

# RECIPE

Recommended Elements of Critical Infrastructure Protection for policy makers in Europe



## GOOD PRACTICES MANUAL FOR CIP POLICIES

For policy makers in europe



# Good practices manual for CIP policies

For policy makers in Europe

*RECIPE*





With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme.

European Commission - Directorate-General Home Affairs

This project has been funded with the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Justice, Freedom and Security. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

# Foreword

The protection of critical infrastructures is a topic that is increasingly relevant in today's society. The dependency of our society and citizens upon services delivered by those infrastructures steadily grows. Disturbances in the functioning of critical infrastructures may have far reaching effects upon our national economies, our health, the well-being of people, our ecology, and the functioning of our governments.

Many countries are currently developing and implementing their critical infrastructure protection (CIP) policies. European CIP policymakers can benefit from sharing each others' good practices in this field. This motivated the RECIPE project team to collect and gather good practices on a number of CIP-policy related topics.

Before you lay the results of our efforts to put together an accessible and helpful manual for you as a CIP policymaker. The manual is meant to support you in composing a balanced and complete set of CIP policies fitting your national or regional needs.

As every good meal begins with good ingredients, we began gathering good practices for CIP policies from all over Europe and abroad. This resulted in an abundance of CIP ingredients. Each would bring their own particular flavour to any given mix of CIP policies and each poses different requirements to the kitchen or the cook.

In this manual we try to give you a balanced overview over a selected set of attractive ingredients. One should realise that one ingredient is not necessarily better than an other; its is the combination that makes the tasty meal.

We hope that this manual will assist you in putting together an attractive and satisfactory menu of CIP policies. Enjoy!

On behalf of the whole RECIPE team,

Marieke Klaver





# Contents

<b>1</b>	<b>Management summary</b>	<b>7</b>
<b>2</b>	<b>Introduction</b>	<b>9</b>
2.1	The need for Critical Infrastructure Protection	9
2.2	The need for good practices in CIP	9
2.3	Areas of interest in CIP policies	9
2.4	Policy transplantation	10
2.5	How to use this manual	13
<b>3</b>	<b>Identification of Critical Infrastructure</b>	<b>15</b>
3.1	General description and main issues	15
3.2	Good practices	19
3.3	References and further reading	25
<b>4</b>	<b>Dependencies</b>	<b>27</b>
4.1	General description and issues	27
4.2	Good practices	31
4.3	References and further reading	38
<b>5</b>	<b>Public-Private Partnerships</b>	<b>39</b>
5.1	General description and issues	39
5.2	Good practices	41
5.3	References and further reading	48
<b>6</b>	<b>Information sharing</b>	<b>51</b>
6.1	General description and issues	51
6.2	Good practices	54
6.3	References and further reading	59
<b>7</b>	<b>Risk management and CIP</b>	<b>61</b>
7.1	General description and issues	61
7.2	Good practices	63
7.3	References and further reading	69
<b>8</b>	<b>Crisis management and CI</b>	<b>71</b>
8.1	General description and issues	71
8.2	Good practices	74
8.3	References and further reading	82
<b>9</b>	<b>Definitions</b>	<b>85</b>
<b>10</b>	<b>Quick reference to good practices</b>	<b>89</b>





# 1 Management summary

## 1.1 Background

The functioning of modern societies relies heavily on the functioning of Critical Infrastructures, such as electricity, gas, water management and information and communication technologies (ICT). The disruption of these infrastructures may have serious consequences for the economy and well-being of citizens.

As these infrastructures are increasingly becoming interconnected, the protection of Critical Infrastructures (CI) goes beyond the responsibility of individual companies, sectors, and sometimes even beyond nations. A number of EU Member States (MS) have already established policies for the protection of their own national CI; other nations are starting up in this field, often stimulated by the European Directive on the identification and designation of European critical infrastructures.

Although Critical Infrastructure Protection (CIP) is a national responsibility, identifying and sharing information on good practices for CIP policies may support all nations in developing their own CIP policies and programmes.

## 1.2 The project RECIPE

The RECIPE project has the objective to integrate CIP knowledge and experiences by identifying good practices in the area of CIP policies and combining them into a good practices manual.

The manual was developed by a consortium led by the Netherlands research organisation TNO, with project partners from government organisations in the Netherlands, Slovakia, Estonia, and OIIP, an Austrian research organisation.

