European Commission

JRC SCIENCE AND POLICY REPORT

Risk assessment methodologies for critical infrastructure protection. Part II: A new approach

Marianthi Theocharidou
Georgios Giannopoulos

2015

Report EUR 27332 EN

Joint Research Centre

European Commission
Joint Research Centre
Institute for Protection and Security of the Citizen

Contact information
Georgios Giannopoulos
Address: Joint Research Centre, Via Enrico Fermi 2749, 21027, Ispra, Italy
E-mail: Georgios.Giannopoulos@jrc.ec.europa.eu
Tel.: +39 0332 78 6211

JRC Science Hub
https://ec.europa.eu/jrc

JRC 96623

EUR 27332 EN

ISBN 978-92-79-49246-4

ISSN 1831-9424

doi:10.2788/621843

Luxembourg: Publications Office of the European Union, 2015

Abstract

This report describes a risk assessment process for Critical Infrastructures (CI) based on the staff working document from DG ECHO namely "Risk Assessment and Mapping Guidelines for Disaster Management" and DG HOME "on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure". As a result of the DG ECHO staff working document, several Member States (MS) have provided overview of risks where the risk of "loss of critical infrastructure" has been identified as a man made risk.

However, we consider that there is a lot of room for improvement in this process mainly because Critical Infrastructures are not yet one more risk at MS level but CIs in their turn are subject to the risks that have been identified my MS. In the present report we identify this gap and we provide a methodology that is based on a different approach with respect to the CI risks.

Contents

List of Figures

List of Tables

Nomenclature

CBRN	Chemical Biological Radiological & Nuclear
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CIPRnet	Critical Infrastructure Preparedness and Resilience Research Network
CIPS	Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks
EC	European Commission
ECI	European Critical Infrastructures
EISAC	European Infrastructures Simulation and Analysis Centre
EPCIP	European Programme for Critical Infrastructure Protection
EU	European Union
GIS	Geographical Information Systems
GRRASP	Geospatial Risk and Resilience Assessment Platform
ICT	Information and Communication Technologies
ISO	International Standardisation Organisation
MS	Member States
NRA	National Risk Assessments
RA	Risk Assessment
RVA	Risk and Vulnerability Analysis
UNISDR	United Nations Office for Disaster Risk Reduction

Summary

This report describes a risk assessment methodology for Critical Infrastructures (CI) based on two staff working documents, one from DG ECHO on “Risk Assessment and Mapping Guidelines for Disaster Management” [1] and one from DG HOME on “A new approach to the European Programme for Critical Infrastructure Protection. Making European Critical Infrastructures more secure”. As a result of the DG ECHO staff working document, several Member States (MS) have provided an overview of risks where the risk of “loss of critical infrastructure” has been identified as a man made risk.

However, we consider that there is a lot of room for improvement in this process mainly because Critical Infrastructures are not yet one more risk at MS level but CIs in their turn are subject to the risks that have been identified by MS. Certainly this is a methodological gap and also based on the results of the report on risk assessment review ([2]), we propose here a methodology that takes stock of these policies and provides key elements that would enable similar and comparable risk assessment process for CIs to be adopted.

The report is structured in five chapters.

The first chapter of the report provides an introduction to the topic presenting the legislative elements that are in place, presents elements on a common language for CIP and also how to bridge the gap between EC policies. The second chapter provides methodological findings in the national risk assessments that have been conducted according to the guidelines provided by DG ECHO in the Staff Working Document.

The third chapter provides a gap analysis on these risk assessments which are then subsequently used in the fourth chapter to set up the RA methodology proposed by this report.

Finally, we conclude this report with some policy recommendations and actions to improve the RA of critical infrastructures that can be applicable at national but also international level.

CHAPTER 1

Introduction

1.1 Background

In 2010, the European Commission issued guidelines on risk assessment to support Member States (MS) in preparing national risk assessments for Disaster Management[1]. Following publication of these guidelines and contributions by MS of their work on risk assessments, the Commission produced in 2014 an overview of natural and man-made risks in the EU [3]. In several of these first, national risk assessment results, the risk of "loss of critical infrastructure" has been identified. The loss of "essential" or "vital services" -which are provided by CIs- is also taken into account in several national risk assessments as an *impact* indicator.

The ECI directive [4] emphasizes the importance of risk assessment for critical infrastructures at a European level. However, in the framework of this Directive no RA methodology was developed and MS are following their own methodologies. With the exception of the *cross-cutting criteria*, i.e. (a) casualties, (b) economic effects and (c) public effects, which serve as a baseline guideline for impact assessment, the MS have not adopted a specific methodology for assessing the risks to their critical infrastructures. This means that the comparison of risk assessment results among MS is not feasible. This is also the case for multi-risk, cross-border assessments based on national results. Moreover, the Directive has a sectoral scope, applicable only to the *Energy* and *Transport* sectors, which does not allow for the assessment of all vital services provided by CIs.

The Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection "Making European Critical Infrastructures more secure" was published in August 2013 [5]. It outlines initiatives of the Commission regarding risk assessment methodologies, mainly under the CIPS Programme. The document identifies the limits of sectoral methodologies when cross-sectoral threats need to be addressed, such as the ones targeted by the DG-ECHO guidelines [1]. A *systems* approach is promoted instead, proposing joint work with four European CIs: *Eurocontrol*, *Galileo*, the *electricity transmission grid* and the *gas transmission network*. The development of tools for risk assessment focuses on these four pilots. Also, hazard risk assessment methodologies for low-probability – high-consequences events are identified as a gap; such methodologies could be applied in future "stress tests" for critical infrastructures, as examined in [6].

