roles and groups. Based entirely on open source technologies, the system can also be deployed in separate servers and used by EU MSs as a means to facilitate the analysis of risk and resilience in CIs. Examples of GRRASP modules are reported next:

- Network metrics, a module to perform graph analysis on directed/undirected networks, with a focus on CIs;
- DMCI (Dynamic Functional Modelling of Vulnerability and Interoperability of Critical Infrastructures), a module to perform time analysis of service loss of interdependent CIs against critical events;
- CINOPSYS, a module to analyse economic losses during critical events according to an inventory dynamic input-output inoperability model.

See **Figure 61** for a representation of the tiered approach to analysis implemented in GRRASP.

**Figure 61:** Tiered approach to analysis of CIs in GRRASP



Source: Thocharidou et al, 2018 <sup>236</sup>

### Anytown tools

Tools of interest in order to assist users (e.g. at the city level) to map their dependencies have been developed in Anytown, an initiative by the London Resilience team<sup>237</sup>. These tools include mind maps and onion-skin diagrams mapping the impacts of infrastructure disruptions for a variety of initial triggers<sup>238</sup>. Figure 62, for instance, refers to the case of electricity failure and its cascading effects on various sectors. In this

<sup>235</sup> <https://ec.europa.eu/jrc/en/grrasp>

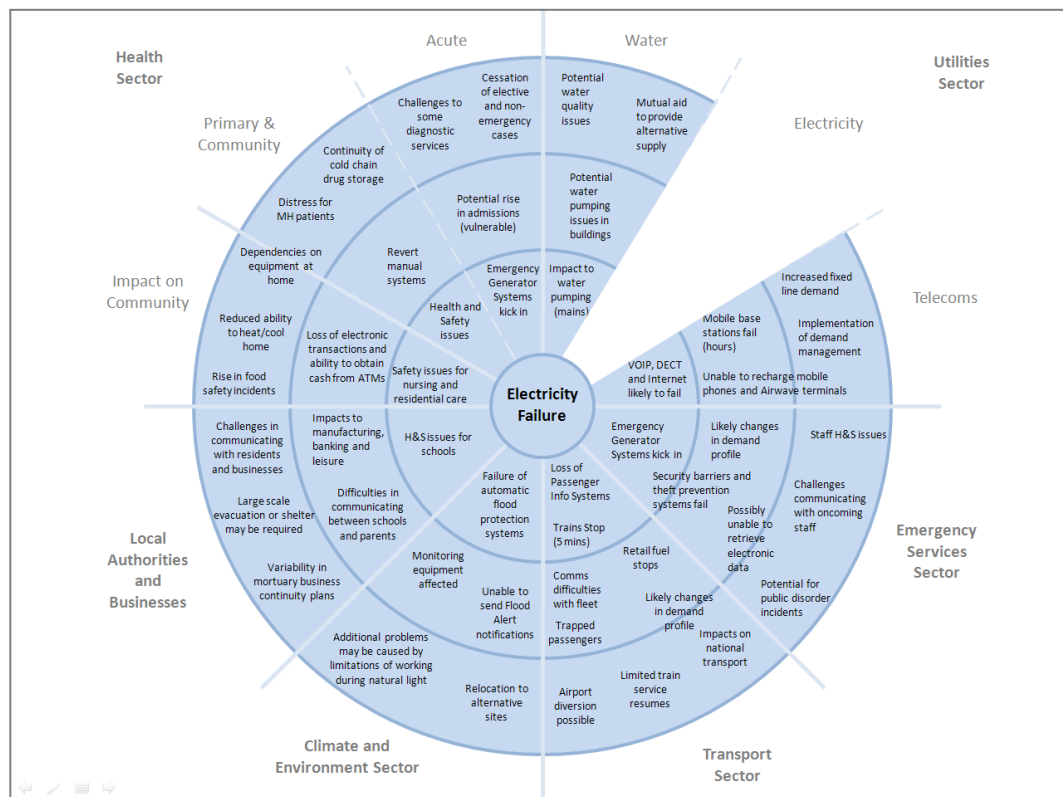
<sup>236</sup> Thocharidou M., Galbusera L., Giannopoulos G. Resilience of critical infrastructure systems: Policy, research projects and tools. In Linkov I., Trump B., Florin M.V. (Eds.) IRGC Resource Guide on Resilience (volume 2) Domains of Resilience for Complex Interconnected Systems in Transition, to appear, 2018.

<sup>237</sup> <https://www.london.gov.uk/about-us/organisations-we-work/london-prepared/>

<sup>238</sup> Hogan M., Anytown: Final Report, London Resilience Team, 2013. Available at: <http://climatelondon.org/wp-content/uploads/2016/11/Anytown-Final-Report.pdf>.

representation, “the concentric circles capture the ripple effect showing spreading consequences from an initiating incident”, which can be considered “a useful metaphor in describing chains of causation”.

**Figure 62:** Onion-skin diagram of Anytown relating to Electricity Failure.



Source: Hogan, 2013 <sup>239</sup>

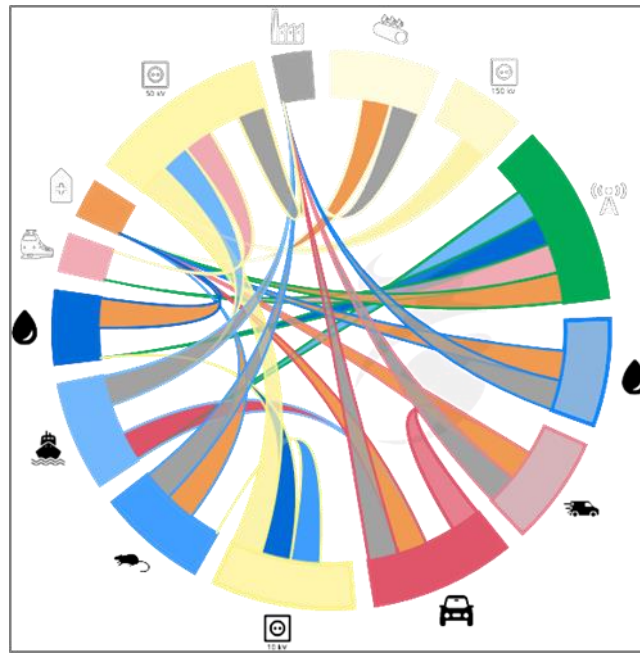
### Circle tool

Another tool that supports CI operators in identifying cascading effects together with other stakeholders in workshop settings is the ‘Critical infrastructures: relations and consequences for life and environment’ (Circle) tool, developed by Deltares. It was designed to map CIs and facilities relevant for an area (e.g. a city) and then visually represent the dependencies of these infrastructures, especially in order to address critical events. A representation of dependency mapping can be seen in **Figure 63**, while an application of the tool to a case study can be found in for a flood scenario relative to Cork, Ireland.

<sup>239</sup> Hogan M., Anytown: Final Report, London Resilience Team, 2013. Available at: <http://climatelondon.org/wp-content/uploads/2016/11/Anytown-Final-Report.pdf>.



**Figure 63:** Circle diagram of dependencies.



Source: Deltares<sup>240</sup>

### **NIST Planning Guide Performance Goal Tables**

Performance goal tables are provided as a complement to the above-mentioned NIST Community Resilience Planning Guide for Building and Infrastructure Systems<sup>241</sup>. In this framework, tables are provided for specific sectors (buildings, transportation, energy, water, wastewater, and communications) taking into account different building clusters (critical facilities, emergency housing, housing/neighbourhoods/businesses, and community recovery). Considering the possible diversity in hazard types and levels, affected area and disruption level, performance is evaluated in the short-, intermediate- and long-term. The specific results are then summarized in an overall performance goal table, as illustrated in **Figure 64**.

<sup>240</sup> <https://circle.deltares.org/>

<sup>241</sup> <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1190GB-9.pdf>



**Figure 64:** NIST Community Resilience Guide: performance goals summary table.

Summary Performance Goal Table													
Building Clusters	Disturbance <sup>1</sup>						Restoration Levels <sup>2,3</sup>						
	Hazard Type	Any					30%	Function Restored					
	Hazard Level	Routine, Design, Extreme					60%	Function Restored					
	Affected Area	Localized, Community, Regional					90%	Function Restored					
	Disruption Level	Usual, Moderate, Severe					X	Anticipated Performance					
Building Clusters	Design Hazard Performance												
	Phase 1: Short-Term			Phase 2: Intermediate			Phase 3: Long-Term						
	Days			Weeks			Months						
	0	1	1-3	1-4	4-8	8-12	4	4-24	24+				
<b>Critical Facilities</b>													
Buildings													
Transportation													
Energy													
Water													
Wastewater													
Communications													
<b>Emergency Housing</b>													
Buildings													
Transportation													
Energy													
Water													
Wastewater													
Communications													
<b>Housing/Neighborhoods/Businesses</b>													
Buildings													
Transportation													
Energy													
Water													
Wastewater													
Communications													
<b>Community Recovery</b>													
Buildings													
Transportation													
Energy													
Water													
Wastewater													
Communications													
<b>Footnotes:</b>	<p><b>1</b> Specify hazard type being considered Specify hazard level – Routine, Design, Extreme Specify the anticipated size of the area affected – Local, Community, Regional Specify anticipated severity of disruption – Minor, Moderate, Severe</p> <p><b>2</b> <table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td>30%</td></tr> <tr><td>60%</td></tr> <tr><td>90%</td></tr> </table> Desired restoration times for percentage of elements within the cluster</p> <p><b>3</b> <table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td>X</td></tr> </table> Anticipated performance for 90% restoration of cluster for existing buildings and infrastructure systems Cluster recovery times will be shown on the Summary Matrix</p>									30%	60%	90%	X
30%													
60%													
90%													
X													

Source: NIST, 2018<sup>242</sup>

## 21.5 Risk treatment

While this document focused mainly on risk assessment, the results of the assessment have limited value if they do not form the basis for examining alternative risk treatment options.

IRGC's 2017 Risk Governance Framework<sup>243</sup> discusses the challenges related to dealing with complexity, uncertainty and ambiguity. These are aspects that also MSs face when performing NRAs. Four risk

<sup>242</sup> Available at: <https://www.nist.gov/document/performancegoalstemplatelxslx>.

<sup>243</sup> IRGC. (2017). Introduction to the IRGC Risk Governance Framework, revised version. Lausanne: EPFL International Risk Governance Center.

management strategies are then identified for simple, complex, uncertain, ambiguous risks. The following two decision-making strategies seem most relevant to MSs<sup>244</sup>:

“Complex risks should be dealt with by risk-based decision-making involving internal or external experts and relying on scientific models. Complex risks can be addressed by acting on the best available scientific expertise and knowledge, aiming for a risk-informed and robustness-focused strategy. [...] Uncertain risks should be managed using precaution-based strategies to avoid exposure to a risk source with large uncertainties, and resilience-focused strategies to reduce the vulnerability of the risk-absorbing systems”.

Practical examples of risk treatment options can be found in the London Risk Register<sup>245</sup>, which lists the controls in place together with the risk assessment results. The US DHS offers a list of measures<sup>246</sup> on how to treat risk and increase resilience. The list is not exhaustive but offers some best practices and practical solutions for risk treatment. Here we list a selection of indicative examples from this guide:

- “working with partners to develop a picture of how this infrastructure investment will fit into the regional landscape of critical infrastructure”;
- “developing a comprehensive incident response plan that includes such components as scenario planning for the most likely risks and clearly articulated roles and responsibilities for all partners”;
- “building redundancy into an infrastructure system so it can handle a localized failure”;
- “budgeting for infrastructure mitigation during the development of a project to ensure the resilience of the infrastructure to threats and hazards”;
- “developing a business continuity plan to ensure rapid recovery from disasters or other disruptions”;
- “planning to conduct periodic updates for the infrastructure asset that can incorporate new technologies and/or upgrades that could enhance mitigation”;
- “determining whether environmental buffers (e.g., dunes or wetlands) can be incorporated into the infrastructure design to mitigate the effects of natural disasters”;
- “ensuring there are manual overrides and physical backups built into automated systems”.

## 21.6 Gaps and Challenges

The body of knowledge on CI risk and resilience management is quite rich and can be a valuable source for authorities and operators to explore. Enabling the operationalization of resources, models and tools still requires substantial efforts and this report is a contribution in this direction. A potential approach could include inventories of models, methods and tools provided by specialists. Work on the interoperability of models is also needed, especially in relation to current risk management practices. Moreover, as discussed, an issue is about the availability and quality of data needed for CI risk management.

Another key challenge for regulators and governments is to encourage private industries to invest in risk reduction and resilience, especially within the current economic conditions and considering the changing environment infrastructures operate in. Moreover, operators have varying technical, financial, political, reputational, legal priorities and constraints, which the policymakers need to comprehend when elaborating strategies for risk and resilience. To this end, stakeholder involvement and information sharing can be enhanced via the participation in networks. For example, Finland’s National Emergency Supply Organisation (NESO) sectors and their respective pools provide an interesting example of voluntary collaboration between public sector and industry. These business-driven groups are responsible for operational preparedness in their fields. The pools are tasked with monitoring, analysing, planning, and preparing measures for the development of security of supply within their individual industries, as well as with determining which enterprises are critical to the security of supply. Similarly, Sector-Based Information Sharing and Analysis Centres can be a solution for exchange between stakeholders. In the United States, several sector-based Information Sharing and Analysis Centres (ISACs) assist federal and local governments with information pertaining to cyber threats. Australia’s Trusted Information Sharing Network (TISN) is another example of a

---

<sup>244</sup> The framework also refers to **Simple risks**, which can be managed using a routine-based strategy, such as introducing a law or regulation, or to **ambiguous risks** which require discourse-based decision-making, by involving all stakeholders in order to eventually reconcile conflicting views and values.

<sup>245</sup> London Risk Register, Version 7.0, February 2018. Available at: [https://www.london.gov.uk/sites/default/files/london\\_risk\\_register\\_v7.pdf](https://www.london.gov.uk/sites/default/files/london_risk_register_v7.pdf).

<sup>246</sup> <https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Incorporating-Resilience-into-CI-Projects-508.pdf>

national engagement mechanism for business-government information sharing and resilience building initiatives. It provides a secure environment in which CI owners and operators across seven sector groups meet regularly to share information and cooperate within and across sectors, in order to address security and business continuity challenges. In the EU, examples of such networks are the European Reference Network on Critical Infrastructure Protection (ERNICIP)<sup>247, 248</sup> with its expert groups and its established series of CI Operators Workshops, or the Thematic Network on Critical Energy Infrastructure Protection (TNCEIP)<sup>249</sup>, which is made up of European owners and operators of energy infrastructures in the electricity, gas and oil sectors. Both networks allow stakeholders to exchange information on threat assessment, risk management, cybersecurity, and other security-related topics, on a voluntary basis and within a trusted environment.

Finally, an identified gap remains the need to perform joint exercises to better comprehend dependencies between CIs, thus generating more accurate risk assessments, and to jointly test risk treatment options. Such exercises need to be designed with a different mentality than civil protection exercises which focus mainly on the operational capabilities of emergency responders. Crisis scenarios that involve both public authorities and infrastructure operators are not widely analysed, but they can be a valuable tool to test risk and resilience strategies and plans, as well as to enhance collaboration.

---

<sup>247</sup> <https://erncip-project.jrc.ec.europa.eu/>

<sup>248</sup> Gattinesi P. (2018). European Reference Network for Critical Infrastructure Protection: ERNCIP Handbook 2018 edition, May 2018.

<sup>249</sup> <https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure>

## 22 Cybersecurity threats

GEORGIOS KAMBOURAKIS

### 22.1 Introduction

The term Cybersecurity<sup>250</sup> has hitherto received several definitions, but more or less all of them converge to “The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets” as expressed by ITU-T (ITU-T, 2008). In this respect, and according to ISO/IEC 27032:2012 (ISO/IEC, 2012), cybersecurity is a multifaceted, intricate, and rapidly changing ecosystem, which involves and is affected by the simultaneous interaction of several factors, including individuals, hardware, software, and the myriad of applications and services in the Internet of Everything (IoE). All these factors and players are typically tightly or loosely interconnected by means of the underlying communication infrastructure, either wired or wireless. It is therefore obvious that the goal of cybersecurity under the prism of a single or a multitude of individuals, organisations, or even countries, is to protect, deter and repel single- or multi-source attacks of any kind that may be potentially triggered against the assets<sup>251</sup> of interest, that is, critical infrastructures, telecommunications systems, computing devices, Internet of Things (IoT) devices, applications, services, as well as every piece of data or information communicated or kept somewhere in the cyberspace.

Given the above, cybersecurity must not be regarded as merely information security. Precisely, information security concentrates on the confidentiality, integrity, and availability of information, and it is concerned with any kind of information either digital or analogue, material or immaterial (ISO/IEC, 2018a). Cybersecurity on the other hand focuses on the cyberspace and cyberassets, and thus pertains to or lies on top of every “*cyber thing*” which is potentially vulnerable via Information and Communication Technology (ICT), including objects like cars, traffic lights, unmanned aerial vehicles, embedded processors and controllers, and so on.

Nowadays, private and public sectors are increasingly reliant on ICT systems to successfully fulfil their missions, and as already pointed out, such systems comprise a diverse collection of cyberassets that typically differ in their level of complexity and sensitivity depending on the particular context. Think for instance of Small Office Home Office (SOHO) environments, financial and industrial control systems, cloud infrastructures, smart grid and smart city systems, power plants, sophisticated anti-warfare systems, environmental control systems, and space-based systems. It is thus evident that today, cybersecurity, especially in the context of any country, union of states, and even globally, is a *sine qua non*. As it is further discussed in section 22.8, particularly for European Union (EU), this necessity has been, among others, already documented in JOIN/2017/0450 (EU, 2017a) and EU directive 2016/1148 (EU, 2016a).

Given the above observations, it can be straightforwardly deduced that for cybersecurity to be properly enforced, a rigorous and continuously reviewed risk<sup>252</sup> assessment method as a part of a holistic risk-oriented Information Security Management System (ISMS) (ISO/IEC, 2013a), must be in place. That is, nowadays, the zero-risk philosophy has been proven unrealistic (CSIS, 2019), hence any type or size of organisation must follow a formalised approach for the identification, assessment, management, and communication of risk in the cyberspace. In fact, this requirement is specifically and well-defined in ISO/IEC 27005:2018, where information security risk assessment comprises three distinct, but closely interrelated phases, namely risk identification, risk analysis, and risk evaluation. Nevertheless, achieving such a goal requires that before everything else, all the stakeholders have a common understanding of the involved terms, methodologies, and practices. While the introductory chapters of the report at hand have already set the general landscape of risk management based on the universal risk ISO standards, namely 3100:2018 (ISO/IEC, 2018b), 31010:2019 (ISO/IEC, 2019), and Guide 73:2009 (ISO, 2009), this chapter examines the topic through the lens of

---

<sup>250</sup> To assist the reader, this chapter provides definitions to the most common terms related to cyber risk assessment. A virtually exhaustive list of all the relevant terms can be obtained either from <https://www.iso.org/obp/ui/#home> (ISO) or <https://csrc.nist.gov/glossary> (NIST). Specifically for Cybersecurity, the reader is suggested to also refer to the cybersecurity taxonomy provided in (EU JRC, 2018).

<sup>251</sup> “Anything that has value to an individual, an organization, or a government” (ISO/IEC, 2012). The cyber environment, also known as *Cyberspace*, comprises mutually reliant information and communication technology infrastructures, and encompasses all assets which process, store or transfer digital data and information. These assets are called *Cyberassets*. In the following, the terms assets and cyberassets are used interchangeably.

<sup>252</sup> The terms “security risk”, “cyber risk”, “cybersecurity risk”, “information security risk”, “information system-related security risk”, and “ICT-related security risk” are used interchangeably in this chapter.

cybersecurity with basic references to ISO/IEC 27000:2018 (ISO/IEC, 2018a), 27001:2013 (ISO/IEC, 2013a), 27005:2018 (ISO/IEC, 2018c), NIST SP 800-39 (NIST, 2011), SP 800-37 (NIST, 2018), SP 800-30 (NIST, 2012), and the relevant recent literature.

Depending on the focus of interest, namely, uncertainty, impact, probability, etc., the literature provides several definitions of the concept of risk (Aven, 2012), (Gritzalis et al., 2018). According to NIST (NIST, 2015), the terms “*risk*” and “*information system-related security risk*” are defined as “*A measure of the extent to which an entity is threatened by a potential circumstance or event*<sup>253</sup>, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation”. From this definition, it is inferred that ICT-related security risk is the intersection of likelihood (probability) and severity of impact (consequences), where likelihood is typically determined from threat<sup>254</sup> and vulnerability<sup>255</sup> factors. Consequently, to aid decision making, security risk can be abstractly quantified using the formula  $Risk = f(\text{likelihood}, \text{impact})$ , which is transformed to  $f(\text{threat}, \text{vulnerability}, \text{impact})$ <sup>256</sup>. Generally, it can be said that threats on assets are materialised via attacks, which exploit vulnerabilities that have not been eradicated or mitigated with appropriate controls (countermeasures). So, while threat is closely related to hazard (as it is defined and used in other chapters of this report), and a threat is always a hazard, a hazard need not be a threat. This also means that risk can be simply defined as the potential for abuse, damage or destruction of an asset as a result of a threat exploiting a vulnerability. In any case, bear in mind that as discussed in the following sections and especially in section 22.7, cybersecurity risk is hard to approximate, let alone accurately measure.