First, a survey was made of CIP methodologies used in MS and other nations. Based on this initial survey a selection of possible good practices was made by the project partners. The selected methodologies were analysed and described in more detail and combined into a “CIP Good practices manual for policy makers”.

For the background knowledge on the good practices, interviews were performed with a number of government agencies and organisations.

## 1.3 The result

The RECIPE manual organises and outlines CIP good practices for policy makers. The topics covered in the manual start with the methods used by nations to *identify CI* for their own national interests. The need for collaboration on CIP is strengthened by the risk of cascading effects caused by *dependencies*: disruptions in one CI may lead to a cascading effect on other CI and may lead to incidents in the provisioning of important government and private

company services. As CI in most nations are run by private companies, CIP is a mutual public-private responsibility and requires a strong *public-private collaboration*. One of the key elements in enhancing this collaboration towards a better protection is *information sharing*. *Risk management* is the key process used to define adequate and balanced protective measures. This process also helps in identifying the risk scenarios that can only partially be mitigated by taking preventive measures. For this, collaboration is necessary in the area of *crisis management*, should such a scenario happen to occur.

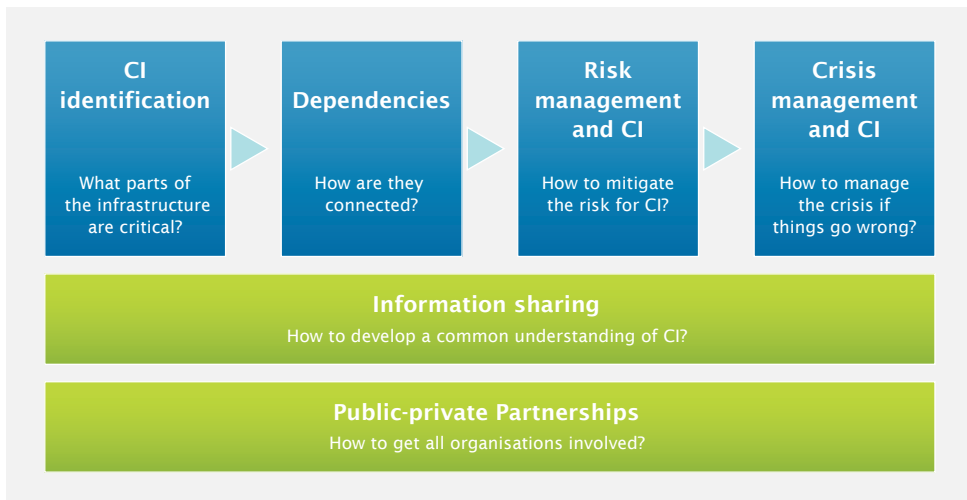


FIGURE 1: CIP fields of interest

In the following sections, you will find a general description of the essential elements of these topics followed by selected good practices. These good practices have been selected to show a number of policy options that have been implemented successfully by other MS. The good practices described cover a wide range of policy options, e.g. ranging from voluntary to more mandated approaches.



## 2 Introduction

### 2.1 The need for Critical Infrastructure Protection

The functioning of modern societies relies heavily on a number of infrastructures, such as electricity, gas, water management and information and communication technologies (ICT). The disruption of these infrastructures may cause serious consequences for the economy and well-being of citizens.

As these infrastructures are increasingly becoming interconnected, the protection of these Critical Infrastructures (CI) goes beyond the responsibility of individual companies, sectors, and sometimes even beyond nations. A number of EU Member States (MS) have already established policies for the protection of their own national CI; other nations are just starting up in this field, often stimulated by the European Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection<sup>1</sup>.

### 2.2 The need for good practices in CIP

Although Critical Infrastructure Protection (CIP) is first and foremost a national responsibility, identifying and sharing information on good practices for CIP policies may support all other nations in developing their own CIP policies and programmes. This manual organises and outlines CIP policy good practices for you as a policymaker. The authors of this manual are grateful to the government agencies, regulators, and CI operators who were kind enough to provide valuable insights into their good and sometimes bad experiences with regard to the development of national CIP strategies and policies. The collaborative knowledge in this manual may help you to strengthen the resilience of your national CI. At the same time, your CIP policies and related activities may improve the overall protection of CI in Europe and are therefore beneficial to all other nations.