The World Economic Forum Report of 2015 [7] recognises the "Critical information infrastructure breakdown" as the no.7 of the top risks worldwide in terms of impact. This is combined with the reported trend of "hyperconnectivity" which is associated with technological risks, among which CI loss is considered. The report highlights the fact that risks cannot be assessed

and treated in isolation. They have causal relationships between them and in several cases, they share underlying trends (or vulnerabilities). This complexity of addressing risks, likelihood and potential consequences raise the question of a multi-risk based approach but also for "*preparedness, on the global, regional, national and local levels.*"

1.2 Bridging the gap of Commission policies at technical level

As presented above, several MS have included *"loss of critical infrastructure"* as a top national risk, which is also supported by other worldwide reports. To our understanding, this is rather ambiguous since many of the risks which were identified constitute hazards to CIs and can cause direct damages to the CI itself, leading to disruption of vital services in an indirect way. In the overview of risks from the MS, loss of CI is identified as a man made risk (non malicious), that has an impact on society, while in principle may occur due to various hazards. It can also be the cascading effect of other CI disruptions due to hazards both natural and man made in nature. This is only marginally touched upon the report. It seems that for *non man-made hazards* the aspect of CI loss is not fully considered with the exception of Natech risks for certain categories of infrastructures (unless it is included in an indirect way on the impact to the society). In this fashion the total impact on society due to a natural hazard seems to be underestimated. In addition to that, *interdependencies* that are pertinent to CI and may trigger secondary effects in case of disruption of service are not methodologically considered.

The aim of the proposed work is to investigate the possibility to merge the technical elements described in these policy and legislative documents towards achieving a *common methodology*. Such effort would allow for a framework for assessing risks to critical infrastructures whose disruption would have an impact on European society. It seems that these documents are complementary in the sense that:

- the ECI directive provides baseline guidelines for energy and transport CIs and how to identify the most critical, European ones. The criteria refer to the impact of the loss of an infrastructure as a way to prioritise them. These guidelines do not correspond to a complete national risk assessment, but cover early stages of risk management, by "establishing the context" (scope definition) and "consequence analysis" (of the risk analysis stage) [8]. In essence, the directive recommends a way for the MS to identify their assets (CIs) that require protection, as a first step towards risk management.

- DG HOME staff working document ([5]) does not provide detailed methodological considerations to perform risk assessment in CIs. It promotes a systems approach as opposed to a sectoral approach and focuses on threats that can cause significant consequences to CIs.

- DG HOME policy focuses on the prevention, preparedness and response side of critical infrastructure protection. However, in order to have a reasonable approach to these elements (mainly for the prevention and preparedness side) it is necessary to have a robust risk assessment methodology that puts hazards, vulnerabilities and finally risks in the right framework.

- DG ECHO guidelines ([1]) focus on the identification of national risks (hazards). These guidelines offer some methodological elements for the assessment of risk. However, these

were neither tailored to critical infrastructures, nor did they provide detailed impact assessment guidelines.

We aim to use the methodological elements of the staff working document issued by DG ECHO back in 2010 and map this to the assessment of risks of critical infrastructures enriching it with elements that are pertinent for CI (e.g. interdependencies). The combination with the "overview of risks report" allows for a clearer picture of how MS interpreted and implemented the recommendations. We foresee that this report should be also useful for conducting risk assessment on the pilot cases of the revised EPCIP and for future national risk assessments with a clearer and stronger CI focus. The pilot projects are focused on a sector and have a very specific mandate, while the RA methodology proposed here extends also the impact of the infrastructure disruption to the whole society. As a consequence these two elements are complementary and certainly not mutually exclusive.

A key element that arises by the overview of the above documents is that, beyond the absence of common methodology, MS do not share common terminology, especially regarding CI-related risk assessment. The multiplicity of terms and definitions is clearly depicted in CIPedia, which is a collection of CI-related terms and definitions[1]. The picture becomes even more complicated when CIP-related definitions should also match the DG-ECHO or UNISDR terminology[2], which mainly focuses on disaster risk assessment.

We are aware that we are still far from proposing a methodology that has to be followed by each MS. For this reason we aim to provide insight and guidance. Such EU level guidance could define the necessary components to be included in the risk assessment or the format of the risk output to facilitate the comparability of results.

Based on the level of maturity of National Risk Assessment approaches, as implemented by MS, it is still not feasible to discuss mitigation or risk treatment methods. This report will focus on the methodological considerations of national risk assessment, with respect to CIs.

1.3 Definitions

In this section, the definitions of the terms used are listed. They were mainly retrieved from CIPedia[3].

Critical Infrastructure is 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 [4].

Consequence. The term "consequence" is not well-defined in the CIP literature. While ISO defines consequence as the "outcome of an event affecting objectives", this general definition does not distinguish between consequences for the system or critical infrastructure itself, for people, for the environment, or for the economy. Such distinctions are required because in the meaning of the ECI directive [4], assessment of consequences for people, the environment and the economy is needed according to the cross-cutting criteria. Moreover, the consequences

[1] CIPedia is a Wikipedia-like online community service focusing on Critical Infrastructure Protection (CIP) and Resilience-related issues, provided by the EU FP7 project CIPRNet, more on http://www.cipedia.eu

[2] United Nations Office for Disaster Risk Reduction, Terminology on Disaster Risk Reduction: http://www.unisdr.org/we/inform/terminology

[3] http://www.cipedia.eu

of cascading effects to other infrastructures may need to be also distinguished and assessed. For this reason, in this document we will try to clearly distinguish between the various forms and types of consequences.

We will also refer to **Impact** as the scale of the consequences of a *hazard* or *threat*. In this document, we will distinguish between *CI Impact* (direct consequences to the CI), *CI Cascade Impact* (indirect consequences to a CI due to a failure of another CI) and *Societal Impact* (consequences for people, the environment and the economy).

Hazard. We adopt the UNISDR definition, where hazard can be any "dangerous phenomenon, substance, human activity or condition that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage" [9]. Throughout this document we refer to this term as synonymous to **threat**.

Resilience. The term resilience means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents [10]. However, resilience is still a relative new term and there is an ongoing debate with respect to its exact definition.

Risk. This is a problematic term because it is used either according to the traditional ISO definition or as an synonym of *hazard* or *threat*. We will consider risk as "the combination of the consequences of an event or hazard and the associated likelihood of its occurrence" [11].