Common categories of threats in the cyberspace are physical damage (fire, corrosion, dust, flood, etc.), compromise of information (passive or active eavesdropping, information tampering or disclosure, privacy violations, etc.), unauthorised actions (illegal processing of data, unauthorised use of equipment, etc.), just to mention a few. By using the aforementioned formula, one is able to practically quantify or qualitatively describe the risk level on a given asset. For example, what is the risk profile of a government employee using a laptop to store sensitive personnel data? Roughly, in a scale of 1 to 5, one can estimate likelihood to be, say, 2 (the employee may lose the laptop, having the information disclosed to unauthorised parties), and impact to be 3 (breach of law regarding data protection, the organisation may be subject to financial penalties, etc.). On the other hand, having the laptop’s disk encrypted it may reduce the impact to an acceptable level. It is therefore clear that, depending on the context, the contributing factors in the abovementioned formula must be clearly defined, assessed, and quantified through a proper security risk management process, which is illustrated in the upper part of **Figure 65**. Simply put, information security risk management refers to the balancing of costs and benefits, i.e., the cost-benefit trade-off associated with any security decision.

It is important to make a distinction between the concepts of cyber risk assessment and cybersecurity assessment. As shown in Figure 65, while these tasks are indeed interrelated, they are not identical. Precisely, the goal of cybersecurity assessment, typically conducted via passive or active testing, examination or interviewing, is to determine the current cybersecurity posture of the assessed entity, namely a system, device or process, and ascertain whether that entity satisfies specific predetermined security objectives (ISO/IEC, 2018b). Cybersecurity assessment embraces different methods, including penetration testing, compliance testing often based on checklist evaluation, vulnerability identification and analysis, testing via modeling,

---

<sup>253</sup> According to (Australian Cyber Security Center, 2020), a cybersecurity event is “an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security”, while a cybersecurity incident is defined as “an unwanted or unexpected cybersecurity event, or a series of such events, that have a significant probability of compromising business operations”. Note that such an event may happen in the cyberspace, but its negative consequences may impact the external context too.

<sup>254</sup> The “potential cause of an unwanted incident, which may result in harm to a system, individual or organization” (ISO/IEC, 2012).

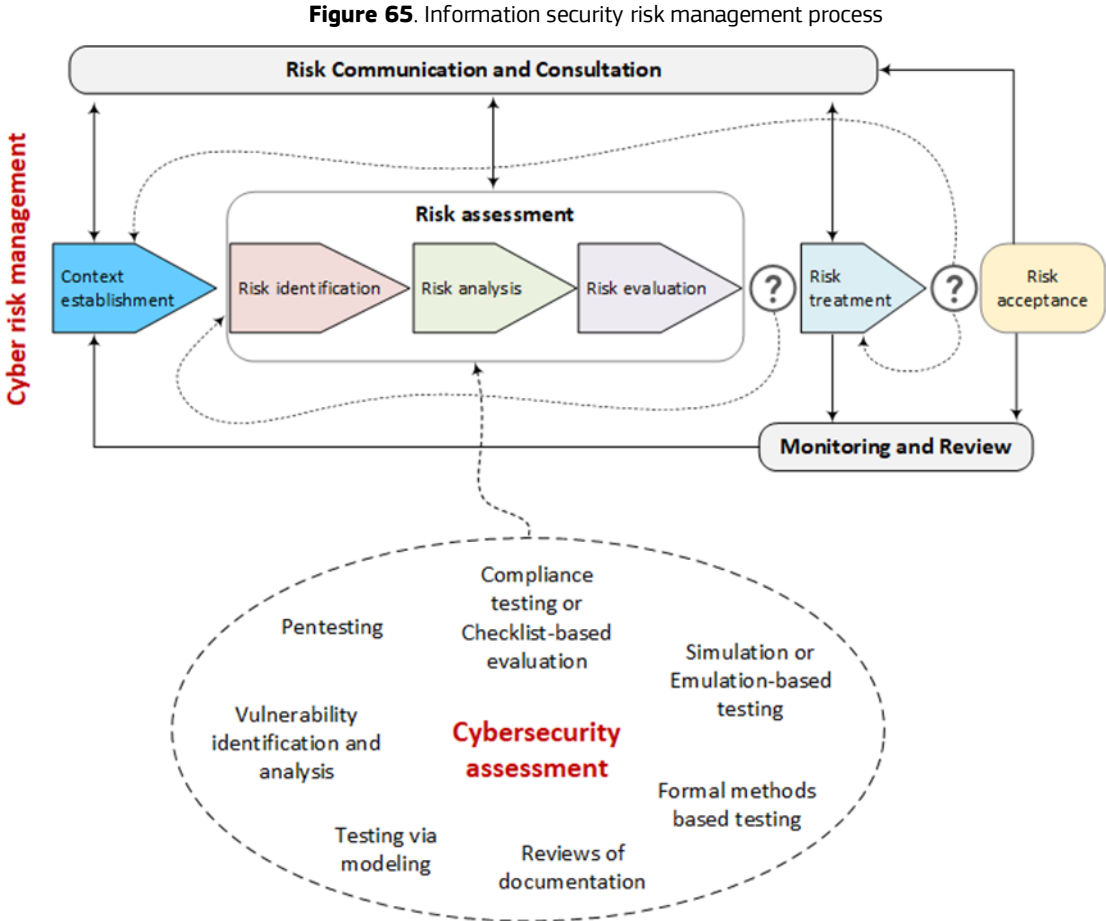
<sup>255</sup> A “weakness of an asset or control that can be exploited by a threat” (ISO/IEC, 2012). Vulnerabilities can be publicly unknown (“living”) either because they have not been discovered yet or linger indefinitely (“immortal”), in a product not anymore updated by its vendor. They can also be publicly known (“dead” or “wannabe dead”) because they have been revealed and already patched, or posted online, but still not remediated by a security advisory or patch. Others are quasi-alive (“zombies”), given that they can be exploited only in past versions of a product (Ablon & Bogart, 2017).

<sup>256</sup> This should be regarded as a risk conceptualization model rather than a mathematical equation, because as explained in the following sections, as of today, there is no commonly agreed, objective units of measurement for quantitatively assessing each factor in the formula. Actually, there exist some efforts to define common units for certain factors (e.g., for vulnerabilities), but these are determined by the context and often subjective to those that utilise the formula. In the literature, there are also other similar equations for approximating risk, including  $Risk = f(\text{vulnerability}, \text{threat}, \text{asset value}, \text{probability of occurrence})$  and  $f(\text{threat}, \text{vulnerability}, \text{asset value}, \text{possibility of detection})$ , while others even add an extra factor called “level of uncertainty”. In any case, risk can never be completely eliminated, so the result of the formula is always greater than zero.

simulation or emulation-based testing, and formal analysis, and hence, as detailed in chapter 22.3, it is mainly related to the risk identification phase of the risk assessment process.

For acquiring a more spherical view of the various IT security or cybersecurity risk assessment frameworks, methodologies and techniques along with comparisons between them, the reader is suggested to refer to (Gritzalis et al., 2018), (Wangen et al., 2018), (Felderer & Schieferdecker, 2014), and (Leszczyna, 2018) especially for smart grid, and (Cherdantseva et al., 2016) especially for Supervisory Control and Data Acquisition (SCADA) systems. Not less important, the ISO/IEC 15408 family of standards can also greatly contribute to the risk management or assessment process as it offers a generic roadmap, i.e., common criteria<sup>257</sup>, to guide the evaluation of security properties of an IT product throughout key phases of its life cycle, including design, manufacturing, marketing, and acquisition by consumers. Precisely, the use of common criteria allows for a direct and formalised way of comparison between the outcomes of independent security evaluations, and thus can provide proof that the security features of a product are as claimed by its vendor or developer.

The next five sections elaborate on the different phases of risk assessment process as well as on the risk treatment activity as seen through the cybersecurity prism. It is to be noted that according to ISO/IEC 27005:2018 (ISO/IEC, 2018c), each of these phases (processes) needs to follow the Input–Process–Output (IPO) model. The penultimate section of the chapter puts forward key thoughts and challenges, while the last section zooms in on the EU and international cybersecurity and cyber risk policy landscape.



Source: adapted from ISO/IEC 2018c

### 22.2 Context establishment

Before everything else, the context under which the organisation operates must be defined vis-à-vis to the information security risk management system. In short, the required pieces of information that need to be

<sup>257</sup> The basis for ISO/IEC 15408 (along with ISO/IEC 18045) is offered under the Common Criteria website, URL: <https://www.commoncriteriaportal.org>.

collected during this stage are concerned with (a) what is analysed, (b) if there exist any technical, human, organizational, or regulatory constraints that should be considered, and (c) who has the required expertise to properly assess. Precisely, the analysts and implementers of the risk management process have to (1) define the purpose of security risk management, (2) collect every information which is specific to the organisation and conclude to basic criteria related to risk and impact, (3) set the scope and boundaries, and (4) create an organisation to govern the security risk management process (ISO/IEC, 2018c). The aforementioned quartet of tasks are described succinctly in the following:

1. Typically, security risk management is an integral part of the corresponding ISMS, thus satisfying specific security requirements, and in some cases, it must exist due to legal compliance. Moreover, normally, risk management is a requirement for devising business continuity, including disaster recovery, and incident response formal plans.
2. Criteria for (a) risk evaluation, (b) impact, and (c) risk acceptance must be set from the onset of the process. Briefly, such criteria should coincide with the organisation's policies and objectives, need to be built around its internal and external context, should take into account the views of all the stakeholders (i.e., those, either individuals or organisations, that may affect or be affected by a decision or an activity pertaining to the organisation), and be grounded on cybersecurity requirements, including security/privacy standards, laws, policies, etc. Regarding point (a), amongst others, the implementers may consider the monetary or other value of the information assets affected, the importance of fundamental security services for the organisation, the reputation of the organisation, the possible effects on the stakeholders either internal or external, etc. For point (b), the criteria should pertain to the extent of loss or the induced cost of any kind due to a cybersecurity incident, e.g., damaged or paralysed operations due to loss of availability, harm in reputation and overall value, etc. For the latter point, criteria on whether a risk is acceptable or not and for how long under the given circumstances, along with relevant thresholds, should be established. This typically depends on the organisation's policies, priorities, objectives, as they are defined by the group of stakeholders.
3. Defining the scope of security risk management along with its boundaries provides guarantees that all the assets of interest have been considered in the risk assessment. Simply put, this may translate into an organisation's blueprint, which includes its divisions, functional structure, mission, activities, policies, objectives, priorities, shortcomings or constraints, the internal and external processes along with the relevant information exchange interfaces, information assets, the underlying economic, social, and cultural environment, and so on.
4. The task of conducting security risk management must be fuelled, supervised, and regulated by an approved organisation, which defines the responsibilities and the main roles of the corresponding group.

### 22.3 Risk identification

Generally, risk identification centres on finding, recognising, and describing the risks that could influence negatively in terms of loss or harm the achievement of objectives. That is, the per-risk possible sources and causes are identified, and the events and circumstances answering the questions of how, where, and why a damage along with its potential consequences may occur are answered. It is stressed that a cybersecurity event can generate a gamut of consequences either direct or indirect due to the ripple effect. Overall, in this phase, the produced risk scenarios should be as descriptive as possible and may refer to rough estimates or qualitative analysis. Moreover, this task needs to be systematic and comprehensive to guarantee that every significant risk, either internal or external in terms of its origin, has been considered and none is unintentionally left out.

In cybersecurity terms, there exist a number of rudimentary factors that can be used to characterise or identify a risk. First off, its origin referring to one or more threat agents<sup>258</sup>, i.e., an individual or group that can manifest a threat, including dissatisfied, terminated or poorly trained employees, hackers, competitors, governments, espionage, cyberterrorists, etc. Second, a given incident pertaining to a threat. That is, a sudden blackout, unauthorised access to confidential data, a privacy violation, the introduction of new regulations

---

<sup>258</sup> According to (ISO/IEC, 2012), a threat agent is an individual or group of individuals who have any role in the execution or support of an attack. Also, NIST (NIST, 2019) defines "Threat agent" as synonymous to "Threat source", namely "(i) intent and method targeted at the intentional exploitation of a vulnerability; or (ii) a situation and method that may accidentally trigger a vulnerability". Resultantly, threat events are caused by threat sources.

regarding security and privacy policies, etc. Third, its consequences or impact, including Denial of Service (DoS), economic damage, loss of reputation, prestige and competitiveness, financial penalties, etc. Forth, a specific reason for its happening assigned to a set of vulnerabilities. That is, poorly designed and tested software, faulty or deficiently maintained hardware, unprotected storage, lack of audit trail, complex user interface, problematic password management, etc. Fifth, the existing defensive schemes and controls, including thorough background checks on critical staff, the implementation of baseline and detailed security policies, role-based access, intrusion detection and prevention systems, security training and education, participation to cyber-intelligence programs, etc. Last, the time and place of occurrence; think for example of extreme weather conditions, earthquakes, terrorist attack anniversaries, demonstrations and strikes, etc.

In this context, security risk identification can be split into five phases, namely identification of (a) assets, (b) threats, (c) existing controls, (d) vulnerabilities, and (e) consequences. It should be emphasised that these phases are interrelated and consecutive, meaning that the output of the previous step is fed to its successor(s). As detailed in the following, to assist and subserve the procedure, the implementers can use theoretical analysis, historical internal or external data on cybersecurity incidents along with any other available information from cyber-intelligence, especially those stemming from similar organisations, results from audit procedures, vulnerability databases, socio-cultural data, and informed opinions. The latter source may include opinions or advices originating from asset owners, experts, stakeholders, legal department, human resources staff, insurance companies, government or other authorities, etc. In the following, we delve into the specifics of each of the above-mentioned phases.

- *Assets*: From a ten feet view, and according to ISO/IEC 27005:2018 (ISO/IEC, 2018c), assets can be classified as primary or supporting. The first includes the organisation's activities and processes and all sort of strategic, vital, personal, and high-cost information which is collected, kept, and managed by the organisation. The latter include assets on which the primary assets rely for completing their mission, namely hardware, software, networking infrastructure, personnel, site, and so on. Note that the supporting assets are potentially prone to vulnerabilities exploited by threats, and in such a case, the harm is reflected on the corresponding primary asset(s). Every asset along with a list of associated processes, e.g., a server providing cloud services, presents certain value to the organisation, and therefore urges for protection. Also, every asset belongs to and/or is assigned to some proprietor who is responsible and accountable for it, and typically they are the best source for obtaining an accurate approximation of the asset's value to the organisation. Firstly, the identified assets can be classified into broad categories, e.g., hardware, software, services, etc. In a subsequent step, they may be specifically determined in conjunction with the relevant organisation's processes and specific criteria used to evaluate possible consequences in the advent of a cybersecurity incident.
- *Threats*: Cybersecurity threats are not static, but constantly evolving becoming more sophisticated, and may affect one or multiple assets, causing diverse impacts on each of them. Harm can be due to a human or not, e.g., think of a cybercriminal vs. a flood, and can be deliberate or by oversight. In addition to those sketchily identified in section 22.1, typical threats include natural events (earthquake, pollution, tsunami, etc.), loss of sustainable services (failure in water supply, electricity surge or blackout, etc.), technical collapses (hardware/software failure or malfunction, etc.), compromise of functions (abuse of rights, denial of actions, etc.), and side-channel analysis<sup>259</sup> (ISO/IEC, 2018c). In addition to conventional threats, today, globalisation, facilitated by rapid technological change and global interconnectivity, has given a dramatic impetus to the phenomenon of hybrid threats<sup>260</sup>. Once a threat is identified, it should be assigned to a specific

---

<sup>259</sup> They exploit (unwitting) information leakage of computing devices or implementations to deduce private information (i.e., a form of reverse engineering). For instance, this can be achieved by observing analog physical side-channels that are anyway and unintentionally generated, say, by the CPU and RAM, during the normal operation of the device. Power consumption, electromagnetic leaks or even acoustic and thermal emanations, and timing information can offer an additional source of data, which can be exploited. From a fifty-thousand foot view, attacks capitalising on side-channel analysis can be active or passive (depending on whether the attacker actively interacts with the device or just observes the information being leaked), and invasive, semi-invasive or non-invasive (whether some sort of tampering with the software or hardware of the device is required or not) (Spreitzer et al., 2018), (Sayakkara et al., 2019).

<sup>260</sup> According to the European Centre of Excellence for Countering Hybrid Threats, the term hybrid threat refers "to an action conducted by state or non-state actors, whose goal is to undermine or harm the target by influencing its decision-making at the local, regional, state or institutional level", URL: <https://www.hybridcoe.fi/what-is-hybridcoe/>. Also, according to The European Energy - Information Sharing & Analysis Centre (EE-ISAC), "Hybrid Threats can be defined as a mixture of coercive and subversive activities, conventional and unconventional methods (i.e., diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.", URL:



class. This would offer an up-to-date view of the evolving threat landscape within the organisation as the case may be. Generally, there exist three basic methods to shape a threat model, which can aid in identifying the threats:

- *Attacker centric*: It starts with the attacker and evaluates their goals and the ways they might accomplish them. The level of adversarial misbehaviour can be analysed as well. For instance, the analysis may separate between malicious and semi-honest (also known as honest but curious) parties or between insiders and outsiders. A semi-honest party abides by the security policy, say, regarding the provision of a communication service, with the exception that they will keep a record of all the intermediate computations and received messages and will try to manipulate the recorded messages in an aggressively adversarial manner to learn additional information. On the other hand, a malicious party can misbehave in arbitrarily ways, say, they may terminate the communication protocol at any stage or change their input before entering the protocol. A particular interesting case of threats, which may be a greater concern today and in the years to come, pertains to what it is called the “*insider threat*”. This term generally addresses individuals with legitimate access to an organisation’s assets (human insiders) and is often overlooked and not proactively dealt with by organisations. Generally, one can discern between three major types of human insider:
  - Those who willingly try to inflict damage to their organisation, say, via theft of intellectual property, espionage, fraud, sabotage, etc.
  - Non-malicious insiders who may consciously infringe the organisation’s security policy, but they do believe that this will benefit their organisation; For instance, in many cases, employees bypass security policies or come up with shortcuts in sake of improving their job, and
  - Unwitting insiders who are not even aware that they are acting wrongfully. This ilk of insiders is considered especially hazardous to organisations, as they are highly prone to social engineering<sup>261</sup> attacks exfiltrating information, and malware. Recall that the compromise of human assets is in many cases the premier step in a cybersecurity incident, even if the rest of the systems are safe. The interested reader is also suggested to refer to the work in (Beebe & Chang, 2019), arguing that technology is not only both a target and an enabler, but it can actually be seen as an insider threat too.
- *Software centric*: It starts with the design of the system and attempts to step through a model of it looking for attacks against each of its aspects. Microsoft Security Development Lifecycle (SDL) (Microsoft Corporation, 2019) is a prominent example of such a method.
- *Asset centric*: It begins by identifying the assets of an organisation entrusted to a system or software, e.g., data processed by the software. Next, the assets are classified according to data sensitivity and their intrinsic value to a potential threat agent in order to prioritise risk levels.

As already mentioned, threat identification should especially consider threats originated by humans either insiders or outsiders. Precisely, there exist multiple ill-motivated groups that may weaponise threats, including script-kiddies, hackers, cyberterrorists, hacktivists, cyberespionage groups, foreign governments, intelligence and counter-intelligence agencies, cybercriminals, and so on – there is no one-size-fits-all. Amongst others, threat identification and analysis stemming from such groups should be done vis-à-vis to the particular group’s motivation or objectives, including monetary, revenge, political gain, political or other sort of activism, fraud and e-crime, theft of intellectual property, espionage, rebellion, greed and opportunism, religion, desire or obsession, anger, ego, self-promotion, curiosity or boredom, convenience, worldview, unintentional and by oversight errors, etc. It is not to be neglected that attackers of any kind need method, opportunity, and motive. At minimum, the output of this phase should be the list of the identified threats along with their type and origin.

---

<https://www.ee-isac.eu/hybrid-threats>. Anti-democracy attacks and cyber influencing, including fake news, cyber-meddling, astroturfing, and infodemic campaigns are typical paradigms of such a situation.

<sup>261</sup> “The act of manipulating people”, i.e., the human asset, mainly via human intelligence and open source intelligence “into performing actions or divulging confidential information” (ISO/IEC, 2010). Typically, such attacks unfold in four stages, namely “*Reconnaissance*” (information gathering), “*Hook*” (cultivating a relationship with the victim), “*Exploit*” (exploitation of information and relationship), “*Exit*” (decampment, leaving a tiny or no evidence of the attack).

- Existing controls: This step has to do with a fundamental principle in information security, namely the principle of adequate protection. That is, the analysts need to identify and possibly re-assess the controls already in place to deal with the identified threats from the previous step with the aim of saving resources and avoiding redundancy. Note that the term “control” refers to any measure or action that alters or regulates security risk, and may be implemented by means of policy, procedure, practice, process, technique, etc. In fact, as discussed in section 1.6, after implementation, risk treatments shape new controls, alter, replace or even drop existing ones, if the latter are deemed ineffective, not sufficient, or not justified. The expected outcome of this step should be a list of all the existing controls along with their operational condition, plus the new ones proposed for implementation. Justifications per proposal may be included as well.
- Vulnerabilities: A vulnerability that may be exploited by an existing threat is concerned with human or other actors, including processes and procedures, personnel, physical environment, hardware, software, and so forth. Finding vulnerabilities and associating them to threats and assets can be achieved via a plethora of tools and methods, including off-the-shelf or custom tailor vulnerability scanning tools, red teams (penetration testing) and relevant testing guides like the OWASP one (OWASP, 2014), Security Testing and Evaluation (ST&E), code review, and bug bounty campaigns. Such endeavour may start by answering basic questions, i.e., what kind of vulnerabilities are we after?, where and how can we find them?, what are the time-bounds and other constraints of finding them?, and also consider face-to-face interviews with users, that is, exploitation of end-users as sensors, questionnaires, offline audit trail analysis, and others. The output of this phase is typically a table associating the identified vulnerabilities with assets, threats, and controls. Orphan vulnerabilities, namely those that could not be associated to a threat, should be kept for future consideration. The interested reader may also refer to the survey works by Shah & Mehtre (2015), Beba & Karlsen (2019), Holm et al. (2011), and Barrere et al. (2014).
- Consequences: Lastly, the task of risk identification is concerned with the manifestation of the consequences an identified threat may inflict, if weaponised by a vulnerability in the context of a cybersecurity incident, to its associated list of assets and related processes. The analysts should consider including damage repair costs, financial and opportunity costs, loss in reputation, etc. The outcomes of this step should relate specific incidents with potential harms to the associated assets.