### 2.3 Areas of interest in CIP policies

The objective of this manual is to share good practices in the area of CIP policies with you as a CIP policymaker. The topics covered in this manual start with the methods used by nations to *identify CI* for their own national interests. The need for collaboration on CIP is strengthened by the risk of cascading effects caused by *dependencies*: disruptions in one CI may lead to a cascading effect on other CI and may lead to incidents in the provisioning of important government and private company services. As CIs in most nations are run by private companies, CIP is a mutual public-private responsibility and requires strong *public-*

---

1 European Council, Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Brussels, December 2008.  
Online: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF>

*private collaboration*. One of the key elements in enhancing this collaboration towards better protection is *information sharing*. *Risk management* is the key process used to define adequate and balanced protective measures. This process also helps in identifying the risk scenarios that can only partially be mitigated by taking preventive measures. For this, collaboration is necessary in the area of *crisis management*, should such a scenario happen to occur.

The Good Practice themes discussed in this manual are shown in Figure 2.

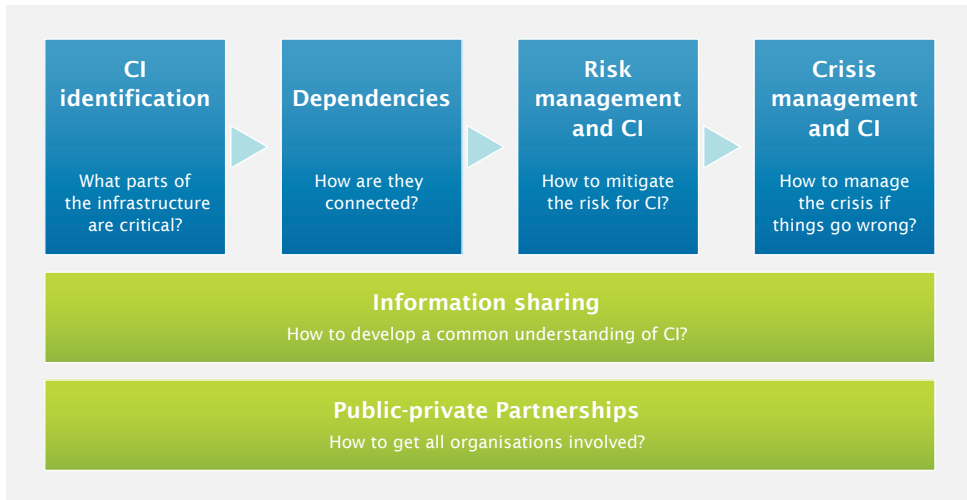


FIGURE 2: Good Practice themes

## 2.4 Policy transplantation

This manual discusses the elements that are essential in adopting the CIP good practices described. This may be linked to the cultural, legal, and political differences between the MS. Some MS prefer to use public-private co-operation to enhance the protection of their CI; other MS prefer to implement legal or other mandatory measures affecting the CI operators. The good practices described in this manual are intended to be accessible to all CIP policymakers in Europe (and even abroad). One should realise, however, that not all good practices are suited to implementation by each nation. Below we will give you some guidance to determine which CIP good practices are better suited to your specific national setting.

To this end, we have formulated three dimensions that describe elements that have a strong influence on the attainability of a large part of the presented CIP good practices. These dimensions are:

– *Involvement of private parties*

Some CIP good practices require extensive co-operation of public and private parties. This is only feasible if a climate of public-private co-operation has been established for the purpose of addressing CIP challenges and trust has been built between the parties.

– *Mandated or voluntary co-operation structure*

In order to get partners involved in new policies that concern them, there are different approaches to involving them:

- The voluntary approach, which in broad terms means that policies are formulated in outlines or in the form of guidance, often in co-operation with the CI sectors. These are communicated to the parties involved, who are encouraged to co-operate by argumentation or negotiation. Additional legislation or supportive actions may be used as a further incentive.
- The mandated approach, which in broad terms means that legislation is used as a starting point and instrument of obligation to achieve co-operation.

Typically, nations are accustomed to one of these structures and will encounter great difficulties using the other.

– *Required CIP maturity*







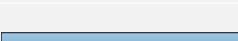
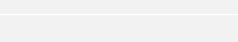

Some nations have extensive experience in CIP; others are relatively new to this field. As some of the CIP good practices in this manual require that a certain amount of CIP groundwork has been done beforehand, the current level of CIP maturity is a strong indicator for the attainability of some of the good practices.

Readers can assess their position in terms of these dimensions. By comparing this to the indicated requirements of each of the good practices, one may get a quick indication of the suitability of the good practice for one's national CIP policy development.