Risk management is the systematic application of management policies, procedures and practices to the activities of *communicating*, *consulting*, *establishing the context* and *identifying*, *analysing*, *evaluating*, *treating*, *monitoring* and *reviewing* risk (based on the ISO Guide 73:2009 [12].

Risk assessment refers to the overall process of:

- *risk identification* - process of finding, recognizing and describing risks,
- *risk analysis* - process to comprehend the nature of risk and to determine the level of risk, and
- *risk evaluation* - process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk treatment refers to any process to modify risk[4] and it can involve:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk,
- taking or increasing risk in order to pursue an opportunity,
- removing the risk source,
- changing the likelihood,

[4] In the CIP domain, this term can be sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction"

- changing the consequences,
- sharing the risk with another party or parties (including contracts and risk financing), and
- retaining the risk by informed decision.

Single-risk assessments determine the singular risk (i.e. likelihood and consequences) of one particular hazard (e.g. flood) or one particular type of hazard (e.g. flooding) occurring in a particular geographic area during a given period of time [1].

Multi-risk assessments determine the total risk from several hazards either occurring at the same time or shortly following each other because they are dependent from one another or because they are caused by the same triggering event or hazard; or merely threatening the same elements at risk (vulnerable/ exposed elements) without chronological coincidence [1].

Scenario is a hypothetical situation consisting of an identified threat or hazard, an entity impacted by that hazard, and associated conditions including consequences, when appropriate [13].

CHAPTER 2

National Risk Assessments: methodological findings

In order to identify methodological gaps on the MS' risk assessments regarding CI, we will first examine which hazards were identified by the MS and how they were assessed in terms of likelihood and impact. In several cases, MS followed a *scenario-based approach*, so we will also comment on the elements required in order to perform a scenario-based analysis with a stronger CI depiction and analysis.

2.1 Risk Assessment Recommendations

The DG-ECHO guidelines of 2010 follow a standard ISO31000 approach, where *risk* is considered as "the combination of the consequences of an event or hazard and the associated likelihood of its occurrence" [11]. When prevention and preparedness against a hazard is considered in the risk assessment, then risk can be quantified as a "function of the probability of occurrence of a hazard, the exposure (total value of all elements at risk), and the vulnerability (specific impact on exposure)".

The recommendations opt for a 5×5 risk matrix as a means to visualise results, such as the one presented in the figure below.

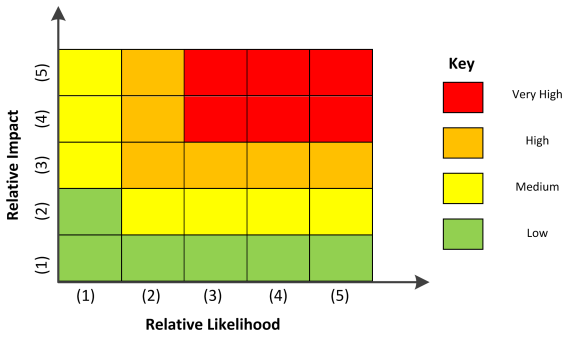

Figure 2.1: *Example of Risk Matrix [1]*

Assessment of risks should be conducted based on three different impact criteria: *human*, *economic* (including *environmental*) and *political*/*social* consequences; quantitatively for the first two categories, such as number of deaths/injuries or costs in euros, and with a qualitative scale for the third category. MS should present their risk assessments for each scenario in a non aggregated way, i.e. in three different risk matrices (see Figure 2.1) – one for each consequence

category. The time horizon for assessments was recommended to be developed from the initial 1–5 years, while MS could include risks foreseen for the coming 25–35 years.

Furthermore, the guidelines describe the dimension of cross-border risks, the implementation of multidimensional risk analyses or risk analyses of multiple incidents that occur independently or as a consequence of other incidents. Finally, the guidelines describe the importance of creating *risk maps*, depicting spatial distribution of major hazards, of assets to be protected and their respective vulnerability, though the use of Geographical Information Systems (GIS). These could be used at a later stage for creating aggregated risk maps (cross-border or multi-risk ones).

The need for a common understanding of risk terminology and methodology within the EU is also highlighted in [14]. This document further urges MS to identify, analyze and assess *single-risk scenarios* and as a further step also consider *multi-risk scenarios*. Methodologically, both qualitative and quantitative methods should be considered.

2.2 Implementation results

All the above recommendations set the conditions for a more unified approach by the MS. Despite the use of a common, 5×5 risk matrix, comparison of the results still remains difficult as, upon implementation, the MS have attributed different likelihood and impact scales, time frames, varying terminology and risk scenarios. While this diversity in approaches enriches the overall recommended approach, a more unified approach would allow for cross-border risk assessments and for better coordinated risk management within the EU. Moreover, the issue of CI loss and the assessment of related risks is not addressed in depth by the MS, as we will observe on the sections that follow.

2.2.1 Hazards

From the overall list of hazards identified in the NRAs, the following ones are identified as the most important [3]:

- Natural Hazards
  - Floods
  - Severe weather
  - Wild/Forest fires
  - Earthquakes
  - Pandemics/epidemics
  - Livestock epidemics
- Man-made hazards
  - Non malicious
    - Industrial accidents
    - Nuclear/radiological accidents
    - Transport accidents
    - **Loss of critical infrastructure**
  - Malicious

- Cyber attacks
- Terrorist attacks

We observe that the *loss or disruption of critical infrastructure* is considered separately as a man-made hazard (unintentional, accident). The inclusion of CI loss as a specific risk highlights the fact that MS consider the probability of such an event as important. More specifically, this risk was identified by seven MS, namely Czech Republic, Germany, Ireland, the Netherlands, Poland, Sweden, and the United Kingdom. This can be partially attributed to the existence of the EPCIP and ECI Directive that have both raised the awareness for the importance of CI disruption and the potential impact on the society.