For addressing the above phases, implementers may use one or a mixture of relevant methodologies and frameworks, including the following.

- Legacy structured methods, including system design review and analysis, flow charting, operational modeling, etc.
- Team-based brainstorming and brainwriting to capitalise on the different expertise and experiences of each member. Security threat brainstorming toolkits, including the “Security Cards” one (University of Washington, 2013) can be exploited here too.
- Legacy security management techniques, including CLA (Checklist analysis), CCA (Cause-Consequence Analysis), CRAMM (CCTA Risk Analysis and Management Method), ETA (Event tree analysis), FMECA (Failure Mode, Effects and Critically Analysis), FTA (Fault Tree Analysis), HAZOP (Hazard and Operability Study), HAZID (Hazard Identification Study), HRA (Human Reliability Analysis), PHA (Preliminary Hazard Analysis), Forecasting, Probability methods, RR (Relative ranking), SA (Safety Audit), and SR (Safety Review).
- Legacy analytical techniques, including What-If sensitivity analysis, forecasting analysis, Pareto Principle also known as Principle 80/20, PESTLE (Political, Economic, Social, Technological, Legal, Ecological) analysis, Scenario technique, SMART (Specific, Measurable, Achievable, Realistic, Time Specific), SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis, VRIO (Value, Rareness, Imitability, Organisation) analysis, and Winterling Crisis Matrix.
- Attack modeling techniques as they are given in Table 24, and in (Nespoli et al., 2018), (LeMay et al., 2011).
- The Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE) (Microsoft Corporation, 2009), the Damage, Reproducibility, Exploitability, Affected users, Discoverability (DREAD) or DREAD minus D (DREAD-D) threat models (Shostack, 2008), the Attack Simulation & Threat Analysis (PASTA) threat modeling methodology (UcedaVelez

& Morana, 2015), the Hybrid Threat Modeling Method (hTMM) method (Mead et al., 2018), which combines features from Security Cards, Persona non Grata, and STRIDE, the Quantitative Threat Modeling Method (Quantitative TMM), which melds features from Attack Tree, Attack Graph, and CVSS methods (Potteiger et al., 2016), and the OWASP's Threat Modeling Cheat Sheet (OWASP, 2020).

- Security automation tools, databases, and standards as summarised in Table 25, and in (Nespoli et al., 2018), (Grossmann & Seehusen, 2015).
- The Diamond model of intrusion analysis (Caltagirone et al., 2013). In the heart of this model lies the “event” of any intrusion activity, which comprises four basic features, namely adversary, infrastructure, capability, and victim. Every malicious activity contains these features, and as a result, the acquisition of adversary intelligence can be based on them. The model also offers several “centred” approaches, given that each one concentrates on a specific feature of the Diamond. Each of these approaches comes with pros and cons and can be used for discovering new malicious activity, reveal activity related to the other connected features and the feature per se, and forecasting adversary operations while planning proper mitigation strategies.
- Cyber Kill Chain (KCK) models, including the more recent “unified” one (Pols, 2018), which describe the structure of an attack, i.e., the focus is on the tactics that comprise the consecutive phases of cyberattacks from the early reconnaissance stages to the exfiltration of data. Such a model may be particularly handy for analysing and combating strong threat actors<sup>262</sup>, which are often backed by nation-states to mount advanced persistent threats (APT)<sup>263</sup> and blended attacks.
- The MITRE ATT&CK framework, which is basically a knowledge base of adversary tactics and techniques based on real-world observations (MITRE, 2020).
- Game-Theoretic approaches, including prospect theory, with a special focus on the study and defence against APT, and on the managing of security risk and ambiguity (Shiva et al., 2010), (Do et al., 2017), (Jajodia et al., 2013), (Fielder et al., 2014), (Hu et al., 2015), (Yang et al., 2018), (Yang et al., 2019), (Xiao et al., 2017), (Wakker, 2010).
- The threat, vulnerability, consequences frameworks proposed in (Caralli et al., 2007), (Karabacak & Sogukpinar, 2005), and (Henry & Haimes, 2009).
- The Persona non Grata (PnG) threat modeling method, which focuses on the motivations and skills of human attacker (Cleland-Huang, 2014).
- The Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance (LINDDUN) threat methodology, which focuses on privacy issues, but can be used for data security too (LINDDUN Team, 2020), (Wuyts et al., 2018).
- Widespread (cyber)security assessment methodologies, tools and frameworks, including the Open Source Security Testing Methodology Manual (OSSTMM) (ISECOM, 2010), the OWASP testing guide (OWASP, 2014), the NIST Technical Guide to Information Security Testing and Assessment (Scarfone et al., 2008), the Information Systems Security Assessment Framework (ISSAF) (The Open Information Systems Security Group, 2006), the Penetration Testing Execution Standard (PTES) (The PTES Team, 2017), and the National Electric Sector Cybersecurity Organization Resource (NESCOR), targeting to the electricity sector (EPRI, 2020).

---

<sup>262</sup> “An individual or a group posing a threat” (Johnson et al., 2016).

<sup>263</sup> “An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders’ efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.” (NIST, 2015).

**Table 24.** Overview of attack modeling techniques existing in the literature with a focus on strengths and weaknesses. For a detailed discussion on these techniques the interested reader may refer to (Nespoli et al., 2018).

Attack Representation	Strengths	Weaknesses
Attack graph	Holistic view of the system, Visual representation of possible attack paths	State explosion for complex network, Probabilities and defence points are not represented.
Bayesian attack graph	Likelihood on the edges to model uncertainties	Extra computation for the probabilities calculation and assignment.
Attack tree	Formal representation of the system states, Visual illustration of possible attacker paths using AND/OR conditions, Absence of defence nodes	Numerous paths between leaves and root, Forest of trees to protect a complex system.
Attack Countermeasure Tree	Attack, detection, and mitigation events on the same tree structure	Countermeasure nodes cannot be refined over time.
Attack Response Tree	State-space model, including attacks and responses on the tree	State explosion due to the use of Partially Observable Markov Decision Process.
Attack Defence Tree	Improvements of the tree structure though defence point and countermeasure representation	Detection and mitigation points are represented in a unique node.
Service Dependency Graph	Visual representation of interdependencies between services, Quantitative attack impact assessment using CIA attributes	Identification of service dependencies requires huge effort from a security expert, Integration with an attacker-centric representation is needed to model possible attack decisions.
Markov Decision Process	Representation of decision making process, Concepts of state, reward, and action	State explosion for complex systems, often used alongside with other attack modeling techniques.
Competitive Markov Decision Process	System states modeled as a stochastic game between attacker and defender	Computation of the attacker and defender steps augments the problem complexity.
Partially Observable Markov Decision Process	Representation of unobservable system states	Interaction with the environment to receive information on unobservable states increases the complexity.

Source: Author

**Table 25.** Standardisation attempts for security automation. For a detailed discussion on these efforts the interested reader may refer to (Nespoli et al., 2018).

Vulnerability management	CVE (Common Vulnerabilities and Exposure)	Provides a reference method for publicly known vulnerabilities and exposures. It is available in several formats, such as CVRF, XML and HTML.
	CVRF (Common Vulnerability Report Format)	XML-based language that enables different stakeholders across different organisations to share critical security-related information in a single format.
	CVSS-SIG (Common Vulnerability Scoring System SIG)	An open industry standard which provides a numerical score to indicate the severity of CVE vulnerabilities.
	NVD (National Vulnerability Database)	XML-based Information security community effort to standardise how to assess and report upon the machine state of a computer system.
	OVAL (Open Vulnerability and Assessment Language)	Provides unique identifiers to system configuration issues for facilitating fast and accurate correlation of configuration data across multiple info sources. It is available in XML and Excel formats.

Configuration management	CCE (Common Configuration Enumeration)	Provides unique identifiers to system configuration issues for facilitating fast and accurate correlation of configuration data across multiple info sources. It is available in XML and Excel formats.
	CCSS (Common Configuration Scoring System)	Set of measures of the severity of the software security configuration issues.
Asset management	CPE (Common Platform Enumeration)	Standardised XML-based method for describing and identifying class of application, operating systems, and hardware devices present in enterprise's computing assets.
	ASR (Asset Summary Report)	XSD data model to express the transport format of summary information about one or more set of assets.
Software assurance	CWE (Common Weakness Enumeration)	Provides a common language to discuss, find and deal with the causes of software security vulnerabilities as they are found in code, design or system architecture. It is available in several formats, including CSV, XML and HTML.
	CWSS (Common Weakness Scoring System)	Provides a mechanism for prioritising software weakness in a consistent, flexible and collaborative manner.
	CMSS (Common Misuse Scoring System)	Set of measures of the severity of software feature misuse (trust assumptions made when designing software features abused to violate security).
	CWRAF (Common Weakness Risk Analysis Framework)	Part of the Common Weakness Enumeration (CWE) project. It provides a graphical framework for scoring software weaknesses.
Remediation information	CRE (Common Remediation Enumeration)	Suite of XML-based remediation specifications that enables automation and enhanced correlation of remediation activities.
	Extended Remediation Information	XML dictionary with additional data about each CRE, including references to CPE, CVE, and CCE.
Intrusion detection	IDMEF (Intrusion Detection Message Exchange Format)	Using XML schema, it defines data formats and exchange procedures for sharing information of interest to IDS/IPS and to the management systems that may need to interact with them.
Cyber threat information sharing and analysis	TMSAD (Trust Model for Security Automation Data)	Common trust model that can be applied to XML specification within security automation domain.
	OpenIOC (Open Indicator Of Compromise)	An extensible XML schema that allows the description of the technical characteristics that identify a known threat, an attacker's methodology, or other evidence of compromise.
	STIX (Structured Threat Information eXpression)	Collaborative community-driven effort to define and develop a language to represent structured threat information. It is based on XML schemes.
	TAXII (Trusted Automated eXchange of Indicator Information)	Open transport mechanism that standardises the automated exchange of cyber threat information.
	CyBOX (Cyber Observable eXpression)	Standardised XML-based language for encoding and communicating high-fidelity information about cyber observables, which are noticeable events or properties in the operational cyber realm.
Security benchmarking	XCCDF (eXtensible Configuration Checklist Description Format)	XML-based specification language to create security checklists, benchmarks and related documents.

Incident management	IODEF (Incident Object Description Exchange Format)	Defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incident.
Malware management	MAEC (Malware Attribute Enumeration and Characterisation)	Standardised language for communicating high-fidelity information about malware based upon attributes such as behaviors, artefacts, and attack patterns. It is available in XSD and HTML formats.

Source: Author

As a final remark, it is advisable that the analysts should right from the onset clarify everything pertaining to terminology depending on the case or asset at hand. For instance, here are two perspectives that can be followed:

- *Target-oriented:* The major components of this perspective are attack surface<sup>264</sup> and vulnerability. The first describes how much exposed is one to attacks. E.g., without a firewall to limit or block access to network ports, the attack surface is all the ports. Blocking all ports, but port 80 reduces the attack surface to a single port. Plainly, if one has a slew of devices and gadgets, including smartphones, tablets, smart speakers, e-readers, smart home hubs, fitness monitors, etc. that talk to each other and the cloud, augments the attack surface by far, making it difficult to manage and defend. Vulnerability on the other hand is a weakness that exposes risk. E.g., unsanitised user inputs can pose a vulnerability by a Structured Query Language (SQL) injection method.
- *Attack-oriented:* The key constituents in this perspective are attack vector and exploit. The first refers to the way by which an attack is carried out. For example, SQL injection is typically carried out using a browser client to the web application. The web application is the attack vector, possibly also the Internet, the client app, and so on depending on the focus. The latter expresses the method of taking advantage of a vulnerability. For example, the code snippet used to send SQL commands to a web application for taking advantage of the unsanitised user inputs is an exploit.

From a victim's viewpoint, the above terms can be easily described using a paradigm: An attacker sends an infected PDF file as an email attachment to a user. The victim opens the PDF file, gets infected, and a malware is installed. The attack vector is the email, the exploit is the code snippet in the PDF file, the vulnerability is the weakness in the PDF file viewer that allowed for code execution, and the attack surface is the user and email system.

## 22.4 Risk Analysis

This task focuses on grasping the nature, sources, and root causes of the relevant security risks and on estimating their level. The per-risk consequences along with its likelihood vis-à-vis to the factors affecting them are studied as well. The depth of the analysis is contingent on the particular risk, the aims of the analysis, the available information and breadth of resources, and the security controls already deployed.

In practice, and for cost-efficiency, the level of security risk can be firstly roughly estimated by using qualitative analysis. This will draw into the surface the major risks, which can be later analysed meticulously using quantitative methods, namely, statistical analysis and calculations combining impact and likelihood. Bear in mind that a cybersecurity event may lead to a range of impacts, thus affecting more than one objective, and as a result, impact and likelihood must be combined to calculate the risk level. Also, both impacts and likelihood are not typically static, but are often characterised by uncertainty and variability. In any case, and as explained in section 22.2, the risk assessing formulas and methods used must coincide with the relevant criteria defined during the context establishment phase. Nevertheless, it should be kept in mind that impact and likelihood may be manifested or mixed in diverse ways, depending on the objective and scope of the risk management operation and the nature of risk.

The information used to estimate impact and likelihood typically stem from:

- past experience and/or relevant data, say, kept in a cybersecurity incident database or acquired via cyber-intelligence;

<sup>264</sup> The "set of attack points" (or vectors) "that an attacker can use in order to enter or capture data in an information system" (ISO/TS, 2017). Professor Steven M. Bellovin says: "Attack surface is one of those core concepts that never gets the attention it deserves. It should, because properly understood, attack surface not only helps people analyze system designs, but also explains why some system changes help and others hinder. Roughly speaking, a system's attack surface is the set of ways that it might be susceptible to an attack." (Bellovin, 2016).

- international standards or guidelines or best practices;
- research and analysis;
- feedback from prototypes;
- expert advice, say, via interviews and questionnaires;
- use of existing attack models as those given in chapter 22.3, simulations, etc.

In the event no concrete adequate or relevant past data are available, think for example of a zero-day vulnerability, other estimates may be employed after being approved by the decision makers.

Security risk analysis may be qualitative, semi-quantitative, quantitative or hybrid:

- **Qualitative analysis:** It uses descriptive, human-readable scales, e.g., from very low to very high, to characterise the magnitude and likelihood of potential consequences. The scale employed may be different per risk, and its range is subject to the case at hand. Recall that this type of analysis is a best fit for initial assessment, and when quantitative analysis is unrealistic due to the lack of credible relevant information.
- **Semi-quantitative analysis:** This is an attempt to sketchily quantify the scales used in the qualitative assessment. That is, assign indicative, but not accurate values to each scale. In this respect, the numbers used must only be regarded and translated under the assumptions and limitations made during the construction of each particular scale. For the aforementioned reason, this type of analysis should be taken with caution because it can easily lead to inconsistencies.
- **Quantitative analysis:** Its aim is to assign realistic and as close as possible accurate numerical values to both impact and likelihood. As already mentioned, these values may stem directly or indirectly from a variety of sources, while the statistical models and the methodology used must be accurate too. For instance, as already pointed out in the previous sections, impacts on the affected assets may be expressed in terms of monetary (more straightforward), technical, operational, human, or other relevant criteria. On the other hand, likelihood can be approximated (a) via the use of past data, including experimental studies, statistical information, and gained experience, (b) by profiling the potential attacker in terms of skills, resources, motives, opportunity, and the level of attractiveness an asset presents to them, (c) geographical, socio-economic and cultural data, (d) the set of vulnerabilities per asset, and (e) the hitherto deployed controls along with an assessment of their effectiveness. For instance, a poor authentication policy on an IoT device, that is, a weak control that bears vulnerabilities, augments by far the chances of the device being compromised and enslaved into a botnet (Kolias, 2017).

For obtaining a more detailed view on the different approaches used in information security risk analysis, the interested reader is suggested to refer to the annex E of ISO/IEC 27005:2018 (ISO/IEC, 2018c). Additionally, the reader should consult the May 2018 report prepared for the United States (U.S.) Department of Homeland Security, titled “*Cyber Risk Metrics Survey, Assessment, and Implementation Plan*” (HSSEDI, 2018), and the literature review works (Landoll, 2011), (Cherdantseva et al., 2016), (Kruse et al., 2017), (Shevchenko et al., 2018), and (Ganin et al., 2020).

## 22.5 Risk evaluation

The aim of the security risk evaluation process is to provide a side-by-side comparison of the outcomes obtained from the risk analysis stage against the risk criteria defined during context establishment for the sake of facilitating decisions on whether a specified level of risk is admissible or not. Recall from section 22.2, that amongst others, such criteria are determined on the basis of the organisation objectives, the stakeholders’ views, and the scope and objective of the security risk management process per se, which however may be revisited at this stage given that more detailed information about the estimated risks may be available. This means that during this phase concrete and justifiable choices have to be made regarding which risks are tolerable, and thus currently do not call for treatment<sup>265</sup>, and which of them need to be dealt with. Treatment priorities associated to the latter category of risks must also be formulated.

---

<sup>265</sup> Sometimes, risk analysts encounter risks that can be characterised as “*exotic*”. This pertains to rare incidents, including solar and geomagnetic storms, and others quite more frequent, including vandalism, sabotage, and terrorism targeting the power grid or other major networked systems. For instance, in April 2013, the “Metcalf sniper attack” took place, where snipers attacked large electrical transformer units in California inflicting more than \$15M damage in the equipment. The opponents may also perceive such

In some cases, if the results are ambiguous, risk evaluation may spur additional analysis, meaning jumping back to a previous phase, as shown in the upper part of **Figure 66**. Typically, the decision taken depends on the level of risk, as it has been quantified by the previous phase. It may also reckon with pre-defined or revised thresholds pertaining to the single or accumulative impact, in case of a series of events happening at the same time or due to a knock-on effect, as well as the degree of confidence put in the previous two phases. The outcomes of this phase must include the prioritised risks vis-à-vis to the cybersecurity incident(s) that are deemed to produce the corresponding risk(s).

## 22.6 Risk treatment

Security risk treatment is basically a risk alteration process, as it typically concentrates on choosing and implementing one or several treatment options to each risk included in the prioritised list of risks generated during the previous stage along with the associated cybersecurity incident scenarios. After justification, the implemented treatment either serves as a new healing control or it alters existing controls (ISO/IEC, 2012), (ISO/IEC, 2013b). Treatment options, which may be applied independently or in tandem are:

- Avoiding the risk, e.g., by removing the affected assets or ceasing/cancelling the associated processes. In some cases, relocating the vulnerable assets, say, due to anticipated seismic activity to a safer location should suffice to forgo the risk.
- Modifying the risk by introducing controls that, say, remove the source of the risk (correction or elimination), alter the consequences of the risk (impact minimisation), change the probabilities of the risk (prevention, deterrence, detection, recovery, etc.).
- Sharing the risk, but typically not the corresponding liability, with others, i.e., external parties. Normally, this is done either by insuring the asset of interest with a (cyber) insurance company (ENISA, 2016) or by outsourcing the implementation and management of a given control, e.g., the intrusion detection task is assigned to a partner.
- Wittingly retaining the risk if it is deemed to satisfy the risk acceptance criteria as they were defined during the context establishment phase (see section 22.2).
- Although it is not generally advisable, sometimes the analysts may even decide to increase the risk with the purpose of pursuing an opportunity. For instance, to reduce the payroll cost, some of the organisation's operations may be relocated to a country which is known to suffer from widespread corruption.

In all the above cases, the remaining risk is called "residual risk". In essence, the goal of this stage is to devise a formal risk treatment plan along with the residual risks to be submitted for approval by the organisation decision-makers' hierarchy.

The decision regarding the option to be selected per risk is typically anchored in risk ranking and cost-benefit analysis, i.e., the value of the asset versus the cost of implementing or acquiring and administering the relevant control, taking also into account the available timeframe and other parameters specific to the context at hand. This means that in cases where the risk is severe and the cost for its remediation is relatively low, then the risk modification approach must be followed. Naturally, the consequences identified per risk is a decisive factor here; major risks, even if they are unlikely to occur, should be considered candidates for modification, despite the incurred implementation cost. This is for example the case when the repercussions of a cyberattack can put human lives at risk. Not less important, a carefully selected risk treatment is anticipated to cater for treatment for a multitude of risks. A typical example of this situation is efforts to raise the personnel's security awareness level, and thus provide them with some sort of "cybersecurity inoculation", e.g., by proactively and regularly briefing frequently targeted users in small groups, organising one-to-one follow-ups on cybersecurity incidents, conducting simulated attacks<sup>266</sup>, training users to be security sensors, etc.

---

incidents as a window of opportunity or use them as a misdirection tactic to immediately after try to penetrate the weakened security controls. Such incidents should be also considered and evaluated depending on the context.

<sup>266</sup> This may be as simple as deliberately sending phishing emails to the organization's personnel and observing their reaction, to training cybersecurity professionals by using advanced multipurpose simulation platforms, namely "Cyber Ranges", running on a virtualised infrastructure. Such platforms are used to conduct cyberwarfare training, evaluate critical vulnerabilities and controls, and estimate how the organization's personnel, procedures, and technology are integrated to safeguard pivotal assets. The reader is suggested to refer to the CYBERWISER.eu initiative, an EU's Horizon 2020 funded project, and the National Cyber Range (NCR) project in U.S. (Ferguson et al., 2014).