The indicated requirements for these dimensions are indicated using three bars:



Within these bars, a marker (▼) indicates the requirements for the corresponding dimension the good practice poses upon the situation in a nation. Some examples:

	Indicates a low requirement of existing Public-Private Partnership (PPP) structures
	Indicates a high requirement of existing PPP structures
	Indicates that the good practice is more suited for voluntary structures
	Indicates that the good practice is more suited for mandated structures
	Indicates that the good practice is more suited for novice CIP practitioners
	Indicates that the good practice is more suited for experienced CIP practitioners
	Indicates the existence of PPP structures is not relevant to the applicability of the good practice
	Indicates the good practice is equally suited for mandated and voluntary structures.
	Indicates the good practice is equally suited for novice and experienced CIP practitioners.

Section 10 contains a quick reference table to the CIP good practices in this manual, in which the good practices are presented, showing the above-mentioned requirements along with some additional properties.

## 2.5 How to use this manual

This manual gives the CIP policymaker an overview of CIP good practices for the following key topics:

- Identification of CI;
- Dependencies;
- Public-private partnerships;
- Information sharing;
- Risk management and CI;
- Crisis management and CI.

In this manual, a CIP policymaker will find a general description of the essential elements of each of these topics followed by a selection of good practices. These good practices have been selected to show which of the policy options have been implemented successfully by other MS and represent the range of options for the specific policy dimensions mentioned in Section 2.4 “Policy transplantation”.

This manual also discusses the many links between the topics and cross-cutting elements such as Critical Information Infrastructure Protection (CIIP). Where relevant, cross-border topics and elements related to CIIP are identified and described.





## 3 Identification of Critical Infrastructure

### 3.1 General description and main issues

#### *The need for CI identification*

CI can be described as “those infrastructures which are 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 serious consequences”. Some nations use a slightly different definition. The CIP Good Practices in this manual will hardly be affected by such differences.

Although the definition of CI seems to be straightforward, it is a challenging task for nations to determine exactly what assets, objects and services comprise the CI. This process is generally referred to as ‘CI identification’. Basically, CI identification has one purpose: to understand which infrastructures are critical for one’s region, nation or the EU depending upon the scope of the CI identification process. Depending on risk management processes, selective and/or heightened CIP measures may be required for a specific CI asset, group of assets, or a process chain.

#### *Approaches to identify CI*

Overall, there are two general approaches to identify the national set of CI. The first approach is a bottom-up evaluation of all national assets, no matter how defined, applying criteria to evaluate their criticality. This approach was partially tried in the United States, but here, as is also the case elsewhere, this approach has largely been discontinued at national level.

Energy 	Nuclear industry 	ICT 	Water 
Food 	Health 	Financial 	Transport 
Chemical industry 	Space 	Research facilities 	

FIGURE 3: EU defined ECI sectors <sup>[7]</sup>

The second approach identifies the set of CI in a top-down way. This approach has been used by most European nations that have implemented a CI policy. Using this top-down approach, an initial set of CI sectors and subsectors (often known as products or services) is defined which can be reduced or extended in a flexible way. Often governments use the areas of their departments' (infrastructure) responsibilities as a starting point.

Figure 3 shows a set of CI sectors most of which have been identified as national CI sectors by nations.<sup>[2]</sup> Table 1, derived from Appendix 2 of <sup>[7]</sup>, may provide an initial set of critical sectors, products and services. Depending on history, culture and specific geographical circumstances, it may be necessary to remove or add CI services, e.g., social security services, mountain or sea rescue services.<sup>[4]</sup>

There are several approaches to differentiating within these sectors and subsectors between what constitutes CI and what is just important or less important infrastructure. Firstly, the *service-based* approach identifies (national) critical assets within each of the critical services identified based on (sector-) specific criteria that define the level of service required, e.g. number of Megawatts delivered. Secondly, the *operator-based* approach leaves the determination of which assets or services are critical to the nation to the CI operator. The emphasis here is on the service(s) provided by the CI operator. Thirdly, the *asset-based approach* uses elements of both the service-orientated and operator-orientated approaches. These approaches will be elaborated in the good practices described below.