Table 2.1: *CI-related risk identified*

Country	***Risk Level***	***Term used***
CZ	High	Critical infrastructure disruption
DE	-	Outage of critical infrastructure
IE	High	Loss Critical Infrastructure
PL	Medium	Disruption of electricity supplies, of fuel supplies, of natural gas supplies
SE	Very High	Disruption in food supply due to fuel shortages
UK	High	Attacks on Infrastructure
NL	Very High	IP Network failure, Malicious prolonged electricity failure
	High	National power failure, malicious power supply failure
	Medium	Malicious gas supply failure

According to the report and as depicted in the table above, Germany, Ireland and the Czech Republic address loss of CI in general terms, while Poland, the Netherlands, Sweden and the United Kingdom focus on disruptions to energy supply linked to loss or damage to infrastructure "essential for the maintenance of vital societal functions". Netherlands also refers to IP Network failure, taking into account the ICT sector. Regarding the Transport sector (ECI directive), several transport related accidents have been taken into account (DK, EE, IE, NL, NO, SE, SI, UK), but without an explicit reference to CIs.

The effects on citizens arising from disruption or damage of the services provided by the CI depend on multiple factors (duration, time of occurrence, presence of mitigation controls, etc.), but can potentially cause impact to the society (well-being of citizens, economic consequences and others). However, the terminology used remains ambiguous. While the technical failure and subsequent unavailability of a CI can occur due to technical vulnerabilities, the use of "loss of CI" as a term does not necessarily reflect the same meaning in all scenarios, an observation which is taken under consideration in Germany's NRA, during the scenario design.

Another issue is that according to their national policies, MS do not include the same types of CI (sectors) in their assessments, nor do they place the same focus on all types of CI disruptions.

Hazard dependency. The dependency between natural hazards is taken into account by few MS in their assessments [3]. As depicted in Table 2.2, MS have considered the increased likelihood of specific natural hazards due to the occurrence of other natural hazards.

CI loss can also be the direct impact of several hazards and may cause additional societal impact, which needs to be considered but, at the same time, not overestimated due to double

Table 2.2: *Hazard Dependency or Correlation*

Hazard	***Cascade or correlated hazard***	***Country***
Severe weather phenomena	Flood	DK, NO, RO, HU, UK
	Landslides	IT
	Forest Fires	HU, IE, LT
	Pollution, **CI loss** or Transport accidents	DK, LT, SE, NO
Earthquakes	Landslides	HU, IT
	Tsunamis	EL
Landslides, Earthquakes, Volcanos	Transport Accidents	NO, IT, EL, UK
Nuclear, chemical and transport accidents, **CI loss**	Contamination, Pollution	DK, LT, UK, NO
	Terrorist & Cyber attacks	NO, UK
CI loss	Flood, Pollution, **CI loss** or Pandemics	UK, IE
		DK
Pollution	Pandemics	EE, SE

quantifications. The issue of cascade effects is partially addressed by some NRAs. In fact, impacts on critical infrastructure and their services can be considered in the risk assessment of other natural and man-made hazards as part of the scenario structure, as is the case of NRA performed by Germany and Denmark. We also observe that CI loss is taken into account when assessing Natech risks. For example, CI loss can occur with a higher likelihood due to *severe weather phenomena*, *landslides*, *earthquakes* or *volcanos* (see Table 2.2).

Moreover, several MS identify correlations between CI loss and other risks. Examples include associating CI loss with an increased risk of contamination, environmental pollution, as well as further cascade effects on other CIs across a range of sectors. CI loss may also be linked to increased risks of terrorist and cyber-attacks. Finally it can affect pandemic risks due to manpower shortages.

2.2.2 Probability/Likelihood criteria

If we consult the detailed results of the EU risks overview[5], we observe that several MS rely on semi-quantitative scales, i.e. “very low/very rare (1)” to “very high/very likely (5)”, while a few attribute the frequency of occurrence to the scale. Examples of approaches include the frequency of one or more incidents in various time scales (CZ, IE, LT, NO, PL, HU) or probability of occurrence within 1 year (EE, EL). Norway also considers intentional events and whether a threat is perceived as likely or not, in terms of motivation.

While the probability of a specific hazard to occur is assessed by the MS (including in some cases the probability of a CI loss), this measure refers to the initial probability of the risk scenario occuring. However, the likelihood that the event will cause damage (a) to specific CI or (b) to dependent CIs is not assessed. This analysis requires a detailed *mapping of potential dependency chains* among CIs [15, 16]. The likelihood that one or more CIs are damaged could be assessed based on previous incidents, on the exposure level or vulnerability of the CI to the initiating hazard and/or to the loss of the service of another CI.

Alternatively, one can assume a *worst-case scenario* where all dependent CIs and their services fail, despite the presence of resilience mechanisms. The overall effect of the loss can

[5] Annex 4(b) of [3]

then be assessed in terms of impact. This, also, requires a detailed depiction of dependencies. The assessment of impact is not a straight-forward process, as impacts shouldn't be *overestimated* (due to double calculations). Moreover, when *mutual dependencies* occur, the overall effect of the initial event may be augmented and the recovery process more difficult.

2.2.3 Impact criteria

For the purpose of the DG-ECHO guidelines three types of impacts were defined:

- Human impacts (in numbers);
- Economic and environmental impacts (in Euros);
- Political/social impacts.

The political/social impacts would generally refer to a semi-quantitative scale comprising a number of classes, e.g. (1) limited/ insignificant, (2) minor/ substantial, (3) moderate/serious, (4) significant/ very serious, (5) catastrophic/ disastrous. To make the classification of such latter impacts measurable, the MS adopted their own varying sets of criteria, while other partially implemented the guidelines. For example, several MS do not offer impact assessments on their scenarios or omit specific criteria, especially the political/social ones, which are more difficult to quantify.

The recommended approach complies with the cross-cutting criteria of the ECI directive, namely:

(a) casualties criterion (assessed in terms of the potential number of fatalities or injuries);

(b) economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);

(c) public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services).

In essence, the impact assessment recommendations are compatible and very similar. However, their implementation depicts clearly the ambiguity when it comes to terminology [3]. Only a few MS (EE, EL, LT, IE) attempt to capture the effect of CI loss, in two main ways:

- as a means to measure *political* or *social* impacts (e.g. loss of "*vital services*"):
  - for different levels of operation (partial or total disruption),
  - for varying time frames,
  - for varying geographical ranges,
- or as a means to measure *economic* losses (e.g. IE renames the criterion as "infrastructure").