However, it is not to be neglected that the implementation of any control, say, application level, server protection, end-user focused, counter-social-engineering, etc., may be subject to certain constraints or inexpediences, which in turn may partially or entirely cancel its benefit. For instance, the use of hefty cryptographic mechanisms to provide confidentiality and integrity in communication may result in the degradation of the underlying services, and thus to dissatisfied consumers or citizens. Also, the introduction of an over-pessimistic access policy in firewalls may bring problems and discontent to employees accessing outside services of need. Another example is when the software displays an excessive number of annoying warnings to the end-user, leading them to click without thinking on the, say, “Agree” option. A last typical instance of such a situation is the password aging policy used by many organisations. While it is (still) believed to mitigate the risk by forcing people to change their passwords every, say, 90 days, it imposes unnecessary fatigue, cost, and even provides the illusion of stronger security, while actually increases risk – the users are simply increment or decrement the number included at the end of their password.

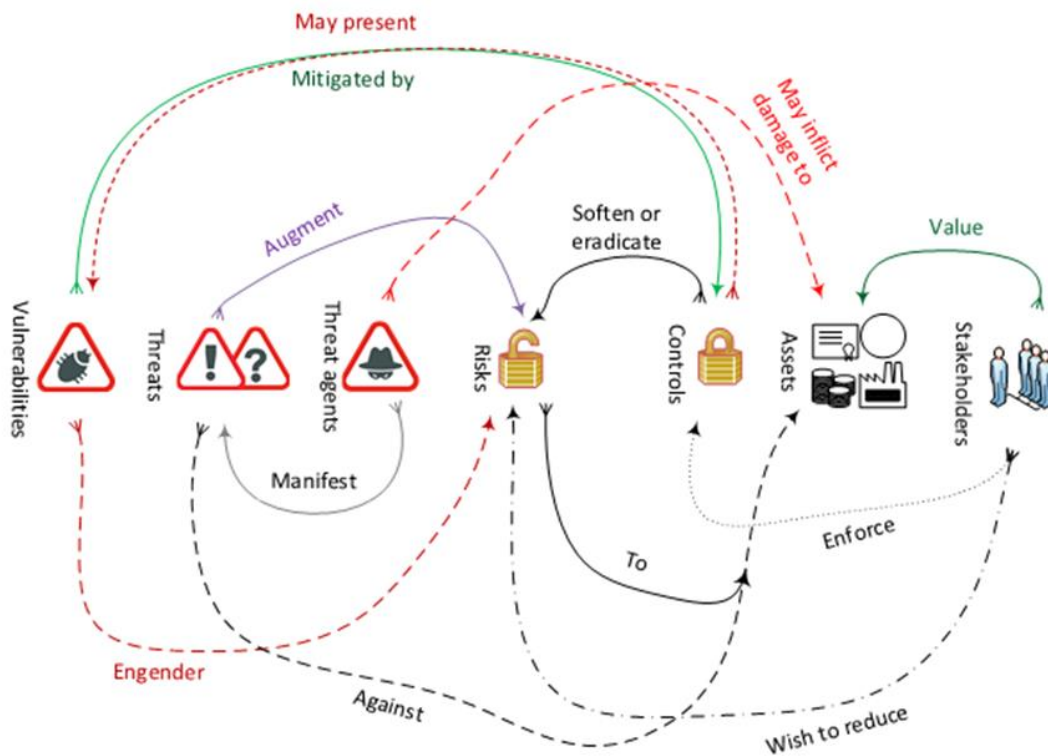
In a nutshell, such poorly designed or outdated controls may cancel or significantly reduce the positive effect of the implemented countermeasure, and even worse, result to a system that is neither secure nor usable. To avoid such inexpediences and hiccups, implementers should work more on usable security and security and privacy by design. In short, to create a truly secure and/or privacy-preserving product, usability must be well tied to security/privacy. After all, the “blame the user” philosophy does not seem rewarding in the least bit (Schneier, 2016a).

Lastly, beyond any legacy control, organisations should apply more advanced ones, focusing on the detection of APTs exercised by powerful threat actors. Simply put, while required, legacy security controls are insufficient to block new attacks and sophisticated threat actors. Controls that may be considered to this end are darknet monitoring, sinkhole operations, and traceback techniques. Additionally, the implementers may think of avoiding monolithic solutions, and instead apply an alloy of more aggressive defensive plans and strategies, including Security through Diversity, Moving Target Defense (MTD) and Cyber Deception (Wang & Lu, 2018). Besides, in the fullness of time, legacy defensive techniques alone are proved inadequate, and may also suffer from inherent serious vulnerabilities, complexity, and be quite easily quantifiable by opponents (Schneier, 2016b). Consequently, defensive schemes it is better to be backed up by “offensive” cybersecurity strategies and methods, including penetration testing and cyber deception, ultimately leading to the development of “advanced persistence resilience”. For a detailed list of possible controls and their associated metrics the reader is suggested to refer to (Center for Internet Security, 2020).

An important yet often neglected aspect when identifying and managing threats and applying controls is the idiosyncrasies of the wireless networks vis-à-vis to its wireline counterparts:

- Access control: Accessing a wireless network realm does not mandate physical access to a network jack or cable. The opponent can be anywhere in the vicinity or further afield depending on the strength/type of the wireless signal/equipment.
- Highly dynamic network conditions: Conditions in wireless networks change more frequently and drastically than in their wired counterparts, that is, the traffic patterns of the users of wired networks are much more predictable. This is not the case with wireless networks where different users, with diverse equipment and usage habits can roam free. For instance, think of the “tide effect” in cellular networks, causing sudden and irregular fluctuations in the traffic of base stations. This however may confuse the deployed security controls by, say, producing a high rate of false positives.
- Distributed nature, (still) limited bandwidth, and big data: In wireless and mobile networks the nodes are by default distributed and mobile, meaning that the underlying monitoring facilities and security controls should be also distributed, but able to apply filtering and minimise the exchange of security-related information with central nodes. And according to Cisco, data from wireless and mobile devices will account for 71% of the total IP traffic by 2022 (Cisco Systems, 2020).
- Zero-day: As wireless technologies evolve in a fast pace, new vulnerabilities emerge, and attackers plot novel penetration methodologies.
- Heterogeneous data: 4G and beyond core networks are based on a flat-IP architecture, providing interfaces to previous generations, which however use dissimilar protocols. Also, from a radio interface perspective, a plethora of technologies exist; cellular, Wi-Fi (IEEE 802.11), IEEE 802.15.4, ITU-T G.9959 to mention just a few.

**Figure 66.** Rumentary risk management concepts and relationships



Source: adapted from ISO/IEC (2012)

A high-level representation of all the basic risk management concepts along with their relationship(s) is illustrated in **Figure 66**. As a final remark, this stage may also utilise some of the methodologies, techniques and attack models summarised at the end of chapter 22.3.

## 22.7 Key thoughts and Challenges

Over the last few decades, governments, companies, and individuals have become critically reliant on ICT. For many of us, it is taken for granted that fundamental services like energy and wired and wireless communications will always run, and that the web and the variety of e-services and data will be always obtainable. The reality however is starkly different; altogether our insecurity is augmenting. Networked systems and infrastructures, even the most fortified ones, think for example of the “Stuxnet” malware, present vulnerabilities and may be exploited at any moment – it is a matter of when, not if. No one would object that organisations of all sizes and types, and even countries, are nowadays faced with frequent data breaches, service disruption, and so on. Even the strongest defensive measures on nations’ critical services and infrastructures may be leapfrogged by the unprecedented speed, magnitude, volume, scope, scale, intensity, and sophistication of modern cyber threats or attacks facilitated by rapid technological change and global interconnectivity.

From a critical infrastructure’s viewpoint, the risks are much elevated because the once isolated systems, including gas, water, electricity, manufacturing, and transportation, are nowadays interlinked to form a multiplex and thus far inadequately comprehensible *system-of-systems*, potentially exposing a tremendous and very fertile attack surface. Even more, IoT and 5G and beyond mobile networks are already culminating in a stronger union of systems, given that certain processes in smart-buildings, smart-cities, transport systems, including autonomous vehicles, and factories will be or are already remotely controlled via the internet. This means that one should not isolate themselves in silos by solely concentrating on threats and vulnerabilities in specific sectors, instead a cross-sectoral cyber thinking and defence approach is needed. In a nutshell, networks are intrinsically susceptible to cyberattacks; the threats are everywhere, and a single penetration exposes the entire system to risk and may trigger a cascading failure. And of course, there is a large financial risk associated with cybersecurity, applying to both prevention and recovery.

Even more, nowadays, cyber threats are tightly or loosely connected with other major global collective challenges the humanity has to deal with, including geopolitical instability, social and wealth inequality, environmental threats, and climate change (Cassotta & Pettersson, 2019). One can say that the aforementioned phenomena, which as cyber threats affect the sustainability of the whole planet, act as threat multipliers – they directly or indirectly affect socioeconomic and political consistency, particularly in insubstantial contexts. To give an instance, a considerable amount of high-skilled cybersecurity workforce is underpaid in comparison to what they can earn if they come over to the dark side. In this sense, all in all, cybersecurity is both a technical and a socioeconomic problem, and even a social justice one, i.e., *“the threat is worse for already-vulnerable population”* (Baer, 2017), and thus cannot be solved by technical means alone.

In a more inclusive sense, today, cybersecurity is a prolonged, unconventional warfare on an asymmetric battlescape - The stakes are much elevated, and the terrain is enormous, boundless, highly diversified, and multilayered. Cyberattacks against critical infrastructures and cyber influencing are powerful weapons in the arsenal of hybrid threats, and virtually all operations in modern society are less or more vulnerable to cyber reconnaissance or cyberattacks. Let us refer to just three major cybersecurity incidents that took place only in 2017. In May, ransomware named *“WannaCry”* targeted vulnerabilities in the MS Windows operating system and paralysed manufacturing operations, transportation and telecommunication systems. In June, *“NotPetya”* malware infected a myriad of Internet connected systems in about 70 countries. In August, a Saudi Arabian oil and gas plant fell victim to *“Trisis”* or *“Triton”*, a malware destined to cripple industrial safety systems. Having this in mind, it is an immediate necessity for countries and organisations to realise that a formalised, rigorous risk management approach must be at the heart of their strategy and digital agenda. Many major losses and damages are the result of mismanaged risks, or putting it another way, the risk of complacency and inaction is sizable. Namely, thinking that everything is safe because our organisation has not yet suffered a major breach is a risky illusion. Unplanned and ad-hoc responses to a cybersecurity incident may be catastrophic and organisations must shift to transparent (always expose the risk and do not swipe it under the carpet), proactive, systematic, and integrated risk management.

Besides, risks can be the source of noteworthy opportunities for improvement, which can make an organisation more efficient and resilient, and potentially provide for a competitive advantage. For instance, social networking sites, blogs, and tools like Twitter, augment reputational risks due to the by far increased speed at which information and news, weather true or false, can propagate. Such platforms may also increase the risk of malware victimisation as well as the leaking of internal classified information, not only because they are prone to vulnerabilities lurking in relatively new software, but also because they tremendously ease the sharing and exchanging of information. On the bright side however, an organisation can capitalise on such sites, tools and services by, say, using them as a public relations and viral marketing tool. This of course, requires the organisation to be aptly ready for copying with the corresponding risks.

As already discussed in the previous sections of this chapter, healthy and robust information and deep knowledge of the organisation and its internal and external surroundings are of major importance in identifying risks. Historical information about similar organisations may also become very handy given that it can bare sound and solid predictions about current, evolving and future threats, not yet dealt with by the organisation per se. Sharing knowledge, i.e., developing a cyber-threat intelligence program, is a key factor here, but still organisations are resisting sharing with fear of embarrassment and liability to be the basic impediments. Early attempts on sharing knowledge focused on vulnerabilities, intrusions, and attribution. Now, the focus should be more on effective threat sharing models as well as on security management teams working side-by-side with operators and vendors, which in conjunction could offer agile defensive posture aligned with threat. In simple terms, this means that defenders become demanding consumers and producers of intelligence at the same time. Several lead questions in this respect could be: Why might our system be attacked and by whom? What assets are of interest? What threats should we look for on our assets and why? What activity are we seeing? Where has this threat or attack been re-seen? What does it do? What vulnerabilities does this threat exploit? Why does it do this? How can these attacks be implemented? Does the cybersecurity incident encompass misdirection or misleading information injected by the opponent? Is this threat persistent? Is this threat related to or affects others? Who is responsible for this threat? What can we do about it? The answers to such questions can bear a rich set of sources, cater for a disciplined indication and warning process, and a sufficient understanding of threat actors in the particular sector.

Another point of consideration with regard to information sharing pertains to vulnerability disclosure policies (also known as *“vulnerabilities equities process”* debate in US). The key question here is how one can optimally balance between the needs of all the stakeholders? For instance, from a state’s viewpoint, once a vulnerability is found, there is an obvious dilemma; either disclose the vulnerability to the affected vendor for patching it, or reserve the vulnerability as an asset so it can be used for national security purposes, but at the cost of

general cybersecurity. In EU, the public discourse around this issue is rather fresh<sup>267,268</sup>, while in the U.S., the debate is going on for almost a decade. Equally important is the fact that there is already a thriving white<sup>269</sup>, grey<sup>270</sup>, and black<sup>271</sup> market of exploitable vulnerabilities (zero-day exploits) available to private sector, governments, brokers, and cybercriminals (Schneider, 2019a), (Albon et al., 2014).

Even so, today networks are too large, complex, and still heterogeneous. Security by design and security by default<sup>272</sup> principles (see for instance (Saltzer & Schroeder, 1975), (Leveson, 2004), and (SCF Council, 2020)), which are aiming at reducing vulnerabilities by considering security requirements at the early stages of the lifecycle of products and services, are often not properly prioritised by ICT vendors who rather centre on the functional ones. Risk analysts are assigned a hard, nearly infeasible task; they are assumed to know all the assets, reduce the attack surface to the bare minimum, be aware of or discover all the vulnerabilities, swiftly adapt to changes, lessen the noise caused by skillful adversaries injecting bogus and misleading information, and overall cope with the “fog of war”<sup>273</sup>. Even, they are required to deal with elemental risks that have been accumulated for many years because designers emphasised on functionality and left security and/or privacy for future work, as in the case of TCP and UDP protocols, the domain name system, the HTML language, the voice over IP protocol, amongst several others. On top of everything else, virtually, every asset may be susceptible to zero-day vulnerabilities and exploits, and even security-savvy user reporting is not to be taken for granted; an organization-wide cybersecurity havoc can be triggered by only one keystroke! All these must be considered as a residual risk. The risk treatment process on the other hand, including patch management, is expected to remediate or at least realistically soften the major risks, but implementers need to bear in mind that everything should start from establishing the internal and external context and reducing the attack surface, although attack surface awareness is no security panacea.

As with cybersecurity in general, it is cumbersome to even approximate cybersecurity risk in straightforwardly understood quantitative terms. Naturally, as already pointed out in chapter 22.3, there exist several methodologies and tools to identify and measure or assess the constituents of cybersecurity risk, but in practice<sup>274</sup> this endeavor especially for large organisations and for nations themselves is complicated. Actually, until now, there is no globally accepted by the relevant communities and standardised way of measuring cybersecurity per se, and hence decide whether an investment on security policies, measures and controls eventually resulted in a safer organisation or not. In short, as of today, there is no explicit system that can be used to quantify cybersecurity in an objective and comparative way. The key problem here is that nowadays the technological risks are inextricable and unclear, and in numerous occasions there is a lack of data to perform risk management properly. On the one hand, it is difficult to measure in absolute terms the capacity of an organisation’s network security in repelling cyberattacks, and on the other, to calculate quantitatively the cost to the organisation if the defenses fail to do so. Even worse, the risks change or mutate around the clock, making the calculations even more cumbersome.

So, how are organisations and even states currently assessing their cybersecurity posture? The truth is that they tend to utilise qualitative measures of security rather than quantitative ones. Actually, according to a recent survey (Moore et al., 2016) involving Chief Intelligence Systems Officers, industry best practices and frameworks were deemed to be the most important factors to access an organisation’s cybersecurity posture, while quantitative methods measuring the effectiveness of security controls were placed quite lower in the

---

<sup>267</sup> Recommendations from a Report of a CEPS Task Force Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges, Feb. 2018, URL: [https://www.ceps.eu/system/files/SVD-%20Flyer%20event%2027%2002%20Parliament-%2024%2002\\_Final.pdf](https://www.ceps.eu/system/files/SVD-%20Flyer%20event%2027%2002%20Parliament-%2024%2002_Final.pdf).

<sup>268</sup> CERT-EU Responsible Disclosure Policy, URL: [https://cert.europa.eu/cert/newsletter/en/latest\\_HallOfFame\\_.html#CERTpolicy](https://cert.europa.eu/cert/newsletter/en/latest_HallOfFame_.html#CERTpolicy).

<sup>269</sup> Typically bug bounties campaigns, i.e., the original developers reward security researchers for reporting vulnerabilities, and thus the discovered vulnerabilities are used for defensive purposes.

<sup>270</sup> Buyers originate from governments, law enforcement and intelligence agencies, the private sector and brokers. Such markets are not directly accessible, but only via requests of confidential information from governments and security vendors to keep the vulnerabilities out of reach of the black market.

<sup>271</sup> Cybercriminals are the typical buyers of this market. If not contented with the available grey markets or due to difficulties to obtain zero-day exploits because of international restrictions and regulations, governments may also be circumstantial buyers. The prices in this market are much steeper than those in the other two types of markets.

<sup>272</sup> In software, security by default, requires that the default configuration settings are the most secure settings possible, without even the end-user knowing it is there, or having to enable it. For example, a social networking website should set users’ profile settings in the most privacy-friendly option in an effort to limit right from the onset the accessibility of the users’ profile to third persons.

<sup>273</sup> The term “fog of war” is attributed to the 19<sup>th</sup>-century Prussian military writer Carl von Clausewitz. It pertains to the uncertainty faced by militaries during a period of war; each side does not fully comprehend or is aware of the opponent’s threat as well as their own capacity to confront it. In the same mindset is the sceptic saying, “I know that I know nothing” ascribed to the ancient classical Greek philosopher Socrates (actually the expression refers to an interpretation of Plato’s account of Socrates’ life).

<sup>274</sup> Benjamin Brewster wrote in “The Yale Literary Magazine” of Feb. 1882 “... in theory there is no difference between theory and practice, while in practice there is”.

list. As a response to this need, very recently, the R Street Institute<sup>275</sup> has launched an initiative which resulted in a partial annotated bibliography entitled *“Resources for measuring cybersecurity”* (Waldron, 2019). In fact, the authors pinpoint that in an effort to assess cyber risk, organisations typically call for or rely on (a) industry standards and scorecards, like the NIST cybersecurity scorecard (Wagner, 2017), (b) cyber insurance metrics (note that cyber insurance is a thriving field during the last few years), despite the fact that according to (Society of Actuaries, 2017) *“Cybersecurity insurance has no standard scoring systems or actuarial tables”*, (c) adjusted or variants of Return on Investment (ROI) legacy equations called Return of Security Investment (ROSI), (d) loss/damage forecasts in terms of, say, monetary or intellectual property loss and by measuring how the deployed security controls perform in mitigating that damage, although cybercrime activities and especially near-misses<sup>276</sup> are often left unreported, and (e) tools and methodologies offered by the Cyber Risk Economics CYRIE project<sup>277</sup> organised by the U.S. Department of Homeland Security Science and Technology Directorate. For obtaining a holistic view on this matter, the reader may refer to (HSSEDI, 2018) as well.

In this context, it is also not to be neglected that for cybercriminals the incentives are crystal clear and, within their capacity, they operate as they see fit. They are bolder and more brazen than ever before, they crowdsource their attacks, they swiftly adapt and innovate to any change, and they capitalise on the elements of maneuver, misdirection, distraction, and surprise to distract the attention of the defenders and inhibit them from seeing and weighting the evidence<sup>278</sup>. Cyberattack methods are becoming increasingly “asymmetric”, i.e., varied, stealthier, uneven, unorthodox, and persistent. Cybercriminals seek to attain the first mover advantage by exploiting the feeblest link, either human or technical, and concentrate on bypassing, undermining, or sabotaging the victim’s strengths. This way, they maximize the inflicted damage, including shock, confusion, and disorder. Even the tools exploited to mount a cyberattack become increasingly ubiquitous, low-cost, and “end-user friendly”. This asymmetric potential, namely flexibility, adaptability, and unpredictability, gives them a salient advantage over defenders who typically do not enjoy such freedom, given that organisations are typically characterised by a strict hierarchy, often having conflicting and/or biased perceptions about risk, which amongst others may hamper decision making, and thus can be seen as an insider threat too. Also, executive management goals regarding risk management and cyber-defence are in several occasions misaligned to that of those who must implement these strategies and put them into practice. Plainly, the worrying reality is that still many organisations think of cybersecurity simply as a compliance exercise<sup>279</sup>, and of course, compliance does not equal security.

On top of that, in the whole process of risk management, lurk inherent traits of human nature that unconsciously affect one’s perception about risk, including the Peltzman and the Dunning-Kruger effects<sup>280</sup>, selective attention (what one pays attention to), *“historical paranoia”*<sup>281</sup>, sunk cost fallacy<sup>282</sup>, and the fact that

---

<sup>275</sup> A non-profit, nonpartisan, public policy research organisation headquartered in Washington, DC, USA. URL: <https://www.rstreet.org/>.

<sup>276</sup> Offensive, fraudulent or any other harmful event which was somehow prevented or was partially successful, suspicious activity that was uncovered by luck or providence, or deliberate or unconscious mistakes which were discovered by luck or coincidence or otherwise. For instance, a tablet containing classified intelligence information was left behind in some airport’s bathroom. Luckily, the tablet was discovered by the janitor who turned it in to the airport’s security department.