TABLE 1: Initial set of potential CI products and services (from:<sup>[7]</sup>)

SECTOR	PRODUCT OR SERVICE
I Energy	1 Oil and gas production, refining, treatment and storage, including pipelines
	2 Electricity generation
	3 Transmission of electricity, gas and oil
	4 Distribution of electricity, gas and oil
II Information, Communication Technologies (ICT)	5 Information systems and networks protection
	6 Instrumentation automation and control systems (SCADA etc.)
	7 Internet
	8 Provision of fixed telecommunications
	9 Provision of mobile telecommunications
	10 Radio communication and navigation (e.g. Loran, GPS and Galileo)
	11 Satellite communication
	12 Broadcasting
III Water	13 Provision of drinking water
	14 Control of water quality
	15 Stemming and control of water quantity
IV Food	16 Provision of food and safeguarding food safety and security

SECTOR	PRODUCT OR SERVICE
V Health	17 Medical and hospital care
	18 Medicines, serums, vaccines and pharmaceuticals
	19 Bio-laboratories and bio-agents
VI Financial	20 Payment services/payment structures (private)
	21 Government financial assignment
VII Public & Legal Order and Safety	22 Maintaining public & legal order, safety and security
	23 Administration of justice and detention
VIII Civil Administration	24 Government functions
	25 Armed forces
	26 Civil administration services
	27 Emergency services
	28 Postal and courier services
IX Transport	29 Road transport
	30 Rail transport
	31 Air traffic
	32 Inland waterways transport
	33 Ocean and short-sea shipping
X Chemical and nuclear industry	34 Production and storage/processing of chemical and nuclear substances
	35 Pipelines of dangerous goods (chemical substances)
XI Space and Research	36 Space
	37 Research

## Steps to identify CI

A stepwise method to identify CI is offered by the European CI Directive<sup>[2]</sup>. The Directive mandates four specific steps for the process of identifying the ECI. The Directive makes the implicit suggestion that this method can be used for the identification of national CI as well. Below we will describe these four steps from a national CI identification perspective:

1. apply sector-specific criteria,
2. assess criticality,
3. assess dependency issues,
4. apply cross-cutting criteria.

### *Step 1: Apply sector-specific criteria*

A first selection of CI within a sector can be made based on sector-specific criteria. This leads to a short-list of CI from which further deliberations are to be made. The described method clearly favours objective, quantifiable criteria rather than subjective, qualitative criteria.

The Directive has defined only some sector-specific criteria (i.e. ‘gas transmission pipelines that ensure a capacity of at least X million normalised m<sup>3</sup>/h at a transit-border point’).

The EU-wide criteria for identifying ECI have been established only for the energy and transport sectors and soon the ICT sector. For other CI sectors such criteria are still being debated. Note that the European criteria are classified, as are the criteria of most MS.

*Step 2: Assess criticality*

The application of the pre-established definition of a CI is an important step in assessing the criticality of a (potential) CI step, especially for nations who use an operator-based approach in which they need to negotiate with the asset or service owner.

For determining CI at European level, the Directive requires that the potential disruption impact of an asset or service may have a significant impact on at least two or more other MS.

*Step 3: Assess dependency issues*

In this step, the dependencies between CI sectors and subsectors are assessed. This step includes the assessment of cross-border dependencies as well. A number of nations have initiated dedicated programmes to map and understand CI dependency issues, as the complexity of dependencies beyond obvious first order effects increases exponentially. Because of the importance and the complexity of this topic, a separate section has been dedicated to it. More information on analysing CI dependencies can be found in Section 4 “Dependencies”.

*Step 4: Apply cross-cutting criteria*

Cross-cutting criteria remain one of the most important instruments in assessing the level of criticality. An important feature of the cross-cutting criteria approach is that it allows for more uniform segmentation of different criticality or severity ‘levels’ to assess the (potential) impact of loss of an asset or service on the overall vital societal functions. This severity is assessed in terms of the effects on society which can be expressed as deterioration of vital societal functions.



FIGURE 4: Examples of societal functions

Some nations (e.g. Spain, Switzerland and the United Kingdom) have defined three vital societal functions, while other nations (e.g. France, the Netherlands) have more, up to five. Overall, these functions cover the categories of casualty (risk to life and quality of life), economy (risk to the economic system or infrastructure), and public impact (risk to the functioning of government, emergency services and territorial issues).

### *Objectivity of criteria*

Other nations have decided that the focus on individual objective metrics is not an adequate reflection of the true level of criticality in any case. At the same time it may be too legally limiting besides being potentially politically sensitive. These nations use subjective or generalist criteria, such as ‘incident requirement response by local / state / federal government’. While adequate for national purposes, such a framework has the disadvantage of not being easily applicable when discussing cross-border criteria with other nations.