In essence, the loss of CI directly translates to loss of vital services and affects the citizens. However, one needs to assess the social effects of the hazard, but also the damage

caused to the CI and then the subsequent loss of services (and their respective consequences to the citizens).

If we also consider the dependencies between CIs, this process does not include only one step, but several of indirect losses of CIs and additional social consequences. Since April 2015, The Netherlands updated the two categories of impact used for NRA [17]:

- Category A: at least impact on one of the following four impact categories:
  - physical impact: > 10.000 casualty, serious wounded or chronically ill
  - economic impact: > 50.000 million euro damages or 5.0% decrease in real income
  - social-psychological impact: > 1 million persons are emotionally affected or experience serious societal survivability problems
  - ***cascade impact***: this disruption causes failure of at least two other (critical) sectors [6]
- Category B: at least impact on one of the following three impact categories:
  - physical impact: $>$ 1.000 casualty, serious wounded or chronically ill
  - economic impact: $>$ 5.000 million euro damages or 1.0% decrease in real income
  - social-psychological impact: $>$ 100.000 persons are emotionally affected or experience serious societal survivability problems

We observe that on the high level criterion (category A), cascade impacts are assessed, in terms of affected sectors. This is an indication that at least one MS has considered the above argument, regarding the assessment of cascading effects.

[6] Note that the conditions under which a sector is considered as failed remain unclear in this document [17].

CHAPTER 3

Identified Gaps

In this section we outline our observations on the current methods and results for NRA, as reported by MS [3], with a strong emphasis on CIs. We envision national risk assessment with a strong CIP focus, namely *CI-rich NRA*. Such an approach would allow to establish closer links at EU level in Disaster Management (DG-ECHO) and Critical Infrastructure Protection (DG-HOME).

Disambiguation of terms. One of the major problems of the current approaches, is that CI loss is considered both as a *hazard* and as a *consequence*. This introduces lack of clarity when it comes to risk assessment, both in terms of results and on their presentation. This indicates that a clearer hazard list is required.

Incomparability of results. In general, when comparing various hazards and respective risk scenarios a quantitative comparison may not always be feasible, due to the different nature of the risks analyzed. When considering similar risk scenarios among different MS and their NRA methodologies, some comparisons can be performed. To this end, it would be useful if MS used similar methods, especially with respect to threat likelihood/impact quantifications. In the previous section, we identified multiple approaches regarding the type and scale of impacts, time frames, etc.

The above observation is general; it applies for disaster-centered assessments, even without considering the specific elements of critical infrastructures. When considering CI-rich NRA, the lack of compatibility between methodologies augments, as this is an inherent more complicated problem to solve.

Absence of dependency modelling and analysis. If we want 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 depicted in Figure 3.1.

We observe that upon the implementation of the DG-ECHO guidelines, the MS had to tackle already the complexity of dependency, both between hazards and between the affected CIs. This is clearly presented in Table 2.2, where few MS have tried to take into account such correlations between the occurrence of hazards, including CI loss.

"Weak consequence analysis". Consequence analysis ideally should address both *direct* and *indirect* effects. As a case example of direct effects, when considering the case of a *flood hazard* scenario, the following possible disruptions are identified [18]:

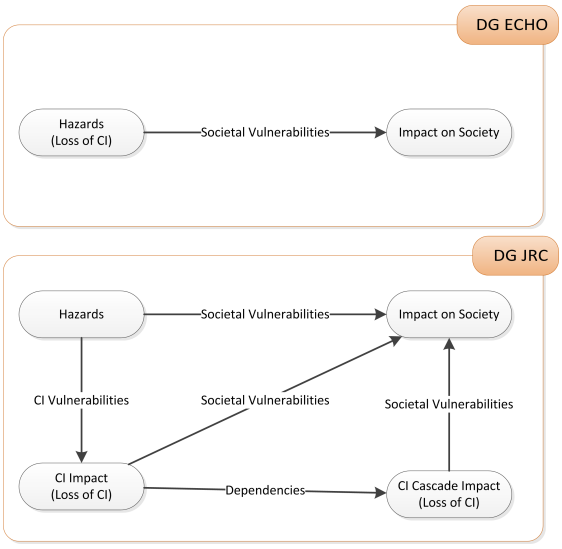

Figure 3.1: *Comparison of single-risk approaches*

- 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.

We observe that a flood can cause multiple, direct damages to CIs of various sectors (e.g. Transport, ICT, Energy, etc.), beyond the immediate societal consequences. While the list is not exhaustive and these disruptions are unlikely to happen all simultaneously, they depict the complexity of mapping the direct and indirect effect of a scenario to national critical infrastructures. Calculating the overall societal impact of a scenario is a difficult process as consequences can be augmented due to parallel disruptions or because it is not easy to avoid double calculations of expected effects. The case of previous incidents may allow for more realistic assessments, but this is not always the case when examining unknown, national risks.

Lack of Vulnerability Assessment. Vulnerabilities may be associated with physical (e.g., no barriers or alarm systems), cyber (e.g., lack of a firewall), or human (e.g., untrained guards) factors [13]. Vulnerability assessment should be part of a full risk assessment. It involves the evaluation of specific threats or hazards to various levels of analysis: to *CI* or *asset* level, to *system* or *network* level (presence of dependencies or likelihood of cascade), or *society* level (degree of exposure to a hazard).

Lack of cross-border scenarios. CIs are complex, interdependent systems (or systems of systems) and the consequences of their disruptions may extend beyond the geographical borders of a MS. The report [3] envisions a pan-European scenario and matrix for each examined hazard. Such pan-European scenarios could build on the scenario-building approach undertaken in national assessments and allow this overview to concentrate its attention on risks with a cross-border dimension. However, the above gaps (comparability of results, ambiguity of terms, need for dependency analysis) hinder even further the development of such scenarios.

Other things to consider is that “including multiple scenarios that contain the same event could lead to double counting the risk.[13].” Moreover, several other infrastructures may face common-cause or cascading disruptions that augment the impact and complexity of the scenario.