<sup>277</sup> URL: <https://www.dhs.gov/science-and-technology/cyrie>

<sup>278</sup> Think for example of a case where the aggressor, being a bot-herder, hacks into a bank and makes several unauthorised money transfers. Immediately after that, they instruct their bots to launch a distributed DoS attack on the bank’s information systems infrastructure. In this way, they hit two birds with one stone; they create confusion to distract the bank’s IT personnel from identifying the fraud (the security officers are now extremely busy in restoring the bank’s system back to normal), and the bank’s clients are incapable of logging in to their accounts to realise that they were robbed. Note that the opponent does not need even to command a botnet. They can instead hire one from the plethora of Attack-as-a-Service services out there. Such a service as well as similar ones, namely Malware-as-a-Service, Fraud-as-a-Service, etc., exploit cloud-based architectures and the dark web, and offered in the underground economy as a response to a demand in constant growth. They are based on a subscription or flat-rate fee making them ideal to “customers”.

<sup>279</sup> Paradoxically, in a Dec. 2018 analysis of the top 100 global companies by market value done by KrebsonSecurity, was found that only 5% included a chief information security officer or chief security officer among the company’s executive leadership team. KrebsonSecurity further pinpoints that fewer than half of high-tech firms that make up the top 50 companies in the NASDAQ market listed a chief technology officer in their executive ranks, and *“only three featured a person with a security title”*.

<sup>280</sup> The Peltzman effect refers to risk compensation, an aspect of psychological theory of behavioral adaptation, postulating that humans adapt their behaviour depending on the perceived level of risk, i.e., they are more cautious in situations when they think the risk is greater, and reckless when they think they are more secure, say, because some compulsory security regulations are in place. The Dunning-Kruger effect in psychology refers to a cognitive bias according to which a large portion of humans assess their cognitive ability to be superior to what it really is, creating an illusory, inflated self-image. This obviously leads to a human-asset prone to manipulation and compromise via, say, social engineering techniques. That is, often such persons do not respond well to criticism, do not abide by instructions or guidelines, and are susceptible to pandering, flattery, jealousies, etc. Much earlier, Socrates, the Greek ancient philosopher, said *“I do not think that I know what I do not know.”*

<sup>281</sup> Chief Security Officer Andy Ellis defines “historical paranoia” as the situation *“where the focus is on not doing something that previously got someone else in trouble, without explaining why”*.

<sup>282</sup> For instance, many organisations insist spending disproportionately on network perimeter security, although attack strategies, including watering holes, phishing, and SQL injection are particularly effective in punching holes in the perimeter.

humans typically value something based on what they have to turn over to acquire it. As a result, even if the organisation's strategic risk management and cybersecurity plan is approved by the senior staff, the reality shows that only half of these organisations eventually implement the plan to its entirety<sup>283</sup>. Internationally renowned security technologist, Bruce Schneier characteristically writes in his 2008 article titled "Does Risk Management Make Sense?" (Schneier, 2008): *"There's never just one risk, of course, and bad risk management decisions often carry an underlying tradeoff. Terrorism policy in the U.S. is based more on politics than actual security risk, but the politicians who make these decisions are concerned about the risks of not being re-elected. Many corporate security decisions are made to mitigate the risk of lawsuits rather than address the risk of any actual security breach. And individuals make risk management decisions that consider not only the risks to the corporation, but the risks to their departments' budgets, and to their careers. You can't completely remove emotion from risk management decisions, but the best way to keep risk management focused on the data is to formalize the methodology. That's what companies that manage risk for a living - insurance companies, financial trading firms and arbitrageurs - try to do. They try to replace intuition with models, and hunches with mathematics"*.

A pertinent remark of this situation is that although Small and Medium-sized Enterprises (SME) comprise the foundation of EU's economy<sup>284</sup>, they are at the same time the feebler victims for cyberattacks<sup>285</sup>. That is, SME idiosyncrasies, including lack of formal cybersecurity policies, skills and expertise, shortage of financial resources, and incorrect attitudes toward risk management and cybersecurity, influence negatively their resilience<sup>286</sup> to security-threats. In line with this viewpoint, frequently, there exist misaligned incentives across network/service providers and other related parties. For instance, while ingress packet filtering (Ferguson & Senie, 2000) have been ratified almost 20 years ago, it has largely missed to resolve the persistent threat of source IP address spoofing due to fundamental incentive misalignment, that is, network providers only assist other networks by implementing the aforementioned practice and do not directly help themselves. This situation ultimately leads to a free riding phenomenon: Stakeholders will not bother investing in cybersecurity if they know or suspect that the rest of the players will not invest, leaving them vulnerable in any case (Varian, 2004). Moreover, as highlighted in (Shackelford, 2014), *"organizations with more lax security become free riders that increase the risk of cyberattacks on other stakeholders, including suppliers"*.

## 22.8 EU and International cybersecurity and cyber risk policy landscape

Arguably, the most significant actors in the cybersecurity risk management arena are the countries per se. That is, everything starts by grasping the country's short- or mid-term strategic vision and plan and deciding the roadmap and actions toward reaching a particular goal in the long-term. Having this in mind, a basic priority of governments, senior statesmen, national and EU-level leaders, policy makers, agencies for cybersecurity, Computer Security Incident Response Team (CSIRT) networks<sup>287</sup>, public-interest technologists<sup>288</sup>, along with other groups of influencers<sup>289</sup> should be the shaping of a comprehensive cybersecurity strategy - accompanied by the appropriate resources that will fund initiatives - that stipulates a competent authority in charge of the national cybersecurity posture of the country. For instance, Netherlands have estimated that by 2020, at least 25% of the country's Gross Domestic Product (GDP) will be owed to the digital economy, thus

<sup>283</sup> McAfee Report, *"Tilting the Playing Field: How Misaligned Incentives Work Against Cybersecurity"*, Feb. 2017 URL: <https://www.mcafee.com/us/resources/reports/rp-misaligned-tilting-playing-field.pdf>

<sup>284</sup> EU's Annual report on European SMEs – 2016/2017 - Focus on self-employment, URL: <https://www.eubusiness.com/topics/sme/sme-report-16-17>.

<sup>285</sup> An Oct. 2018 report by a UK-based insurance group estimates that (a) *"UK small businesses targeted with 65K attempted cyberattacks per day, (b) A small business in the UK is successfully hacked every 19 sec, and (c) cyber breaches cost the average small business £25,7K in basic 'clear up' costs every year"*, URL: <https://www.hiscoxgroup.com/news/press-releases/2018/18-10-18>. Remarkably, the University of Maastricht disclosed that paid a Bitcoin ransom of 200K Euros to hackers who infected the university's system with malware on Dec. 2019 after an employee fell for a phishing attack, URL: <https://www.reuters.com/article/us-cybercrime-netherlands-university/university-of-maastricht-says-it-paid-hackers-200000-euro-ransom-idUSKBN1Z22HH>.

<sup>286</sup> According to (Ross et al., 2019), the term "resilience in cyberspace" is defined as *"The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption"*.

<sup>287</sup> ENISA, *"CSIRTs by Country interactive map"*, URL: <https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map>.

<sup>288</sup> Bruce Schneier defines the term "public-interest technologist" as *"people who combine their technological expertise with a public-interest focus: by working on tech policy, by working on a tech project with a public benefit, or by working as a traditional technologist for an organization with a public benefit"* (Schneier, 2019b).

<sup>289</sup> Cambridge University's Professor David Spiegelhalter, in his Jan. 2009 article in "The Times" titled *"Probability lessons may teach children how to weigh life's odds and be winners"*, pinpointed that *"I regard myself as part of a movement we call risk literacy. It should be a basic component of discussion about issues in media, politics and in schools."*, URL: <https://www.thetimes.co.uk/article/probability-lessons-may-teach-children-how-to-weigh-lifes-odds-and-be-winners-2fkmkdv6nx3>. The interested reader may also refer to the works of Professor Gerd Gigerenzer entitled *"Reckoning with Risk: Learning to Live with Uncertainty"* (Gigerenzer, 2003), and *"Risk Savvy: How To Make Good Decisions"* (Gigerenzer, 2015).

deliberately acknowledging that their future development and growth relies on their capacity to safeguard their digital economy. Certainly, to achieve such a goal, it requires doing the necessary investments and structural reforms, and always have in mind that the future is coming faster than the current set of policy tools can cope with.

Plainly, almost no one will dispute that the design, implementation, and constant re-evaluation of a robust national cybersecurity strategy along with the associated risk management processes, is a sine qua non in securing the national cyber infrastructure and services, and strengthening the nation's digital sovereignty overall – nowadays, cybersecurity is national security. This will also cater for bolstering and securing the digital future and economic well-being on which every nation depends for its survival and prosperity.

In this mindset, the following subsections outline the most significant efforts done so far by countries, unions of states, agencies for cybersecurity, academia, and think tanks to mold and develop security and risk management strategic plans and frameworks.

### **22.8.1 EU landscape**

The EU spurs or enforces, either directly or indirectly, security and risk management practices on Member States, critical infrastructures, and operators of essential services. First off, the EU endorsed a cybersecurity strategy in 2013, where cybersecurity is defined as *“the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein”* (EU, 2013). The importance of cybersecurity is also emphasised in the *“European Agenda on Security”* ratified in April 2015 - *“Cybersecurity is the first line of defence against cybercrime”* (EU, 2015). Jointly these two documents portray the EU policies and initiatives on cybersecurity and cybercrime, ranging from legislation to increasing Member State capabilities and fostering intra-EU and international synergies.

In July 2016, the EU Network and Information Security Directive (NISD) (EU, 2016a) has been adopted. Amongst others, this directive requires essential service operators in Member States to impose appropriate security measures and alert their relevant national competent authority or CSIRT upon any major cybersecurity incident: *“It is essential that all Member States have minimum capabilities and a strategy ensuring a high level of security of network and information systems in their territory. In addition, security and notification requirements should apply to operators of essential services and to digital service providers to promote a culture of risk management and ensure that the most serious incidents are reported”*. Accountability, as it is enforced in this case, may lower cyber risk given that it is pushing industry and relevant players to act upon toward reducing vulnerabilities and strengthening cyber resilience. Also, the EU and the European Cyber Security Organisation (ECSO) signed a *“Cyber Security contractual Public-Private Partnership”* (cPPP) in July 2016 (ESCO, 2016). This partnership intends to empower the cooperation between the public and private sectors by supporting all types of projects or initiatives that concentrate on developing and promoting cybersecurity in the Union.

In March 2017, the report issued by the High Level Advisory Group of the EC Scientific Advice Mechanism (EU, 2017b) provides the European stance *“on cybersecurity in the Digital Single Market directed towards EU-level policy makers”*. The report offers ten recommendations in an effort to *“inform a revised cybersecurity policy which enables a strong and growing Digital Single Market where security, innovation, citizen participation and informed choice go hand in hand with protecting fundamental rights and European values”*.

Moreover, in Sept. 2017, the Commission released a package of high-level measures to horizontally address growing challenges and build a strong EU cybersecurity. To date, this joint communication on Cybersecurity (EU, 2017a) represents the most comprehensive piece of EU policy making regarding cybersecurity. The communication assembles all measures in the three fundamental aspects of European cybersecurity policy, namely:

- Resilience: Promoting cybersecurity and enabling effective responses to cyberattacks in the EU building cyber resilience and strategic autonomy;
- Deterrence: Measures aimed in enabling more effective law enforcement response to dissuade, detect, trace, and prosecute perpetrators of cyberattacks;
- Defence: Strengthening international cooperation on cybersecurity.

In the same month of 2017, the “Cybersecurity Act” proposed regulation (EC, 2017c) provided the basis for a European Cybersecurity certification Framework, which centres on the definition of cybersecurity certification processes and standards for ICT products. As far as the hybrid (cyber) threats are concerned, the Union has issued two joint communication reports to the European parliament and the council titled “*Joint Framework on Countering Hybrid Threats*” (EU, 2016b) in April 2016, and “*Increasing resilience and bolstering capabilities to address hybrid threats*” in June 2018 (EU, 2018a). In the same line of thought, in June 2017, the Council adopted the draft Council conclusions on a “*Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (“Cyber Diplomacy Toolbox”)*”. Once approved, this Toolbox will offer the means of coordinating a response of EU Member States to malicious cyber activities at the EU level<sup>290</sup>.

On top of that, in Sept. 2017, the Commission ratified a recommendation (“*Blueprint*”) addressing severe, large-scale cybersecurity incidents, which are deemed crisis (EU, 2017d). The Blueprint gives directions on “*how well-established Crisis Management mechanisms should make full use of existing cybersecurity entities at EU level as well as of cooperation mechanisms between the Member States*”. Further, in Sept. 2018, the EU issued a proposal for the creation of a regulation for the sake of strengthening cybersecurity capability via a network of cybersecurity competence centres coordinated by a European Cybersecurity Competence Centre (EU, 2018b).

In March 2019, the Union has proposed an array of operational steps and measures to guarantee a high and homogenous level of cybersecurity of 5G networks in the Union (EU, 2019). The recommendation identifies three actions which should be taken to enable: (a) “*Member States to assess the cybersecurity risks affecting 5G networks at national level and take necessary security measures*” (b) “*Member States and relevant Union institutions, agencies and other bodies to develop jointly a coordinated Union risk assessment that builds on the national risk assessment*”, and (c) “*The Cooperation Group set up under Directive (EU) 2016/1148 to identify a possible common set of measures to be taken to mitigate cybersecurity risks related to infrastructures underpinning the digital ecosystem, in particular 5G networks*”.

In the context of Horizon 2020 (H2020), the pilot research projects titled CONCORDIA, ECHO, SPARTA and CyberSec4Europe are launched in expectation to advance and boost the EU's cybersecurity capacity and address forthcoming challenges toward a safer European digital single market. Finally, some other H2020 funded projects, like the EUNITY one on “*Cybersecurity and Privacy Dialogue between Europe and Japan*”, aim at fuelling and ultimately developing the dialogue between Europe and third countries on cybersecurity and privacy research.

## 22.8.2 International landscape

In U.S., NIST has published the “*Framework for Improving Critical Infrastructure Cybersecurity*” in Feb. 2014 (Barrett, 2018), which contains a set of voluntary standards to assist organisations in assessing, managing, and responding to cybersecurity risks. According to the framework, risk evaluation is driven by five components, namely identify, protect, detect, respond, and recover. Not less important, the appendix to this document maps NIST Cybersecurity Framework's risk reduction categories to a number of internationally agreed standards. In Sept. 2017, NIST updated its special publication on “*Risk Management Framework for Information Systems and Organisations: A System Life Cycle Approach for Security and Privacy*” (NIST, 2018). The goal of this framework is to assist organisations in identifying high-value assets and high-impact systems, for the sake of better assessing operational risk. It also proposes a method to decide on security and privacy controls and evaluate their effectiveness. On top of that, in Sept. 2018, the U.S. government released a National Cyber Strategy (U.S. Government, 2018), which adopts a more offensive cybersecurity posture, and is aligned with the U.S. Department of Defense's (DoD) new Cyber Strategy in 2018 (U.S. DoD, 2018), which marks out the military's role in relation to cyberspace. More interestingly, the latter document induces the concept of defending “*forward*”: “*... We will defend forward to halt or degrade cyberspace operations targeting the Department, and we will collaborate to strengthen the cybersecurity and resilience of DoD and non-DoD Defense Critical Infrastructure and Defense Industrial Base entities networks and systems*”.

China on the other hand, seems to follow a similar approach to EU by embedding elements of the NIS Directive into its new national cybersecurity law that became active in June 2017 (People's Republic of China, 2019). This law states explicitly the responsibilities of relevant government agencies, Internet service providers, and end-users. Precisely, relevant organisations, that is, any network or service provider and especially any critical information infrastructure operator that would endanger national security if

---

<sup>290</sup> However, as of today, there is no global agreement about the way legacy rules or laws of diplomacy and conventions will fit and apply to the multidimensional, multilayered, and asymmetric battlescape of cyberspace (Guiora, 2017). Graphically, it can be said that no flags, uniforms, and mutually established rules of engagement exist.



compromised, must establish stringent technical or other necessary type of measures, such as establish a specialised security management body, carry out disaster recovery backups, etc., to make sure the Internet is safe and available, deal with cybersecurity incidents adequately, deter and prevent cybercriminal activities, and preserve the integrity, secrecy, and usability of internet data.

Cybersecurity is a major topic in the agenda of Russian Federation as well. Precisely, in July 2017, Russia adopted Federal law No. 187-FZ addressing the security of critical information infrastructures, namely, telecommunication networks and information systems of state authorities, and generally any kind of system and network supporting transportation, healthcare, communication, finance, energy, etc., which is considered vital for the economy, and thus should be protected against cyber threats. In essence, this law outlines the doctrines for ensuring the security of such infrastructures, including the involved state authorities, and the rights, responsibilities, and obligations of any direct or indirect proprietor of such facilities, not excepting all the cooperating communication providers and information systems. Under this law, such facilities must enforce sufficient protection measures and register with Federal Service for Technical and Export Control (FSTEK). To cope with the risks related to the illicit use and potential abuse of information systems, any software produced abroad, especially those related to ICT security, like firewalls, antivirus applications, or any software using encryption, is subject to review by certified Russian agencies. This means that before a piece of software is imported and sold in Russia, its source code may be examined to ensure that is, say, backdoor-free.

In addition, the Federal law No. 90-FZ was introduced in April 2019, imposing strict controls over the Internet within the Russian Federation. The goal of this law is to protect Russian websites and online services from external threats, and to block any prohibited or unwanted services, especially those hosted by foreign-based providers. Simply put, the law provides the cornerstone for isolating the Russian segment of the Internet from the rest of the World Wide Web (WWW) - allegedly with the use of a parallel "national DNS infrastructure" - therefore the so-called "Runet" will still remain operational in the advent of a foreign cyberattack. Regarding this latter point, the debate about "sovereignty in cyberspace" is ongoing and in its core is a problem of misalignment. That is, there is an obvious mismatch between the internet's single space multinational realm for societal interaction, and the areal boundaries of national governments. So, a key question arises here in relation to whether sovereignty in cyberspace can exist hand in hand with globalised connectivity; will national borders in cyberspace eventually soften risks and strengthen security and order?

In Jan. 2020, the Australian Cyber Security Centre within the Australian Signals Directorate of the Australian Government concluded the *"Australian Government Information Security Manual"* (Australian Cyber Security Center, 2020). The manual, destined for information security officers, cybersecurity professionals and information technology managers, provides strategic guidance and portrays *"a cybersecurity framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats"*. It offers cybersecurity principles grouped into key activities, namely govern (identify and manage security risks), protect (implement security controls to reduce security risks), detect (detect and understand cyber security events), and respond (respond to and recover from cybersecurity incidents). The manual underlines that *"organisations should be able to demonstrate that the cybersecurity principles are being adhered to within their organisation"*. Additionally, the Australian Government has developed a *"Protective Security Policy Framework"* (The Australian Government, 2019) with the purpose to help *"entities to protect their people, information and assets, at home and overseas"*. The framework comprises five principles to apply to every major area of security, four security desired outcomes, sixteen core requirements which detail on what entities must do to achieve the government's desired outcomes, and guidance. Also, the framework contains a security planning and risk management policy illustrating *"how entities establish effective security planning and can embed security into risk management practices"*.

Regarding international frameworks, in 2007, the International Telecommunications Union (ITU) announced its Global Cybersecurity Agenda (GCA) and published a framework that spurs intra- and inter-cooperation between the involved parties. In a next step in 2011, ITU developed the National Cybersecurity Guide, which amongst others concentrates on national values and culture, as the cornerstones of any efficient national strategy development, and offers guidelines to governments that wish to face cybersecurity as a strategic national policy area and not just as a technical issue. Later on, in 2014, the ITU announced a Global Cybersecurity Index (GCI) to assist countries in evaluating their cybersecurity strategies and programs against those implemented by other countries. In the same context, in 2018, the World Economic Forum (WEF) published its Cyber Resilience Playbook for Public-Private Collaboration (World Economic Forum, 2018). The goal of this endeavor is to steer public-private collaboration on cybersecurity policy development. It also highlights on the need for constructing a clear national cyber governance framework, including unambiguous roles and responsibilities.

### 22.8.3 Others

Academia, think tanks, cybersecurity agencies, and relevant communities have also started compiling methodologies to assist countries and organisations ameliorate their cyber preparedness. The Cyber Readiness Index 2.0 (CRI), created in 2015 by a team of experts at the Potomac Institute for Policy Studies, offers an experience-based methodological framework for assessing a country's cyber readiness. Also, the Oxford Cyber Security Capacity Maturity Model (CMM), released in 2016 by the Global Cyber Security Capacity Centre (GCSCC) at Oxford University, sketches different levels of countries' cybersecurity maturity based on five pillars, namely (a) cybersecurity policy and strategy, (b) cyber culture and society, (c) cybersecurity, education, training, and skills, (d) legal and regulatory frameworks, and (e) standards, organisations, and technologies, and can be used toward diagnosing cyber preparedness.

The e-Governance Academy in Estonia developed a multi-region National Cyber Security Index (NCSI) (Estonia's e-Governance Academy, 2020), which measures countries' readiness level on cybersecurity, and tracks down the major priorities that need to be addressed per country so as to prevent and fight against cyberattacks and crimes.