EU MS have concluded that publishing details on the nature of the EU-wide cross-cutting criteria is politically sensitive and not in the public interest. In particular, this applies to such delicate issues as to defining the number of casualties that could arise at various levels of impact. Rather than marking the relevant documents classified and not for public distribution, some nations have decided to use general descriptive criteria (i.e. ‘substantial casualties’) in place of actual metrics.

## 3.2 Good practices

This section will provide you with four good practices for identification of CI:

- Using an operator-based approach is a good practice that shows to what extent CI operators can be involved in the national CIP programme provided that structures for co-operation of operators are in place;
- The Swiss CI identification using a service-oriented approach derives the definition of CI from cross-sectoral criteria applied to centrally defined services;
- The United Kingdom provides a good practice combining the abovementioned approaches into an asset- or hybrid-based approach;
- In contrast to these three centralised approaches, a bottom-up, cross-border approach is found in the Washington – British Columbia corridor that shows how local initiatives can play a role in identifying and protecting CI.

## Operator-based approach

PPP ▼

MANDATED ▼

CIP MATURITY ▼

### Background

France is one of the few examples of a so-called ‘Operator-based approach’ to identifying CI. A very strong ‘mandated’ legal basis for co-operation (most recently updated in the French ‘Sectors of Activity of Vital Importance’ document<sup>[5]</sup> but based on older cold war systems), as well as strong traditional connections with ‘professional and industrial associations’ allows the government to eschew the need to identify individual CI assets directly. Instead, they identify ‘vital operators’, who themselves are legally bound to implement a number of French risk-analysis and risk management directives. While individual assets are also identified as part of this process, the focus of the CI programme is not on individual assets, nor on the services delivered by these assets, but on the existing providers of those services – the ‘vital operators’.

### Description

France has defined 12 critical sectors and 21 subsectors. Each ministry is responsible for identifying the ‘vital operators’ within their own respective area of responsibility. These operators are then legally obliged to fulfil the requirements set out in<sup>[5]</sup> at their own cost. The first overall criterion that is applied is the market share of the individual operator. The second overall criterion maps a ‘failure of service’ of the vital operator against four high-level criteria.

Each ministry maintains close contact with their relevant professional or trade association. In some cases sectoral representation is effected by the national regulator, such as ARCEP (the telecom regulator). The ministry will negotiate with them on, for instance the inclusion of certain operators, and the details of various confidential planning documents. Currently, these planning documents comprise approximately 21 National Security Directives (mandated risk analysis frameworks), the Operator Security Plans, the Special Protection Plan (for each asset) and the External Protection Plans.

Currently, over 220 vital operators have been identified. These vital operators, in turn, have identified around 1,000 critical assets.

### Experiences / Lessons learned

France has shifted more towards an all-hazard approach and examines the applicability of using cross-cutting criteria to identify CI. Holding individual operators accountable has the advantage for the government of being able to delegate risk and responsibility to this level, and have the assessments done from the inside, by the people most familiar with the infrastructure. Such a system to identify CI is generally only possible within a highly mandated CIP approach (i.e., one in which participation of the private sector is compulsory).

Note that some nations that started with voluntary participation of CI operators, e.g., the United States, have increasingly seen the need to strengthen their legal framework for co-operation. In a purely voluntary (non-mandated) framework, the application of the operator-based approach might present considerable challenges.

## Service-oriented approach

PPP ▼

MANDATED

CIP MATURITY ▼

### Background

Switzerland had engaged in CIP-type activities for many decades previous to the advent of the official CIP program, and was thus able to start their dedicated CIP program on the basis of relatively in-depth programs and strong institutional linkages between government and the private sector.

### Description

A “societal-service” approach categorises each subsector into relative levels of criticality, which is determined by the expected impact of a failure of the critical sub-sector on other sub-sectors (interdependencies), on the population, and on the economy. Based on the basic CIP strategy approved by the Swiss Federal Council in June 2009, 28 sub-sectors within 10 sectors have been defined

The Federal Office for Civil Protection as the coordinating agency of the CIP program is responsible – together with the respective federal offices – for the completion of a confidential “CI Inventory” according to three basic criteria: the (if applicable) quantifiable output of the asset (e.g. Megawatt), the role that asset plays in the overall supply chain (functionality), and the hazard potential of that asset (e.g. major accidents). The protection measures of the CIP program are also related to the “National Hazard Analysis” project, which will be periodically reviewed and adapted.