CHAPTER 4

A new approach: CRitical Infrastructures & Systems Risk and Resilience Assessment Methodology (CRISRRAM)

In this chapter we aim to provide a methodology that takes into account the methodological findings and gaps identified in the previous chapters. The main characteristics of the proposed methodology is that it adopts a system of systems approach and aims to address issues at *asset level*, *system level* and *society level*. In addition, it follows an all-hazards approach, which is an important element considering that DG ECHO policy is more focused on natural disasters while DG HOME policies embark on the security and man-made hazards.

What is described in Figure 4.1 is a single hazard, scenario-based approach, that is certainly applicable for conducting NRAs however, focused on CIs. The society layer matches the requirements of DG-ECHO guidelines but it goes a step further and includes in a more robust and coherent way the aspect of critical infrastructure disruption which is a crucial element of EPCIP. According to the methodology, a hazard may pose direct impact to society or it may also affect key assets and systems, which in turn may affect the citizens, the environment or the economy.

These various direct or indirect impacts are reflected in the layered approach which is proposed.

- **Society layer.** The proposed methodology starts with the definition of a hazard scenario that may directly have an impact on the society (e.g. flooding, earthquake) but at the same time it may impact a critical infrastructure. This layer complies with the national risk assessment guidelines as risk is 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 CIs (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*).
- **Asset layer.** It is possible to provide an estimation on the direct impact on one or more directly affected CI, on the basis of historical data, the results of vulnerability assessment of the CI or the presence of resilience mechanisms. This is usually assessed in terms of inoperability level or economic loss per each asset. This direct effect to each CI - a service degradation, a disruption or a failure- is related to an impact at societal level. If this is not the case then this infrastructure should not be considered as a CI at first hand. This assessment links asset level disruptions with societal impact.
- **System layer.** When the selected hazard scenario indirectly affects other CI, then we

have to consider the dependencies among these CIs. Interdependencies are a key issue in modern critical infrastructures. As a consequence, dependency assessment should be introduced in our risk assessment framework. Modelling, simulation and analysis tools provide a good idea of the rippling effects in interconnected systems that finally lead to societal impact due to these indirect effects. However, this may be a continuous loop since interdependencies among infrastructures may lead to cyclic increase of indirect effects. It is clear that this can lead to augmented impact at societal level.

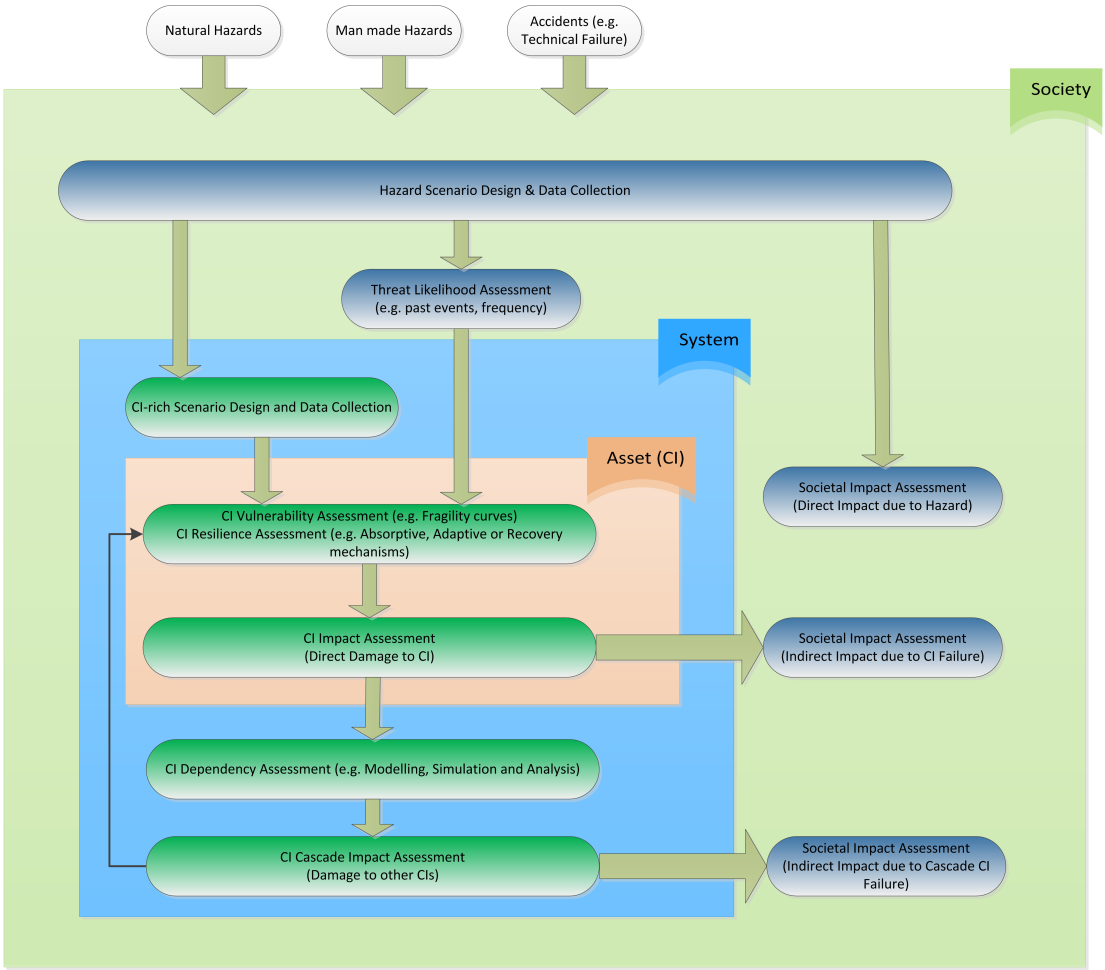

Figure 4.1: *Proposed CI-rich NRA methodology*

The risk assessment layers and steps of this methodology are partially covered by existing risk assessment methodologies identified in [2]. Several of them cover the overall risk management process (not only the risk assessment step). Risk treatment is achieved through various mitigation strategies, countermeasures or resilience mechanisms, but this methodological step is considered out of scope for this report.