The European Union Agency on Cybersecurity (ENISA) has published a report on risk assessment on cloud computing business model and technologies, titled *"Benefits, risks and recommendations for information security"* (ENISA, 2012) in the context of the Emerging and Future Risk Framework project. This effort has been bolstered by groups of experts from industry, academia and governmental organisations. Additionally, in Nov. 2019, ENISA published a report titled *"Good practices in innovation on Cybersecurity under the National Cyber Security Strategies (NCSS)"*. This report concentrates on three aspects of innovation, namely Innovation Priorities, Industrialisation and Collaboration, and Market and Policy, and incorporates several key findings and recommendations (ENISA, 2019a). Given that the global 5G rollout has just started, bringing a sizable, if not unprecedented, impact in the economy and society, ENISA published in Nov. 2019 its *"Threat Landscape for 5G networks"* (ENISA, 2019b). Among others, the report focuses on the identification of key assets in the 5G ecosystem, provides a threat taxonomy map, and interrelates risk scenarios to cyber threats. In the same month of 2019, ENISA published the *"EU Member States incident response development status report"* (ENISA, 2019c). This report offers *"a deeper insight into NISD sectoral Incident Response capabilities, procedures, processes and tools to identify the trends and possible gaps and overlaps"*, and pinpoints seven key findings related to this matter. Other notable contributions of ENISA include the *"ENISA good practices for security of Smart Cars"* (ENISA, 2019d), *"Port Cybersecurity - Good practices for cybersecurity in the maritime sector"* (ENISA, 2019e), and *"Good Practices for Security of IoT - Secure Software Development Lifecycle"* (ENISA, 2019f) published also in Nov. 2019. Last but not least, ENISA maintains an interactive map containing the NCSS per EU Member State along with their guidelines on implementation and information sharing (ENISA, 2020).

## 22.9 References

- Ablon L. and Bogart A., "Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits," 2017. [Online]. Available: [https://www.rand.org/pubs/research\\_reports/RR1751.html](https://www.rand.org/pubs/research_reports/RR1751.html). [Accessed: 07-Dec-2020].
- Ablon L., Libicki M. C., and Abler A. M., "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," 2014. [Online]. Available: [https://www.rand.org/pubs/research\\_reports/RR610.html](https://www.rand.org/pubs/research_reports/RR610.html). [Accessed: 07-Dec-2020].
- Aven, T. "The risk concept - historical and recent development trends," Reliability Engineering & System Safety, vol. 99, pp. 33-44, Mar. 2012, DOI: 10.1016/j.ress.2011.11.006.
- Baer M., "Cybersecurity is a Social Justice Issue | Fels Institute of Government," Nov-2017. [Online]. Available: <https://www.fels.upenn.edu/recap/posts/1404>. [Accessed: 07-Dec-2020].
- Barrere M., Badonnel R., and Festor O., "Vulnerability Assessment in Autonomic Networks and Services: A Survey," IEEE Communications Surveys Tutorials, vol. 16, no. 2, pp. 988-1004, Second 2014, DOI: 10.1109/SURV.2013.082713.00154.
- Barrett M. P., "Framework for Improving Critical Infrastructure Cybersecurity." NIST, 2018.
- Beebe N. L., and Chang F. R., "Cybersecurity: Revisiting the Definition of Insider Threat," NAE Website, 2019. [Online]. Available: <https://nae.edu/216551/Cybersecurity-Revisiting-the-Definition-of-Insider-Threat>. [Accessed: 07-Dec-2019].

Bellovin S. M., "Attack Surfaces," IEEE Security Privacy, vol. 14, no. 3, pp. 88–88, May 2016, DOI: 10.1109/MSP.2016.55.

Caltagirone S., Pendergast A., and Betz C., "The Diamond Model of Intrusion Analysis," CENTER FOR CYBER INTELLIGENCE ANALYSIS AND THREAT RESEARCH HANOVER MD, Jul. 2013.

Caralli R. A., Stevens J. F., Young L. R., Wilson, W. R., "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. | National Technical Reports Library - NTIS," May 2007.

Cassotta S. and Pettersson M., "Climate Change, Environmental Threats and Cyber-Threats to Critical Infrastructures in Multi-Regulatory Sustainable Global Approach with Sweden as an Example," Beijing Law Review, vol. 10, no. 3, pp. 720–726, Jun. 2019, DOI: 10.4236/blr.2019.103035.

Center for Internet Security, 2020. "CIS Controls V7 Measures and Metrics," Jan-2020. [Online]. Available: <https://www.cisecurity.org/white-papers/cis-controls-v7-measures-metrics/>. [Accessed: 07-Dec-2020].

Cherdantseva Y. et al., "A review of cyber security risk assessment methods for SCADA systems," Computers & Security, vol. 56, pp. 1–27, Feb. 2016, DOI: 10.1016/j.cose.2015.09.009.

Cisco Systems, 2020. "Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper," Cisco, Updated March 9, 2020. [Online]. Available: <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html>. [Accessed: 31-Jan-2020].

Cleland-Huang J., "How Well Do You Know Your Personae Non Gratae?," IEEE Software, vol. 31, no. 4, pp. 28–31, Jul. 2014, DOI: 10.1109/MS.2014.85.

CSIS, 2019. "Significant Cyber Incidents - Center for Strategic and International Studies," 2019. [Online]. Available: <https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents>. [Accessed: 7-Dec-2020].

Do C. T. et al., "Game Theory for Cyber Security and Privacy," ACM Comput. Surv., vol. 50, no. 2, pp. 30:1–30:37, May 2017, DOI: 10.1145/3057268.

ENISA, 2012. "Cloud Computing: Benefits, risks and recommendations for information security," Rev. B, Dec. 2012. [Online]. Available: <https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/view>. [Accessed: 07-Dec-2020].

ENISA, 2016. "Cyber Insurance: Recent Advances, Good Practices and Challenges," Nov-2016. [Online]. Available: <https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges>. [Accessed: 07-Dec-2020].

ENISA, 2019(a). "Good practices in innovation on Cybersecurity under the NCSS," Nov-2019. [Online]. Available: <https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1>. [Accessed: 07-Dec-2020].

ENISA, 2019(b). "ENISA threat landscape for 5G Networks," Nov-2019. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks>. [Accessed: 07-Dec-2020].

ENISA, 2019(c). "EU Member States incident response development status report," Nov-2019. [Online]. Available: <https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report>. [Accessed: 07-Dec-2020].

ENISA, 2019(d). "ENISA good practices for security of Smart Cars," Nov-2019. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-good-practices-for-security-of-smart-cars>. [Accessed: 07-Dec-2020].

ENISA, 2019(e). "Port Cybersecurity - Good practices for cybersecurity in the maritime sector," Nov-2019. [Online]. Available: <https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector>. [Accessed: 07-Dec-2020].

ENISA, 2019(f). "Good Practices for Security of IoT - Secure Software Development Lifecycle," Nov-2019. [Online]. Available: <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1>. [Accessed: 07-Dec-2020].

ENISA, 2020. "National Cyber Security Strategies - Interactive Map," Jan-2020. [Online]. Available: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map>. [Accessed: 07-Dec-2020].

- EPRI, 2020. Electric Power Research Institute (EPRI), “The National Electric Sector Cybersecurity Organization Resource (NESCOR).” [Online]. Available: <https://smartgrid.epri.com/NESCOR.aspx>. [Accessed: 07-Dec-2020].
- ESCO, 2016. European Cyber Security Organisation (ESCO), “Cyber Security contractual Public-Private Partnership,” ECSO - European Cyber Security Organisation, Jul-2016. [Online]. Available: <https://ecs-org.eu/cppp>. [Accessed: 07-Dec-2020].
- Estonia’s e-Governance Academy, 2020. “National Cyber Security Index,” 2020. [Online]. Available: <https://ncsi.ega.ee/>. [Accessed: 07-Dec-2020].
- EU JRC, 2018. “European Cybersecurity Centres of Expertise Map - Definitions and Taxonomy,” EU Science Hub - European Commission, 10-Sep-2018. [Online]. Available: <https://ec.europa.eu/jrc/en/publication/european-cybersecurity-centres-expertise-map-definitions-and-taxonomy>. [Accessed: 7-Dec-2020].
- EU, 2013. “Joint Communication to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN/2013/01,” 2013. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001>. [Accessed: 07-Dec-2020].
- EU, 2015. “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - The European Agenda on Security - COM/2015/0185,” Apr-2015. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0185>. [Accessed: 07-Dec-2020].
- EU, 2016(a). Directive 2016/1148, “Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.” Jul-2016.
- EU, 2016(b). “Joint Communication to the European Parliament and the Council - Joint Framework on countering hybrid threats a European Union response - JOIN(2016) 18,” Apr-2016. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018>. [Accessed: 07-Dec-2020].
- EU, 2017(a). “Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU - JOIN/2017/0450,” Sep-2017. [Online]. Available: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450>. [Accessed: 7-Dec-2020].
- EU, 2017(b). EU Scientific Advice Mechanism - High Level Group of Scientific Advisors, “Cybersecurity in the European Digital Single Market,” Scientific Opinion No. 02/2017, Mar. 2017. [Online]. Available: [https://ec.europa.eu/research/sam/pdf/sam\\_cybersecurity\\_report.pdf](https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf). [Accessed: 07-Dec-2020]. [108]
- EU, 2017(c). “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the ‘EU Cybersecurity Agency’, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (‘Cybersecurity Act’), COM/2017/0477 final - 2017/0225 (COD),” Sep-2017. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN>. [Accessed: 07-Dec-2020].
- EU, 2017(d). “Commission Recommendation 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises,” Sep-2017. [Online]. Available: <https://eur-lex.europa.eu/eli/reco/2017/1584/oj>. [Accessed: 07-Dec-2020].
- EU, 2018(a). “Joint Communication to the European Parliament and the Council - Increasing resilience and bolstering capabilities to address hybrid threats - JOIN/2018/16 final,” Jun-2018. [Online]. Available: <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016>. [Accessed: 07-Dec-2020].
- EU, 2018(b). “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres,” Sep-2018. [Online]. Available: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018PC0630>. [Accessed: 30-Jan-2020].
- EU, 2019. “Commission Recommendation (EU) 2019/534 - Cybersecurity of 5G networks,” 32019H0534, Mar. 2019.
- Felderer M. and Schieferdecker I., “A taxonomy of risk-based testing,” *Int J Softw Tools Technol Transfer*, vol. 16, no. 5, pp. 559–568, Oct. 2014, DOI: 10.1007/s10009-014-0332-3.
- Ferguson B., Tall A., and Olsen D., “National Cyber Range Overview,” in 2014 IEEE Military Communications Conference, 2014, pp. 123–128, DOI: 10.1109/MILCOM.2014.27.

Ferguson P., Senie D., "BCP 38 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," May-2000. [Online]. Available: <https://tools.ietf.org/html/bcp38>. [Accessed: 07-Dec-2020].

Fielder A., Panaousis E., Malacaria P., Hankin C., and Smeraldi F., "Game Theory Meets Information Security Management," in *ICT Systems Security and Privacy Protection*, Berlin, Heidelberg, 2014, pp. 15–29, DOI: 10.1007/978-3-642-55415-5\_2.

Ganin A. A. et al., "Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management," *Risk Analysis*, vol. 40, no. 1, pp. 183–199, 2020, DOI: 10.1111/risa.12891.

Gigerenzer G., *Reckoning with Risk: Learning to Live with Uncertainty*, New Ed edition. London: Penguin, 2003, ISBN: 978-0140297867.

Gigerenzer G., *Risk Savvy: How To Make Good Decisions*. New York, NY: Penguin, 2015, ISBN: 978-0143127109.

Gritzalis D., Iseppi G., Mylonas A., and Stavrou V. "Exiting the Risk Assessment Maze: A Meta-Survey," *ACM Comput. Surv.*, vol. 51, no. 1, pp. 11:1–11:30, Jan. 2018, DOI: 10.1145/3145905.

Grossmann J., and Seehusen F., "Combining Security Risk Assessment and Security Testing Based on Standards," in *Risk Assessment and Risk-Driven Testing*, Cham, 2015, pp. 18–33, DOI: 10.1007/978-3-319-26416-5\_2.

Guiora A. N., *Cybersecurity: Geopolitics, Law, and Policy*. Routledge, 2017, ASIN: B06X9ZM48L.

Henry M. H., and Haimes Y. Y., "A Comprehensive Network Security Risk Model for Process Control Networks," *Risk Analysis*, vol. 29, no. 2, pp. 223–248, 2009, DOI: 10.1111/j.1539-6924.2008.01151.x.

Holm H., Sommestad T., Almroth J., and Persson M., "A quantitative evaluation of vulnerability scanning," *Information Management & Computer Security*, vol. 19, no. 4, pp. 231–247, Jan. 2011, DOI: 10.1108/09685221111173058.

HSSEDI, 2018. The Homeland Security Systems Engineering and Development Institute (HSSEDI), "Cyber Risk Metrics Survey, Assessment and Implementation Plan Briefing," Nov. 2018. [Online]. Available: <https://www.mitre.org/publications/technical-papers/cyber-risk-metrics-survey-assessment-and-implementation-plan-briefing>. [Accessed: 07-Dec-2020].

Hu P., Li H., Fu H., Cansever D., and Mohapatra P., "Dynamic defense strategy against advanced persistent threat with insiders - IEEE Conference Publication," 2015.

ISECOM, 2010. The Institute for Security and Open Methodologies (ISECOM), "The Open Source Security Testing Methodology Manual (OSSTMM) Ver. 3," Dec-2010. [Online]. Available: <https://www.isecom.org/OSSTMM.3.pdf>. [Accessed: 07-Dec-2020].

ISO, 2009. "ISO Guide 73:2009 - Risk management - Vocabulary." ISO, 2009.

ISO/IEC, 2010. "ISO/IEC 27033-3:2010(en), Information technology - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues," 2010. [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27033:-3:ed-1:v1:en:term:3.4>. [Accessed: 07-Dec-2020].

ISO/IEC, 2012. "ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity." 2012.

ISO/IEC, 2013(a). "ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements." 2013.

ISO/IEC, 2013(b). "ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls." 2013.

ISO/IEC, 2018(a). "ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary." 2018.

ISO/IEC, 2018(b). "ISO/IEC 31000:2018 Risk management." Feb-2018.

ISO/IEC, 2018(c). "ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management." 2018.

ISO/IEC, 2019. "ISO/IEC 31010:2019 Risk management - Risk assessment techniques." ISO/IEC, Jun-2019.

ISO/TS, 2017. "ISO/TS 12812-2:2017(en), Core banking — Mobile financial services — Part 2: Security and data protection for mobile financial services," 2017. [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:iso:ts:12812:-2:ed-1:v1:en:term:3.4>. [Accessed: 15-Jan-2020].

ITU-T, 2008. "X.1205: Overview of cybersecurity." ITU-T, 2008. [Online]. Available: <https://www.itu.int/rec/T-REC-X.1205-200804-I>. [Accessed: 7-Dec-2020].

Jajodia S., Ghosh A. K., Subrahmanian V. S., Swarup V., Wang C., and Wang X. S., Eds., *Moving Target Defense II: Application of Game Theory and Adversarial Modeling*. New York: Springer-Verlag, 2013.

Johnson C., Badger M., Waltermire D., Snyder J., and Skorupka C., "Guide to Cyber Threat Information Sharing," National Institute of Standards and Technology, NIST Special Publication (SP) 800-150, Oct. 2016.

Karabacak B., and Sogukpinar I., "ISRAM: information security risk analysis method," *Computers & Security*, vol. 24, no. 2, pp. 147–159, Mar. 2005, DOI: 10.1016/j.cose.2004.07.004.

Kolias C., Kambourakis G., Stavrou A., and Voas J., "DDoS in the IoT: Mirai and Other Botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017, DOI: 10.1109/MC.2017.201.

Kruse C. S., Frederick B., Jacobson T., and Monticone D. K., "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technology and Health Care*, vol. 25, no. 1, pp. 1–10, Jan. 2017, DOI: 10.3233/THC-161263.

Landoll D., *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*, Second Edition. CRC Press, 2011, ISBN: 978-1439821480.

LeMay E., Ford M. D., Keefe K., Sanders W. H., and Muehrcke C., "Model-based Security Metrics Using Adversary View Security Evaluation (ADVISE)," in *2011 Eighth International Conference on Quantitative Evaluation of Systems*, 2011, pp. 191–200, DOI: 10.1109/QEST.2011.34.

Leszczyna R., "Standards on cyber security assessment of smart grid," *International Journal of Critical Infrastructure Protection*, vol. 22, pp. 70–89, Sep. 2018, DOI: 10.1016/j.ijcip.2018.05.006.

Leveson N., "A new accident model for engineering safer systems," *Safety Science*, vol. 42, no. 4, pp. 237–270, Apr. 2004, DOI: 10.1016/S0925-7535(03)00047-X.

Li J., Beba S., and Karlsen M. M., "Evaluation of Open-Source IDE Plugins for Detecting Security Vulnerabilities," in *Proceedings of the Evaluation and Assessment on Software Engineering*, Copenhagen, Denmark, 2019, pp. 200–209, DOI: 10.1145/3319008.3319011.

Mead N. R., Shull F., Vemuru K., Villadsen O., "A Hybrid Threat Modeling Method," Mar. 2018.

Microsoft Corporation, 2009. "The STRIDE Threat Model," Dec. 2009. [Online]. Available: [https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878\(v%3dcs.20\)](https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v%3dcs.20)). [Accessed: 07-Dec-2020].

Microsoft Corporation, 2019. "Microsoft Security Development Lifecycle," 2019. [Online]. Available: <https://www.microsoft.com/en-us/securityengineering/sdl>. [Accessed: 07-Dec-2020].

MITRE, 2020. "MITRE ATT&CK," [Online]. Available: <https://attack.mitre.org/>. [Accessed: 07-Dec-2020].

Moore T., Dynes S., and Chang F., "Identifying how firms manage cybersecurity investment," presented at the 15th Workshop on the Economics of Information Security (WEIS), 2016.

Nespoli P., Papamartzivanos D., Marmol F. G., and Kambourakis G., "Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 2, pp. 1361–1396, 2018, DOI: 10.1109/COMST.2017.2781126.

NIST, 2011. "Managing Information Security Risk: Organization, Mission, and Information System View," National Institute of Standards and Technology, NIST Special Publication (SP) 800-39, Mar. 2011.

NIST, 2012. "Guide for Conducting Risk Assessments," National Institute of Standards and Technology, NIST Special Publication (SP) 800-30 Rev. 1, Sep. 2012.

NIST, 2015. "Security and Privacy Controls for Federal Information Systems and Organizations," National Institute of Standards and Technology, NIST Special Publication (SP) 800-53 Rev. 4, Jan. 2015.

NIST, 2018. "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," National Institute of Standards and Technology, NIST Special Publication (SP) 800-37 Rev. 2, Dec. 2018.

NIST, 2019. "Glossary - Computer Security Resource Center (CSRC)," 2019. [Online]. Available: <https://csrc.nist.gov/glossary>. [Accessed: 02-Dec-2019].

OWASP, 2014. "OWASP Testing Guide v4," 2014. [Online]. Available: [https://www.owasp.org/index.php/OWASP\\_Testing\\_Project](https://www.owasp.org/index.php/OWASP_Testing_Project). [Accessed: 07-Dec-2020].

OWASP, 2020. "Threat Modeling Cheat Sheet," Jan-2020. [Online]. Available: [https://cheatsheetseries.owasp.org/cheatsheets/Threat\\_Modeling\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html). [Accessed: 07-Dec-2020].

People's Republic of China, 2019. "Cyber-security Law of the People's Republic of China," 2019. [Online]. Available: <https://www.dezshira.com/library/legal/cyber-security-law-china-8013.html>. [Accessed: 28-Dec-2020].

Pols P., "The Unified Kill Chain," Feb-2018. [Online]. Available: <https://www.csacademy.nl/en/csa-theses/february-2018/104-the-unified-kill-chain>. [Accessed: 28-Nov-2019].

Potteiger B., Martins G., and Koutsoukos X., "Software and attack centric integrated threat modeling for quantitative risk assessment," in Proceedings of the Symposium and Bootcamp on the Science of Security, Pittsburgh, Pennsylvania, 2016, pp. 99-108, DOI: 10.1145/2898375.2898390.

Ross R., Pillitteri V., Graubart R., Bodeau D., and McQuaid R., "Developing Cyber Resilient Systems: A Systems Security Engineering Approach," National Institute of Standards and Technology, NIST Special Publication (SP) 800-160 Vol. 2, Nov. 2019.

Saltzer J. and Schroeder M., "The Protection of Information in Computer Systems," Communications of the ACM, vol. 17, no. 7, Apr. 1975.

Sayakkara A., Le-Khac N.-A., and Scanlon M., "A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics," Digital Investigation, vol. 29, pp. 43-54, Jun. 2019, DOI: 10.1016/j.diin.2019.03.002.

Scarfone K., Souppaya M., Cody A., and Orebaugh A., "Technical Guide to Information Security Testing and Assessment," National Institute of Standards and Technology, NIST Special Publication (SP) 800-115, Sep. 2008.

SCF Council, 2020. Secure Controls Framework Council, LLC (SCF Council), "Security & Privacy by Design Principles," scf-website, Jan-2020. [Online]. Available: <https://www.securecontrolsframework.com/security-privacy-design-principles>. [Accessed: 07-Dec-2020].

Schneier B. (2016a), "Stop Trying to Fix the User," IEEE Security & Privacy Magazine, vol. 14, no. Sept.-Oct., pp. 96-96, 2016.

Schneier B. (2016b), "Cryptography Is Harder than It Looks," IEEE Security Privacy, vol. 14, no. 1, pp. 87-88, Jan. 2016, DOI: 10.1109/MSP.2016.7.

Schneier B. (2019a), "Prices for Zero-Day Exploits Are Rising - Schneier on Security," Jan-2019. [Online]. Available: [https://www.schneier.com/blog/archives/2019/01/prices\\_for\\_zero.html](https://www.schneier.com/blog/archives/2019/01/prices_for_zero.html). [Accessed: 07-Dec-2020].

Schneier B. (2019b), "Cybersecurity for the Public Interest," IEEE Security Privacy, vol. 17, no. 1, pp. 84-83, Jan. 2019, DOI: 10.1109/MSEC.2018.2889891.