We observe that only a limited number of these methods and tools focuses on designing scenarios. An example is the Risk and Vulnerability analysis (RVA) by DEMA, which dedi-

cates a specific step on scenario design. Most methods usually focus on a specific, predefined threat scenario 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.). Regarding vulnerability assessment, the BIRR method introduces the concept of VI (Vulnerability Index) and PMI (Protective Measures Index), 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 scale for vulnerability assessment. Sandia Risk Assessment Methodology takes into account the protection system effectiveness and this is expressed in terms of reducing the probability that a threat is successful. In terms of resilience, BIRR introduces a RI (Resilience Index), which provides an evaluation of how resilience an asset based on Robustness, Resourcefulness and Recovery mechanisms. CARVER2 similarly considers the presence of redundancy mechanisms even if resilience is not mentioned clearly. RAMCAP-Plus includes a step named “Risk and Resilience Management” which highlights how central is this element in the methodology. Interdependencies are covered by most methods as this is a key element for CIs, but the techniques used and the level of detail varies significantly among these methods.

4.1 CI-rich scenario design and data collection requirements

A scenario-based approach to NRA was recommended both by DG-ECHO [1] and applied by several MS [3]. It is also supported by the DHS’ guidelines for National CI Risk Management [13]. The use of scenarios is considered a means to tackle the complexity of the problem; scenarios are used in order to “divide the identified risks into separate pieces that can be assessed and analyzed individually” [13]. The use of such scenarios should identify which infrastructures are more critical (potential consequences would be highest) and then where security and resilience activities should be focused on these nodes.

During the FP7 CIPRNet project, JRC in collaboration with Fraunhofer and CEA examined the requirements of such cross-border scenarios [18]. It quickly became apparent that the identification of key assets (infrastructures) and their operational condition is essential when running a cross-border, scenario-based exercise.

In the CIPRNet project, each scenario phase is described according to a specific template which covers the following information [18]:

- **Timeframe** / **Duration:** This can be marked with specific points of time or specific events;
- **Incident description:** This reflects the current situation of the phenomenon/threat studied;
- **Affected infrastructure(s):** Information to be included is the name, the sector, the location, the operational status and the mode of operation (e.g. normal, stressed, recovery, etc.) for each affected infrastructure;
- **Maps:** This is needed in order to depict visually the status of each phase;
- **Consequences:** Direct damage to infrastructures is also needed in each phase, as this will allow for overall estimate of the societal consequences of the whole scenario.

We consider that the approach presented in this report is certainly applicable to cross-border regions and scenarios. However, the applicability is not straightforward and this is related

to the governance models that exist in different regions. Several steps need to be taken that can be summarised into the following points:

- Agreement on a common glossary of terms in order to facilitate communication and define scenarios in a consistent way
- Identification of critical infrastructures or elements of CIs that are of common interest
- Define a common threat scenario

Once those steps are performed then the RA methodology presented here can be applied in the same manner as it would be the case for a national CI. In other words the RA methodology presented here is the kernel around which certain features have to be added or omitted depending on the case study (national, cross-border or EU level analysis).

4.2 Multi-risk assessments

If we consider multi-risk scenarios, the problem becomes even more complex, as multiple hazards can modify the capacity of infrastructures in unexpected way. If we consider cross border scenarios, such complexity becomes further increased. The Threat Likelihood Assessment (see Figure 4.1) would need to take into account correlations between hazards. As a consequence it is a challenge that remains to be tackled mainly due to its intrinsic complexity. Certain hazards (e.g. flooding) may kick-off other disasters (e.g. landslides) that may increase the direct effect on both the CIs and society. One approach would be that this is already taken into account in the definition of the scenario and then follow the whole RA methodology as already described. However, a robust methodology for defining multi-hazard scenarios is necessary taking into account correlations among hazards.

4.3 Risk and Resilience Management

While this report focuses mainly on risk assessment, this can form the basis for alternative risk treatment options to be examined. Since the approach is scenario-based it considers known or foreseen threats. However, risk management should also consider unknown threats, which is more in line with the current approach to focus on resilience-oriented approaches. This means that the countermeasures should not only focus on preventing a hazard or protecting an asset, but also on enhancing the asset resilience, i.e. enhancing the absorptive, adaptive and recovery capabilities of a CI [19] or a combination of CIs, which offer vital services to a community.

CHAPTER 5

Conclusions and recommendations

The aim of the present report is to provide an overview of the RA status in MS and how this can be linked with the work and policies on Critical Infrastructures (EPCIP) in order to provide elements that could be useful for shaping future policies in the domain of Critical Infrastructure Protection and Resilience taking stock of existing efforts and legislation. Resilience needs certainly to be considered as an element that can complement traditional risk assessment.

In order to implement the risk assessment framework presented in the previous chapters a number of elements need to be further developed. In the following paragraphs these are listed and recommendations for action at policy level are also presented.

Need for modelling and simulation

Critical infrastructure owners and operators have expressed on several occasions the importance of developing tools and methodologies for modelling and simulation in CIP. It is true that in the recent years, an important number of tools has been developed and can be used for the assessment of a wide range of disruptive scenarios. It seems though that most of those tools lack the features to be used throughout Europe and become the standard in the field. In principle, these represent ad-hoc efforts that are tailored to the needs of a particular region/state and as a consequence lack the capability to scale to international level. A common repository or toolbox, comprising risk assessment methodologies and the tools necessary to perform a risk analysis (e.g. checklists, scenarios, templates, models, etc.) is needed. Furthermore tools to tackle multiple hazards, consider the asset, system and society dimensions as well as interdependencies are required in order to implemented a holistic approach.

Several efforts take place in Europe and aim to obtain this. An important example is the CIPRnet EISAC effort that aims to create a centre to develop such competencies and tools to simulate critical infrastructure disruptions at various levels. Such efforts need to be appraised and appropriately considered at EU policy level. JRC is also contributing in this direction with the development of GRRASP (Geospatial Risk and Resilience Assessment Platform) that aims to provide capabilities to MS to analyse critical infrastructures disruptions. In order to further support the need for developing tools with a more abstract view we quote [13]: “The level of detail and specificity achieved by using the most sophisticated risk assessment models and simulations may not be practical or necessary for all assets, systems, or networks. In these circumstances, a simplified dependency and interdependency analysis based on expert judgment may provide sufficient insight to make informed risk management decisions in a timely manner.”

Need for harmonized impact scales

By performing the study in this report we identified that harmonised impact scales are required in order to facilitate the development of international or cross-border risk assessments. An important issue is that a clarification between direct and indirect effects is necessary since in that way it is possible to avoid double counting of impact. The aim is to be able to present comparable results and exchange expertise among MS.

An open issue remains the uncertainty of the assessments ([13]). Even when a scenario with reasonable worst-case conditions is clearly stated and consistently applied, there is a range of outcomes that could occur. For some incidents, the consequence range is small, and a simple estimate may provide sufficient information to support decisions. If the range of outcomes is large, the scenario may require more specificity about conditions to obtain appropriate estimates of the outcomes. However, if the scenario is broken down to a reasonable level of granularity and there is still significant uncertainty, the estimate should be accompanied by the uncertainty range to support more informed decision making. The best way to communicate uncertainty will depend on the factors that make the outcome uncertain, as well as the amount and type of information that is available.

Identification of common or cross-border scenarios

The adoption of a common RA methodology across countries and cross-border regions opens the way for a closer collaboration on issues of common interests. Borders impose discontinuity in terms of governance but this is not the case for several threats. In addition many cross-border regions operate and depend on the infrastructures that are based on both sides of the borders and as a consequence coordinated and harmonised action may be needed. In this framework the development of exercises is crucial and the adoption of a harmonised RA process helps in defining common or joint scenarios.

Involvement of the private sector (CI operators)

Due to the evolved governance model of modern critical infrastructures it is necessary to involve CI operators in performing Risk Assessments. Operators have a much better overview of the risks that their infrastructures may face and also what would be the impact (at asset level though). Close collaboration and exchange of information is necessary with the authorities in order to feed this information into the RA framework that can allow to identify the impact at system level taking into account interdependencies and finally to obtain an overview of the total economic impact.

Dynamic analysis is needed

In accordance with the report [3] a pan-European scenario and matrix for each hazard could be conceived. This is the point where the CIP element should be identified and tackled accordingly. All the modelling and simulation activities which will be needed both for the depiction of the scenario and the assets (CIs) that are affected should allow for time-based analysis as both the operability levels of each affected CI and the dependencies between them may change over time.

Acknowledgements

This work has been supported by the “Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme” by means of an Ad-

ministrative Arrangement (contract no. HOME/2011/CIPS/AA/001-A1). This support is greatly appreciated.

Bibliography

[1] E. Commission, "Commission staff working paper: Risk assessment and mapping guidelines for disaster management." 21.12.2010, sEC(2010) 1626 final.

[2] 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.

[3] E. Commission, "Commission staff working document overview of natural and man-made disaster risks in the eu," Brussels, 8.4.2014, sWD(2014) 134 final.

[4] E. Council, "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." 2008.

[5] E. Commission, "Commission staff working paper on a new approach to the european programme for critical infrastructure protection - making european critical infrastructures more secure," 28.8.2013, sWD(2013) 318 final.

[6] L. Galbusera, G. Giannopoulos, and D. Ward, "Developing stress tests to improve the resilience of critical infrastructures: a feasibility analysis," Luxembourg: Publications Office of the European Union, JRC Science and Policy Reports JRC91129, 2014.

[7] "Global risks 2015: 10th edition," World Economic Forum, Tech. Rep. REF: 090115, 2015.

[8] "ISO31010:2009 - Risk management – Risk assessment techniques," *International Organization for Standardization*, 2009.

[9] UNISDR. (2009, May) 2009 UNISDR Terminology on Disaster Risk Reduction, United Nations International Strategy for Disaster Reduction. [Online]. Available: http://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf

[10] "Presidential Policy Directive – Critical Infrastructure Security and Resilience, PPD-21, The White House, Office of the Press Secretary, U.S.A." The White House, Office of the Press Secretary, February 2013.

[11] "ISO31000:2009 - Risk management–Principles and guidelines," *International Organization for Standardization*, 2009.

[12] "ISO Guide 73:2009 - Risk management–Principles and guidelines," *International Organization for Standardization*, 2009.

[13] "Supplemental tool: Executing a critical infrastructure risk management approach," U.S. Department of Homeland Security, Tech. Rep., 2013. [Online]. Available: http://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf

[14] C. of the European Union, "Council conclusions on further developing risk assessment for disaster management within the european union," 11 and 12 April 2011, 3081st JUSTICE and HOME AFFAIRS Council meeting.

[15] P. Kotzanikolaou, M. Theoharidou, and D. Gritzalis, "Cascading effects of common-cause failures in critical infrastructures," in *Critical Infrastructure Protection VII*. Springer, 2013, pp. 171–182.

[16] ——, "Assessing n-order dependencies between critical infrastructures," *International journal of critical infrastructures*, vol. 9, no. 1, pp. 93–110, 2013.

[17] M. of Security and Justice, "Voortgangsbrief crisisbeheersing, the netherlands," 09-04-2015. [Online]. Available: https://www.nctv.nl/Images/voortgangsbrief-150415_tcm126-590874.pdf

[18] Y. Barbarin, M. Theocharidou, and E. Rome, “CIPRNet deliverable D6.2: Application scenario,” CEA, JRC, Fraunhofer IAIS, Tech. Rep., May 2014. [Online]. Available: https://www.ciprnet.eu/

[19] R. Francis and B. Bekera, “A metric and frameworks for resilience analysis of engineered and infrastructure systems,” *Reliability Engineering & System Safety*, vol. 121, pp. 90–103, 2014.

LB-NA-27332-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

doi:10.2788/621843
ISBN 978-92-79-49246-4

Publications Office