Schneier B., "Does Risk Management Make Sense? - Schneier on Security," Oct-2008. [Online]. Available: [https://www.schneier.com/blog/archives/2008/10/does\\_risk\\_manag.html](https://www.schneier.com/blog/archives/2008/10/does_risk_manag.html). [Accessed: 07-Dec-2020].

Shackelford S. J., Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge University Press, 2014, ISBN: 9781139021838.

Shah S., and Mehtre B. M., "An overview of vulnerability assessment and penetration testing techniques," J Comput Virol Hack Tech, vol. 11, no. 1, pp. 27-49, Feb. 2015, DOI: 10.1007/s11416-014-0231-x.

Shevchenko N., Chick T., O' Riordan P., Scanlon T., and Woody C., "Threat Modeling: A Summary of Available Methods," Aug-2018. [Online]. Available: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=524448>. [Accessed: 07-Dec-2020].

Shiva S., Roy S., and Dasgupta D., "Game Theory for Cyber Security," in Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, New York, NY, USA, 2010, pp. 34:1–34:4, DOI: 10.1145/1852666.1852704.

Shostack A., "Experiences Threat Modeling at Microsoft," Jan. 2008. [Online]. Available: <https://adam.shostack.org/modsec08/Shostack-ModSec08-Experiences-Threat-Modeling-At-Microsoft.pdf>. [Accessed: 07-Dec-2020].

Society of Actuaries, 2017. "Cybersecurity Insurance: Modeling and Pricing | SOA," Apr-2017. [Online]. Available: <https://www.soa.org/resources/research-reports/2017/cybersecurity-insurance>. [Accessed: 07-Dec-2020].

Spreitzer R., Moonsamy V., Korak T., and Mangard S., "Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices," IEEE Commun. Surv. Tutorials, vol. 20, no. 1, pp. 465–488, 2018, DOI: 10.1109/COMST.2017.2779824.

The Australian Cyber Security Centre, 2020. "Australian Government Information Security Manual," Jan-2020. [Online]. Available: <https://www.cyber.gov.au/ism>. [Accessed: 07-Dec-2020].

The Australian Government, 2019. "Protective Security Policy Framework," Nov-2019. [Online]. Available: <https://www.protectivesecurity.gov.au/node/45>. [Accessed: 07-Dec-2020].

The LINDDUN Team, 2020. "LINDDUN privacy engineering," LINDDUN, Dec-2020. [Online]. Available: <https://www.linddun.org>. [Accessed: 07-Dec-2020].

The Open Information Systems Security Group, 2006. "Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1," May-2006. [Online]. Available: <https://epdf.pub/information-systems-security-assessment-framework-issaf-draft-021.html>. [Accessed: 07-Dec-2020].

The PTES Team, 2017. "The Penetration Testing Execution Standard (PTES) Ver. 1.1," Feb-2017. [Online]. Available: [http://www.pentest-standard.org/index.php/Main\\_Page](http://www.pentest-standard.org/index.php/Main_Page). [Accessed: 07-Dec-2020].

U.S. DoD, 2018. "Department of Defence Cyber Strategy." U.S. Department of Defence, 2018.

U.S. Government, 2018. "National Cyber Strategy." The White House, 2018.

UcedaVelez T., and Morana, M. M., Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. 2015.

University of Washington, 2013. "The Security Cards: A Security Threat Brainstorming Kit," 2013. [Online]. Available: <http://securitycards.cs.washington.edu/>. [Accessed: 04-Feb-2020].

Varian H., "System Reliability and Free Riding," in Economics of Information Security, L. J. Camp and S. Lewis, Eds. Boston, MA: Springer US, 2004, pp. 1–15.

Wagner U. J., "CSRC Presentation: Creating a Cybersecurity Scorecard | CSRC," CSRC | NIST, 17-Aug-2017. [Online]. Available: <https://csrc.nist.gov/Presentations/2017/Creating-a-Cybersecurity-Scorecard>. [Accessed: 07-Dec-2020].

Wakker P. P., Prospect Theory: For Risk and Ambiguity. Cambridge University Press, 2010.

Waldron K., "Resources for Measuring Cybersecurity | R Street," Oct-2019. [Online]. Available: <https://www.rstreet.org/2019/10/29/resources-for-measuring-cybersecurity/>. [Accessed: 07-Dec-2020].

Wang C. and Lu Z., "Cyber Deception: Overview and the Road Ahead," IEEE Security Privacy, vol. 16, no. 2, pp. 80–85, Mar. 2018, DOI: 10.1109/MSP.2018.1870866.

Wangen G., Hallstensen C., and Snekenes E., "A framework for estimating information security risk assessment method completeness," Int. J. Inf. Secur., vol. 17, no. 6, pp. 681–699, Nov. 2018, DOI: 10.1007/s10207-017-0382-0.

World Economic Forum, 2018. "Cyber Resilience: Playbook for Public-Private Collaboration," 2018. [Online]. Available: [http://www3.weforum.org/docs/WEF\\_Cyber\\_Resilience\\_Playbook.pdf](http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf). [Accessed: 07-Dec-2020].

Wuyts K., Van Landuyt D., Hovsepyan A., and Joosen W., "Effective and efficient privacy threat modeling through domain refinements," in Proceedings of the 33rd Annual ACM Symposium on Applied Computing, Pau, France, 2018, pp. 1175–1178, DOI: 10.1145/3167132.3167414.



Xiao L., Xu D., Xie C., Mandayam N. B., and Poor H. V., "Cloud Storage Defense Against Advanced Persistent Threats: A Prospect Theoretic Study," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 3, pp. 534–544, Mar. 2017, DOI: 10.1109/JSAC.2017.2659418.

Yang L.-X., Li P., Yang X., and Tang Y. Y., "A risk management approach to defending against the advanced persistent threat," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2018, DOI: 10.1109/TDSC.2018.2858786.

Yang L.-X., Li P., Zhang Y., Yang X., Xiang Y., and Zhou W., "Effective Repair Strategy Against Advanced Persistent Threat: A Differential Game Approach," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1713–1728, Jul. 2019, DOI: 10.1109/TIFS.2018.2885251.

## 23 Hybrid Threats

GEORGIOS GIANNOPOULOS, GEORGIOS THEODORIDIS, MARIANTHI THEOCHARIDOU, LUCA GALBUSERA

### 23.1 Introduction

The “hybrid threats” (HT) term has been proposed by Hoffman (2007) to frame modern conflict and the threats faced by the US in the military domain. According to the author, *“hybrid threats incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder”*. In time, HT have emerged across the world even beyond the context of purely military operations, see e.g. (Fiott and Parkes, 2019) for the case of Crimea in 2014. According to the Joint Communication to the European Parliament and the Council Joint Framework on countering hybrid threats – a European Union response (European Commission, 2016), HT are qualified as a *“mixture of coercive and subversive activities, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare”*.

Even though HT have been around for a while, the concept still needs to be clarified and elaborated so that it can be operationalised in a harmonised manner across the EU countries, also towards its integration in the broader risk management landscape. As suggested by recent studies, their unconventional nature sets HT apart with respect to well-known and defined threats and hazards (such as natural hazards). Correspondingly, a change in mindset is needed to counter them effectively and efficiently. The objective of this chapter is to provide a better understanding of this subject and additionally to offer guidance for risk management initiatives related to such kind of threats. Clearly Hybrid Threats have not been included yet in the framework of National Risk Assessments and this can be attributed to their novelty and their complexity.

Recently, the JRC in collaboration with the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) developed a conceptual framework, which addresses the mentioned needs and helps towards the identification and development of resilience tools for HT<sup>291</sup>. According to the proposed model, HT exhibit a series of characteristics that render them difficult to identify, detect, attribute and consequently address. In principle, they employ several tools across several domains in a perhaps synchronised manner. A hybrid threat is always a combination of several attack vectors while, conversely, not all attack combinations configure as a hybrid activity. While practically hybrid activities very often include a cyber dimension, the latter statement makes an important point against the misconception that cyber activities are per se hybrid activities.

A signature characteristic of HT is their “stealth mode”, namely the way they deliberately play with reaction thresholds so as to remain somehow unnoticed. Obviously, this hinders attribution and consequently the application of measures against adversaries. Furthermore, from a risk management perspective, it can be rather difficult to take the right actions early enough to prevent the outbreak of a full-blown crisis.

Hybrid activities exploit vulnerabilities well beyond the domain being directly targeted and aim, for example, to take advantage of the gaps between national and international legislation. The legal aspects related to hybrid activities are particularly important for responding to such activities. The main question here is how a state or an international organisation can apply sanctions to adversaries if no adequate legal instruments exist to govern the type of actions to be taken. Furthermore, in principle hybrid activities aim at achieving strategic and overarching objectives such as undermining core values of western democratic societies, trust in institutions and decision making capability of countries.

An additional parameter is related to the opportunistic nature of HT. For example, large scale disasters (such as the COVID-19 pandemic) stress the capabilities of countries and render them more susceptible to hybrid activities. There are pieces of evidence of adversaries who have employed tools such as disinformation and cyber-attacks to push their narratives in our societies, discredit leadership and promote a positive image of specific political systems and their capacity to handle this unprecedented crisis.

Ambiguity is also a key aspect of an aggressor’s hybrid strategy. As illustrated in this document, ambiguity touches several faces of a hybrid threat, as it can mask the true objectives of the aggressor and render decision-making or response a rather cumbersome process. Especially when it comes to a collective response in the framework of existing structures (e.g. NATO), ambiguity can defy the development of a common

---

<sup>291</sup> <https://ec.europa.eu/jrc/en/news/jrc-framework-against-hybrid-threats>

understanding and approach to problem resolution, even bringing decision-making to a halt. Similarly at EU level, the activation of articles such as TFEU 42.7 and TFEU 192 is equally challenging.

One can think of HT as an expression of the complexity around us, as well as a product of the evolution of technologies and means available to adversaries to conduct their actions. Nowadays, for instance, critical infrastructure sectors, essential services and supply chains are more interconnected and subject to digitisation. This new reality, in fact, has introduced key systemic risks (Goldin and Mariathasan, 2014), and adversaries will aim to exploit the new vulnerabilities. Such aspects have to be seen also through the prism of societal vulnerabilities due to local or global circumstances such as economic crises, political instability and population discontent.

Taking into account the aspects mentioned above, addressing HT requires out-of-the-box thinking and innovative risk management paradigms. Given the complexity of hybrid activities and the creativity of adversaries, it seems rather difficult to elaborate an exhaustive set of plausible scenarios, appropriate measures and risk barriers. Also, a probabilistic treatment of this subject may be unfeasible or insufficient. Perhaps, some core developments in this area can be better described as exercises meant to identify and manage intrinsic vulnerabilities and systemic risks which, sooner or later, would be exploited by adversaries. Given the openness and power of open source intelligence tools, often it is practically difficult to avoid disclosure of exploitable systemic vulnerabilities. It is thus to the interest of authorities to set-up processes to identify vulnerabilities and mitigate them in a timely manner. However, in several cases this is a long process (i.e. systemic vulnerabilities at societal level) and requires significant investment.

Taking into account what illustrated so far, the discussion that follows in this chapter is mainly vulnerability- and resilience-based, rather than articulated according to a general risk management approach. In a sense, the proposed approach follows the example of 0-day vulnerability patching found in cyber risk management and elaborates over the concept of continuous vulnerability assessment. Threat probability estimation is not considered, and it is assumed that actors implementing hybrid initiatives will take advantage of any existing vulnerabilities as these become evident to them. Moreover, beside the identification of vulnerabilities, what seems to be equally important in our context is the identification of potential adversaries, their motives and geopolitical interests.

### **23.2 The political landscape and the respective conceptual model**

The objectives of a hybrid campaign can be quite comprehensive and ambitious: for instance, disrupting societal functions, undermining governments in their decision-making capabilities, eroding societal cohesion and functions, or fostering mistrust in leadership. According to the EU Member States (MS), a clear understanding of the underlying objectives or motives of the attacker is essential for identifying those weak signals that indicate the deployment of a hybrid campaign. The above-mentioned Joint Framework on countering hybrid threats published in April 2016 proposed a whole-of-government approach with 22 areas for action in order to counter HT and foster the resilience of the EU and the MS, as well as that of international partners.

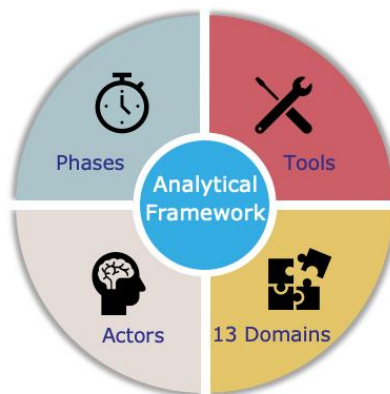
Most actions defined in the Joint Framework are focused on improving situational awareness and building resilience, with a better ability to respond. The document can be interpreted as mainly a vulnerability-based framework. For example, both action 1 and action 5 aim at the identification of vulnerabilities. In addition, emphasis is given to improving the level of resilience of MS. This element fits perfectly to the concept of HT illustrated above in this chapter, given the broad spectrum and complexity of attack vectors that can be part of a hybrid activity as well as the challenges related to forecasting and uncertainties.

This inherent complexity sets apart HT from conventional attacks including cyber-attacks. HT constitute of complex attack vectors taking place simultaneously or sequentially, e.g. information attacks, attacks on critical infrastructures and dissemination of fake news, etc., remaining both below detection thresholds and appearing as uncorrelated. They affect several domains of a state's activities. While there is a strong correlation between attack vectors, this correlation is not always obvious, at least during the priming phase of such an activity.

The Joint Framework set the cornerstone for future work in the domain of HT. However, a more detailed characterisation of the problem still appeared necessary to drive the efforts of practitioners towards three main areas: improving understanding, raising awareness and planning the necessary actions to counter hybrid activities. To address these needs and gaps, The JRC and Hybrid CoE have jointly developed a conceptual

model (Giannopoulos et al)<sup>292</sup>. The model provides clarity and a detailed characterisation of HT. It is based on 4 pillars (namely actors, tools, domains and timeline), applied and validated against three case studies (and partially also to the COVID-19 crisis). In particular, two main categories of actors are identified, namely state and non-state actors. In order to pursue their objectives, actors may use several hybrid tools in order to target one or more domains. Specifically, the conceptual model identifies several tools and 13 domains of statecraft which can be affected by hybrid activities. A timeline describing the evolution of hybrid activities completes the representation.

**Figure 67:** Conceptual model pillars



Source: JRC and Hybrid CoE

The conceptual model fosters comprehensive thinking, according to which responding to the inherent complexity of HT and the combination of hybrid tools requires the involvement of stakeholders from various domains, such as cyber, strategic communication and counter-intelligence to name a few. This adds a layer of complexity at the tactical, operational and strategic levels. As often claimed in the literature, a whole-of-government approach or even a whole-of-society approach is needed in order to detect, prevent and respond to HT. The conceptual model also implicitly fosters vulnerability-based thinking by focusing on the mentioned 13 domains and on how these can be impacted by hybrid tools.

Activities aimed at building resilience against HT are underway in many areas. The June 2018 Joint Communication (European Commission, 2018) links CBRNE attacks to HT, following the Salisbury attack in the UK. It reinforces the need to fully implement the October 2017 CBRNE Action Plan (European Commission, 2017a), which proposed 23 practical actions and measures aimed at better protection of citizens and infrastructures against these threats, including through closer cooperation between the EU and its Member States, as well as with the NATO. Another example is the work within the Commission (DG ECHO) on national risk assessments (NRA) and risk management capability assessments (RMCA). The implementation of Directive (EU) 2016/1148 and the Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (European Commission, 2017b) describes the work performed on the cybersecurity front.

### 23.3 Examples of hybrid activity

Awareness of HT increased rapidly with the events in Ukraine in 2014. These have been considered as one of the most refined hybrid campaigns so far, involving coordinated actions affecting several domains of the Ukrainian government and leveraging existing vulnerabilities in the country.

One of the main characteristics of the Ukrainian crisis was the fact that no warfare was officially declared, which is a key element of hybrid activities. All actions took place at such a level of intensity that, despite the fact that the adversary was known, attribution was rather difficult (from the perspective of international law), thus compromising the efforts of the international community to react in a credible manner.

During the Ukrainian crisis, the adversary compromised the country's administration by seizing government buildings, thus reducing the capability of the state to respond to the aggression. Furthermore, cyber-attacks to telephony and internet not only in Crimea but also in other areas of Ukraine and in particular in Kiev

<sup>292</sup> G. Giannopoulos, H. Smith, M. Theocharidou, The Landscape of Hybrid Threats: A conceptual model, JRC 117280

compromised the capability of the political leadership to take the right actions in a timely manner. Crimea's unique internet exchange point was heavily compromised. This was a clear example of a lack of resilience. It also clearly showed how, in the framework of a hybrid activity, affecting the operation of critical infrastructures can be not the end but a means to an end.

In addition, disinformation campaigns took place before and also during the main phase of the hybrid activity. These campaigns aimed at changing the perspective of the population and preparing the ground for the results of the Crimean referendum. Finally, support to specific ethnic groups has been considered a key element for the success of the hybrid activity, which stresses the importance of thoroughly considering societal vulnerabilities in the framework of HT.

In the considered circumstances, the adversary leveraged several vulnerabilities in various domains (administration, defence, infrastructure, etc.) in a very innovative way. From the government perspective, it would have been very difficult to forecast the combination of actions surfacing in time, as well as their specific objectives. The examples mentioned so far, if thoroughly analyzed, can support arguments in favour of a vulnerability-based approach to risk management. Among the plausible options in this sense, what governments can do is to monitor continuously the level of vulnerabilities in the country across sensitive domains. A high level of awareness of one's own vulnerabilities is a very credible way for active deterrence.

**23.4 Assessing vulnerabilities: what to look for?**

Given the complex nature of HT, it is necessary to assess vulnerabilities in a comprehensive manner. Despite the fact that HT touch upon national security and defence, it is required to gain a deep understanding of a wide range of vulnerabilities scattered across domains of statecraft which are not directly related to security and/or defence (as described in the JRC/Hybrid CoE conceptual model). As support to the aforementioned claim, we can mention the fact that several European countries are referring to the expression "comprehensive security" or manifesting the need for a whole of governance/whole of society approach to counter HT.

Domains represent the most relevant pillar for analysing vulnerabilities, according to the introduced conceptual model. While each country can apply a different approach, the division of a country's structure into 13 domains can guide MS to focus their efforts on identifying and mitigating vulnerabilities. In **Figure 68** these domains are depicted. Beyond that, one should also consider vulnerabilities at the interfaces between the various domains. These, in turn, might be exploited by adversaries for unleashing a hybrid activity.

**Figure 68.** Domains of a country's structure that might be affected by a hybrid activity



Source: JRC and Hybrid CoE

In the next sections, a methodology for vulnerabilities assessment is presented based on ISO 33020.

### **23.5 Changing paradigm of risk management: vulnerabilities self-assessment methodology**

Given the fact that internal security is an exclusive competence of MS the Analysis and assessment of vulnerabilities have to take place at the MS level following a self-assessment process. Activities should be designed taking into account the following high-level requirements.

- The methodology needs to be suitable for self-assessment and flexible enough to be adjusted to all MS needs and context characteristics.
- The methodology requires a common understanding of HT in order to develop vulnerability indicators fit for purpose and similar across MS. The latter is significant not for the sake of comparing the performance of countries, but mainly for exchanging best practices.
- The methodology should not focus on the quantitative results of individual assessment, as these may be of confidential nature, but instead to facilitate the exchange of best practices among the MS.

To address these requirements, a process-based assessment loosely based on the ISO/IEC standard 33020<sup>293</sup> is hereby proposed. For each vulnerability identified by MS, a relevant process maturity level needs to be evaluated and assessed. The main underlying assumption is that the more mature a process to measure a vulnerability is, the higher the probability that actions will be taken to mitigate this vulnerability. In principle, a structured approach to implementing controls or measures to tackle a specific vulnerability will provide tangible results in the long run and reduce the potential impact even if this vulnerability is exploited. Instead, the absence of a structured process or any controls or measures may lead to a higher level of vulnerability or leave a MS exposed to hybrid attack in the long run.

When it comes to vulnerability indicators and vulnerability self-assessment, another important aspect is the dilemma between the use of single and composite vulnerability indicators. It is recommended to avoid a single aggregated measure of vulnerability, as this may mask vulnerabilities in the various domains.

The self-assessment process can be generalized according to the following steps:

#### **Step 1 – Scoping and planning the assessment**

This step includes all the preparatory steps required to initiate the assessment. It includes the identification of scope, stakeholders (assessment team), and most importantly the decision on which areas/processes to assess. Processes are related to vulnerabilities, so this step implies that the MS need to select which vulnerabilities are applicable and should be assessed.

#### **Step 2 – Assessing vulnerability levels**

At this stage, the respective processes for assessing the level of vulnerability are being evaluated, based on a pre-selected scale. Regardless of the selected quantification method, this step investigates whether or not the implemented process achieves its purpose and outcomes. This process is qualitative and requires an expert judgement on specific criteria to be met.

#### **Step 3 – Evaluating assessment results**

The step allows the entity performing the assessment to compare different vulnerability areas, with respect to various domains. Its goal is to support decisions. Decisions on how to deal with a specific vulnerability in the future should take into account the context and potential consequences resulting from its exploitation. The outcome of this step should be recorded, communicated and validated by the decision makers.

#### **Step 4 – Identifying areas for improvement & creating action plans**

The entity performing the assessment must produce plans in order to make improvements on the vulnerabilities identified, focusing on the processes that are not mature enough or on the areas where a greater benefit can be achieved. This process will also facilitate the prioritisation of resources in terms of investments to reduce vulnerabilities. Moreover, decision makers and other stakeholders should be aware of

---

<sup>293</sup> ISO/IEC 33020:2015(en), Information technology — Process assessment — Process measurement framework for assessment of process capability.

the remaining vulnerabilities and, thus, these should be documented and submitted for future review and monitoring.

For the assessment of vulnerability indicators, six levels of capability that a process can achieve are identified (**Table 26**), including an ‘incomplete process’ designation if the practices in it do not achieve the intended purpose of the process.

**Table 26.** Quantification of vulnerability based on process capability

Process Capability	Description
<b>0 Incomplete process</b>	Controls are not implemented or fail to achieve their purpose. At this level, there is little or no evidence of any systematic process to deal with this vulnerability.
<b>1 Performed process</b>	There are implemented controls which achieve their purpose.
<b>2 Managed process</b>	The previously described performed controls are now implemented in a managed fashion (planned, monitored and adjusted process) and the work products of this process are appropriately established, controlled and maintained.
<b>3 Established process</b>	The previously described managed controls are now implemented using a defined process that is capable of achieving their outcomes.
<b>4 Predictable process</b>	The previously described established controls now operate within defined limits to achieve their outcomes.
<b>5 Optimising process</b>	The previously described predictable process is continuously improved to meet relevant current and projected business goals.

Source: JRC elaboration based on ISO/IEC 33020:2015

Defining target capability levels is up to each country to decide. This approach reflects a motivation to achieve at least capability level 1 for the identified indicators and the related processes, which can be an important landmark for a MS. This could also imply a simpler quantification method, such as following only a checklist approach, using only a two level scale indicating the presence of controls or not (**Table 27**).

**Table 27.** Assessment of vulnerability based on a checklist

Process Capability	Description
<b>0 Incomplete process</b>	Controls are not implemented or fail to achieve their purpose. At this level, there is little or no evidence of any systematic process to deal with this vulnerability.
<b>1 Performed process</b>	There are implemented controls which achieve their purpose. <sup>[1]</sup> <sub>SEP</sub>

Source: JRC elaboration based on ISO/IEC 33020:2015

Alternatively, more traditional vulnerability scales can be used, such as the one adapted by the NIST framework and proposed on **Table 28** below (NIST, 2012).

**Table 28.** Quantification of vulnerability based on NIST Special Publication 800-30, Rev 1 (2012)

Qualitative Values	Semi-Quantitative Values		Description
<b>Very High</b>	96-100	10	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant controls are not implemented and not planned; or no control can be identified to remediate the vulnerability.
<b>High</b>	80-95	8	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.
<b>Moderate</b>	21-79	5	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant control or other remediation is partially implemented and somewhat effective.
<b>Low</b>	5-20	2	The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant control or other remediation is fully implemented and somewhat effective.
<b>Very Low</b>	0-4	0	The vulnerability is not of concern. Relevant control or other remediation is fully implemented, assessed, and effective.

Source: NIST Special Publication 800-30, Rev 1 (2012)

The rationale for proposing such a flexible methodology is based on the assumption that the aim of this work is not to compare the assessment results of all MS, but rather to assist MS in performing their own self-assessment and sharing their best practices. We believe that sharing what processes or controls have been implemented could facilitate a discussion among the MS, in order to improve collectively the security posture of EU countries against HT.

### 23.6 Beyond vulnerabilities assessment: fostering resilience

HT borrow elements from the military domain, with some older practices empowered using modern technologies and capabilities as enablers. Given the fact that hybrid activities are taking place below the radar and threshold of attribution and detection, victims –while aware of the existence of HT – might not be aware of methods, modus operandi or objectives. This further stresses the need for identifying and mitigating one’s own vulnerabilities.

Vulnerabilities can be both intrinsic and extrinsic, and they can also change in time. For example, harsh environmental conditions can bring energy networks close to their limits and reduce the level of resilience of infrastructures. What is more, society is also less tolerant of energy supply issues in circumstances such as cold weather or heat waves. This reflects the fact that at a certain moment in time the external conditions (in this example mainly environmental) may alter the level of vulnerability. Such temporary conditions have to be thoroughly considered. Consequently, maintaining a vulnerability identification process up-to-date is a continuous and dynamic process.

Once vulnerabilities are identified, the next step is to embark on an effort to foster resilience. When it comes to resilience against HT, there are many ways that this can be applied and many phases given the



multifaceted nature of the concept. In fact, this resilience-based approach complements the transition from traditional risk management to a vulnerability and resilience management approach (Rod et al, 2020). Resilience measures can be applied for absorbing the shock, reducing the time span over which the disruption is taking place, and bouncing back to normal operations as soon as possible. In any case, the main argument for fostering resilience in order to address HT is based on the assumption that the attack vector can be complex and difficult to predict in advance and that adversaries will take advantage of existing vulnerabilities in targeted countries in order to tailor their efforts accordingly. As a consequence, MS can do an important part of the work by identifying and mitigating vulnerabilities. However, for all these aspects of HT that cannot be known a priori (i.e. combination of tools and impact on domains) MS need to go the extra mile and develop resilience measures in each of the domains identified before (and if possible between the interfaces of these domains).

### **23.7 Future Challenges in the domain of hybrid threats**

HT represent a relatively new domain for MS and their national security. Given the strategic nature of the threat and the fact that both man-made and natural hazards may be part of a hybrid activity, MS need to be in a position to identify their vulnerabilities across a number of domains and mitigate them as part of their plans to improve their resilience. HT also suggest the importance of specific paradigms in the domain of risk management, with a focus on the identification and analysis of vulnerabilities rather than the estimation of an incident's likelihood and impact. In fact, adversaries will exploit vulnerabilities and, as a consequence, the probability of a hybrid activity becomes a function of vulnerability levels.

Another important aspect of HT is their detection. The earlier the detection takes place, the better it is in terms of responding to such threats. However, detecting HT requires strong analytical tools and correlating different streams of information from intelligence, open sources as well as sectoral reports (reports from the administrations in the various domains shown in Figure 1). The main challenge here is the fact that large amounts of seemingly uncorrelated information need to be assessed in order to improve the situational awareness of countries.

In this respect, solutions for efficiently exploring the bulk of disparate information will be needed. Visual analytics, AI and similar techniques for analysing large amounts of data can be the right solution; however, the experienced analyst will always be a central piece in this effort. The main advantage of such technologies is that they are utilised for supporting the most effective exploitation of human experience and background knowledge.

Being more specific, in the case of the HT, the users (e.g. MS officials) will be provided with multiple views (i.e. graphical representations) of the available information, i.e. all the related events that may occur in the various Hybrid Threat components with an appropriate representation of their attributes with respect also to the components' evolving conditions. As a result, this scheme will allow for incorporating the combinational thinking of the expert analysts and their general personal and professional experience and knowledge (MS officials) into the detection process. Furthermore, given that the visual analytics provide an overall view of the phenomena in hand and their dynamic evolution in time and space, the expected result is not limited to the mere detection of the Hybrid Threat, but the investigation of its root causes and the exposure of the attackers' modus operandi is also accommodated.

### **23.8 References**

European Commission, 2016, Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats, a European Union response, JOIN(2016) 18 final.

European Commission, 2017a, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks, COM(2017) 610 final.

European Commission, 2017b, Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final.

European Commission, 2018, Joint Communication to the European Parliament, the European Council and the Council, Increasing resilience and bolstering capabilities to address hybrid threats, JOIN(2018) 16 final.

Fiott, D., & Parkes, R., 2019, Protecting Europe: The EU's Response to Hybrid Threats, Publications Office of the European Union.

Goldin, I., Mariathan, M., 2014, *The Butterfly Defect: How Globalization creates systemic risks and what to do about it*, Princeton University Press, ISBN 978-0-691-16842-5

Hoffman, F.G., *Conflict in the 21st Century: The rise of the Hybrid Wars*, Potomac Institute for Policy Studies, 2007

NIST, 2012, *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30, Revision 1

Rod, B., Lange, D., Theocharidou, M., Pursiainen, C., 2020, *From Risk Management to Resilience Management*, *Journal of Management in Engineering*, vol. 36, no.4.

**List of boxes**

Box 1: Reporting on disaster risk management under Article 6 of the Decision No 1313/2013 on the Union Civil Protection Mechanism, as amended by Decision No 2019/420/EU .....25

Box 2: What is Risk Management Capability in the framework of the UCPM (Decision No 1313/2013/EU) ....37

Box 3: EU Strategy on adaptation to climate change (COM/2013/0216) .....52

Box 4: Article 19(1) of Governance of Energy Union and Climate Action (Regulation (EU) 2018/1999) .....53

Box 5: The priorities of The New EU Strategy on Adaptation to Climate Change: .....54

Box 6: Article 4 of the Commission’s proposal for the first European Climate Law (COM/2020/80).....54

Box 7: Adaptation to climate change impacts vs. mitigation of climate change (IPCC, 2014a) .....56

Box 8: Shared socio-economic pathways .....57

Box 9: European fire risk: simple, consistent maps to support policy..... 102

Box 10: Campi Flegrei (Italy)..... 141

Box 11: The NERIS platform ..... 186

Box 12: The ASAMPSA\_E project ..... 187

Box 13: SOURCE TERM ..... 187

Box 14: An example application of the JRodos Emergency model chain..... 191

**List of figures**

**Figure 1:** Risk assessment provides an opportunity to better understanding of the underlying disaster risk drivers and informs disaster risk management measures (H: Hazard, E: Exposure, V: Vulnerability, R: Risk). ..27

**Figure 2:** Stages of Risk Assessment process according to ISO 31010 .....29

**Figure 3:** DRM cycle as suggested in RMCA guidelines (Commission notice, 2015) vs. classical 6 stage evidence based policy cycle. ....38

**Figure 4:** Policy cycle for the implementation of integrated disaster risk management .....40

**Figure 5:** The interaction between the policy cycle covered by RMCA and the integrated DRM .....49

**Figure 6:** The common risk concept involved in disaster risk management and climate change adaptation, and the interaction of these with sustainable development. ....55

**Figure 7:** Risk of climate-related impacts results from changes in any of the dimensions of the risk concept due to the climate change: hazard, exposure or vulnerability of human and natural systems.....56

**Figure 8:** The most common risks in national risk assessments (NRAs) in 2015 and 2018 reporting cycles .58

**Figure 9:** The global risk landscape 2020 with the risk addressed in this V1 of Recommendation for NRA ..59

**Figure 10:** Harmonization of risk assessment process .....63

**Figure 11.** 1-in-100-year flood hazard map for the Ebro River, Spain, near the city of Zaragoza,, published by Ministerio para la Transición Ecológica y el Reto Demográfico. ....74

**Figure 12.** Comparison of expected annual damages in 2100 for all EU contries and United Kingdom, assuming no adaptation to future river flood risk conditions, and with the implementation of three different adaptation strategies. Results are calculated assuming a 2°C warming scenario. ....78

**Figure 13.** Drought hazard, exposure, vulnerability and risk for the agricultural sector in Europe according to the conceptual approach .....84

**Figure 14.** Current and projected annual losses (in € billion, 2015 values) under different global warming levels relative to pre-industrial conditions (1.5°C; 2.0°C and 3.0°C) for EU-28 countries by region, for all economic sectors considered and assuming that current socio-economic conditions continue into the future. The top of each bar shows the average estimate and the vertical lines indicate climate uncertainty. ....86

**Figure 15.** A summary workflow highlighting the key components of the wildfire risk. ....94

**Figure 16.** (a) Annual fire frequency (number of fires per province (NUTS3)/years) and (b) average burned area (total burned area per province (NUTS3)/years) mapped in EFFIS, classified in four categories for the period 2008 - 2018.....95

**Figure 17.** Examples depicted from EFFIS for the (a) Canadian Forest Fire Weather Index (FWI), (b) Fine Fuel Moisture Content (conditions on October 21 2019). ....96

**Figure 18.** Examples depicted from EFFIS for (a) Duff Moisture Code, and (d) Drought Code (conditions on October 21 2019). ....96

**Figure 19.** Example of the Initial Spread Index in EFFIS (conditions on October 21 2019).....96

**Figure 20.** Frequency of days with high fire danger (Fire Weather Index greater than 30). ....97

**Figure 21.** Fuel map of Europe.....98

**Figure 22.** Topography of the pan-European region derived from the European Atlas of Forest Tree Species .....99

**Figure 23.** Percentage of land area which lies in the WUI. .... 100

**Figure 24.** Natura 2000 network sites. .... 101

**Figure 25.** Socio-economic value (reconstruction cost of different land cover types. .... 102

**Figure 26.** The Global Risks Landscape 2020 perceived by business leaders (A) and by scientists (B). .... 107

<b>Figure 27.</b> Assessment of past (~1950–2000) and current (~2001–2017) trends in biodiversity status of marine, inland surface water and terrestrial ecosystems for the four sub-regions and the whole of Europe and Central Asia. ....	110
<b>Figure 28.</b> Trends in nature’s contributions to people (1960–2016) for Europe and Central Asia and the sub-regions. ....	111
<b>Figure 29.</b> Regions of the world exposed to high intensities of multiple drivers. The main map shows the number of the 16 driver variables for which each grid cell was in the highest 10% of values within each realm. Regions in the darkest orange are exposed to high intensities of multiple variables, whereas those in off-white are exposed to lower intensities (i.e. within the 90% quantile of values) of all variables. The smaller plots below show the same for each of the separate drivers. ....	112
<b>Figure 30.</b> Projections of the impacts of land use and climate change on biodiversity (measured as change in species richness across a wide range of terrestrial plant and animal species at regional scales) and nature’s material (food, feed, timber and bioenergy) and regulating (nitrogen retention, soil protection, crop pollination, crop pest control and ecosystem carbon storage and sequestration) contributions to people between 2015 and 2050. ....	114
<b>Figure 31:</b> Left: peak ground acceleration from the SHARE project for 475 years return period. Right: reference peak ground acceleration from the National Annexes to Eurocode 8. All countries adopted a reference return period of seismic action for the no-collapse requirement of 475 years, except Romania that adopted 100 years and UK that adopted 2500 years ....	122
<b>Figure 32.</b> Seismic vulnerability of buildings in Europe. ....	123
<b>Figure 33.</b> Low-probability and high-impact risk region in a F-N chart ....	129
<b>Figure 34.</b> Framework proposed by ENSURE project to describe the interaction between hazard, vulnerability and resilience ....	137
<b>Figure 35.</b> Generalized sketch for the compilation of a volcanic risk assessment for individual volcanic hazards. Multi-hazard risk assessments should result from the combination of individual analysis associated with each individual hazard. Similarly, individual dimensions of vulnerability need to be treated separately and for each exposed element (e.g. population, buildings, and infrastructures). ....	139
<b>Figure 36.</b> Single algorithm combining probability and impact resulting in single overall risk level (combined approach – option 1). ....	153
<b>Figure 37.</b> Algorithm for calculating probability and impact (option 2). ....	153
<b>Figure 38.</b> Categorization of zoonotic potential ....	157
<b>Figure 39.</b> Framework to be followed in decision-making of all activities carried out in the facility. ....	159
<b>Figure 40.</b> The maximum potential levels of socio-economic impacts as ranked for different types of consequences. ....	168
<b>Figure 41.</b> Distribution of the ~10,000 Seveso Directive sites (high hazard fixed facilities) in the European Union as reported by countries in 2014. In addition, numerous other industries that are not part of these hazardous chemicals industries also can be sources of chemical accident risk. ....	172
<b>Figure 42.</b> Box tie illustration of chemical accident sequence of events. ....	173
<b>Figure 43.</b> Scenarios for anhydrous ammonia atmospheric pressure refrigerated storage tank. ....	174
<b>Figure 44.</b> Layers of Protection Model for a Chemical Plant ....	176
<b>Figure 45.</b> Toxic dispersion from a catastrophic rupture of a tank wagon containing sulphur dioxide .....	179
<b>Figure 46.</b> Example of an individual risk curve. ....	182
<b>Figure 47.</b> Example of an F/N diagramme ....	182
<b>Figure 48.</b> Example of risk matrix. ....	183
<b>Figure 49.</b> Risk matrix to combine the Caesium Bioavailability Index and the Transfer Factor Index to obtain the Radiological Vulnerability Index. ....	190

<b>Figure 50.</b> Priorisation map of the Iberian Peninsula for cereals and <sup>137</sup> Cs deposit .....	191
<b>Figure 51.</b> Fatalities per month from global terrorism database 1970-2017 (year 1994 is missing in the recordings) and Control Risks (2018-2019).....	199
<b>Figure 52.</b> Risk assessment process. ....	200
<b>Figure 53.</b> Threat level from terrorist attacks in central Africa and Middle East in 12/2019-03/2020 by JRC terrorism database using EMM. ....	201
<b>Figure 54.</b> Worldwide terrorist attacks by a) utilized modus operandi and b) target. ....	201
<b>Figure 55.</b> Indicator point system for assessing criticality of exposed assets. ....	205
<b>Figure 56:</b> EU policy milestones towards the resilience of CIS. ....	212
<b>Figure 57:</b> Risk Assessment for CI Loss. ....	217
<b>Figure 58:</b> NIPP's Critical Infrastructure Risk Management Framework .....	217
<b>Figure 59:</b> Critical Infrastructures & Systems Risk and Resilience Assessment Methodology. ....	219
<b>Figure 60:</b> ICI-REF: integration of resilience management in risk management.....	221
<b>Figure 61:</b> Tiered approach to analysis of CIS in GRRASP .....	224
<b>Figure 62:</b> Onion-skin diagram of Anytown relating to Electricity Failure. ....	225
<b>Figure 63:</b> Circle diagram of dependencies. ....	226
<b>Figure 64:</b> NIST Community Resilience Guide: performance goals summary table. ....	227
<b>Figure 65.</b> Information security risk management process .....	232
<b>Figure 66.</b> Rumentary risk management concepts and relationships .....	244
<b>Figure 67:</b> Conceptual model pillars .....	262
<b>Figure 68.</b> Domains of a country's structure that might be affected by a hybrid activity .....	263

## List of tables

<b>Table 1:</b> History of reporting process for national risk assessment and risk management capability assessment .....	23
<b>Table 2:</b> Questions in Reporting Guidelines on Disaster Risk Management (Commission Notice, 2019) addressing risk assessments, risk management capability assessment and priority prevention and preparedness measures. ....	25
<b>Table 3:</b> Dimensions of capability applicable to different capacities in different phases of DRM policy cycle	43
<b>Table 4:</b> Possible rubrics for Loss data collection and reporting capability .....	46
<b>Table 5:</b> Conceptual framework for capability needs of the risk assessment phase .....	50
<b>Table 6:</b> List of steps identified by the Floods Directive and the milestones for implementation and review. WFD: Water Framework Directive.....	70
<b>Table 7:</b> Short term actions to be implemented during and after a drought emergency .....	87
<b>Table 8:</b> Long-term actions to be implemented before, during and after a drought emergency .....	88
<b>Table 9:</b> Overview of actions accompanied by a quantification method allowing them to be comparable between Member States.....	89
<b>Table 10:</b> Earthquakes in Europe since 2002, for which the EU Solidarity Fund intervened .....	121
<b>Table 11:</b> European research projects related to seismic risk assessment.....	126
<b>Table 12:</b> Example of pipe failure frequencies .....	177
<b>Table 13:</b> Effects related to different kind of scenarios .....	178
<b>Table 14:</b> Consequence classification for human and environmental impacts .....	179
<b>Table 15:</b> Endpoints values of fires and explosions for different severity levels .....	180
<b>Table 16:</b> Stationary, non-stationary and fixed effects.....	180
<b>Table 17:</b> Example of a risk matrix with quantified likelihood .....	183
<b>Table 18:</b> Contamination levels modified from NGR, 2014, referred to the activity concentration deposited on the ground for gamma and beta emitters. Contribution of the <sup>137</sup> Cs to the total activity concentration and Deposition weighting factor corresponding to each level. ....	189
<b>Table 19:</b> Caesium Bioavailability Index (I <sub>Cs</sub> ) definition, considering clay and K soil content. ....	190
<b>Table 20:</b> Transfer Factor Index associated to each transfer factor value, corresponding to the soil texture, for the grain of cereals in temperate climates. ....	190
<b>Table 21:</b> Soft target categories. ....	202
<b>Table 22:</b> Scoring criteria per indicator .....	205
<b>Table 23:</b> Assessment of an asset's criticality.....	206
<b>Table 24:</b> Overview of attack modeling techniques existing in the literature with a focus on strengths and weaknesses. For a detailed discussion on these techniques the interested reader may refer to (Nespoli et al., 2018). ....	238
<b>Table 25:</b> Standardisation attempts for security automation. For a detailed discussion on these efforts the interested reader may refer to (Nespoli et al., 2018). ....	238
<b>Table 26:</b> Quantification of vulnerability based on process capability .....	265
<b>Table 27:</b> Assessment of vulnerability based on a checklist .....	265
<b>Table 28:</b> Quantification of vulnerability based on NIST Special Publication 800-30, Rev 1 (2012).....	266

## **GETTING IN TOUCH WITH THE EU**

### **In person**

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)

### **On the phone or by email**

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696, or
- by electronic mail via: [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)

## **FINDING INFORMATION ABOUT THE EU**

### **Online**

Information about the European Union in all the official languages of the EU is available on the Europa website at: [https://europa.eu/european-union/index\\_en](https://europa.eu/european-union/index_en)

### **EU publications**

You can download or order free and priced EU publications from EU Bookshop at: <https://publications.europa.eu/en/publications>. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)).



## The European Commission's science and knowledge service

Joint Research Centre

### JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.



**EU Science Hub**

[ec.europa.eu/jrc](https://ec.europa.eu/jrc)



@EU\_ScienceHub



EU Science Hub - Joint Research Centre



Joint Research Centre



EU Science Hub



Publications Office  
of the European Union

doi:10.2760/80545

ISBN 978-92-76-30256-8