### Experiences / Lessons learned

The Swiss approach provides a comprehensive risk landscape for functional services to society. The approach determines the critical services and the potential need for CIP. The Swiss hazard analysis method includes a regular reassessment of the national risk and thus of the need to (re)adjust CI protective measures.



## Asset- or hybrid-based approach

PPP ▼

MANDATED

CIP MATURITY ▼

### Background

The United Kingdom maintains one of the most extensive CIP programmes in the world. It is best described as asset-based or as a hybrid of a service-based and an operator-based approach.

### Description

The United Kingdom recognises nine critical sectors and twenty subordinate critical services. These services are composed of assets, which need to be identified. The ministry responsible for a sector performs an initial selection of assets and operators (operators are picked on the basis of their relative market share). The Centre for Protection of National Infrastructure (CPNI) does its own assessment in parallel. Based on the combined input of operators, ministry responsible and CPNI, an asset (which can also be a process) is mapped against the consequences of a potential service failure. Six criticality levels (from CAT0 to CAT5) have been identified and are mapped against three specific cross-cutting criteria, namely: impact on life, economic impact, and impact on essential services.

At a public level these criteria are descriptive and subjective only. At the classified level, each of eighteen possible criteria have quantitative and objective values (metrics) assigned to them. This segmentation is done in conjunction with sector-specific criteria which are unique to each of the nine critical sectors. The result is a very small set of assets at the highest criticality levels. Only assets at CAT3 and above are considered to be truly 'critical'. The combination of the CAT-level and the likelihood of attack, which is a combination of the vulnerability (e.g., ease of access to the asset) and threat (e.g., attack type and probability of the attack, or, for hazards, the likelihood of failure), identifies the asset priority. Note that the scale of likelihood can be very dynamic and may change many times a year as far as security threats are concerned.

### Experiences / Lessons learned

The system to identify CI in the United Kingdom is very detailed. It also requires considerable resources to maintain. This approach is most appropriate for nations with a very wide asset base, and/or a high self-perception of being at risk in terms of human threats and natural hazards. As it is (for the most part) completely voluntary, the participation of the relevant CI operators has to be encouraged, rather than mandated. It is not clear what consequences there are if a CI operator refuses co-operation.

## A bottom-up, cross-border approach

PPP ▼

MANDATED

CIP Maturity ▼

### Background

The Canadian-US border is the longest border in the world. In Canada, over 90% of the population lives within 160 km of the US border. This means that regional cross-border infrastructure dependencies exist. Rather than at national level, CI identification occurs in these regions bottom-up with state/provincial/regional government and private asset operators (as well as their associations) playing a key role.

### Description

The need for protection of cross-border infrastructure on which the regional population is critically dependent drives cross-border co-operation initiatives. Legislative aspects may set some preconditions. Agreements at the local/regional community level are primarily made on the basis of mutual infrastructure dependencies. Efforts at the national level seek to support, rather than define, these types of local initiatives.

In some cases, agreements (e.g. Memorandum of Understanding) have been made for ‘common resource sharing’, where a CI is identified as having an important cross-border role (e.g. a hospital).

### Experiences / Lessons learned

A leading example of such wide-ranging regional co-operation is the Pacific North West Economic Region (PNWER), the Washington-British Columbia corridor. Identification of CI and their dependencies has been given special emphasis by PNWER. Regional disaster resilience exercises have helped to identify and manage potential cross-border CI, using dependencies as a key determining factor.

In 2010, the Canada-US Action Plan on Critical Infrastructure Protection<sup>[6]</sup> was announced. This includes a methodology for cross-border CI identification and supports regional and sectoral initiatives in the sharing of information and the development of risk management tools.

### 3.3 References and further reading

- [1] OECD, Protection of 'Critical Infrastructure' and the role of investment policies related to national security, May 2008.  
Online: <http://www.oecd.org/dataoecd/2/41/40700392.pdf>
- [2] European Council, Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Brussels, December 2008.  
Online: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF>
- [3] Luijff, E., Burger, H., Klaver, M., "Critical Infrastructure Protection in The Netherlands: A Quick-scan", In U.E. Gattiker (Ed.), EICAR 2002 Conference Best Paper Proceedings (ISBN: 87-987271-2-5) 19 pages. Copenhagen: EICAR.  
Online: [http://www.alexandrobarrros.com/media/users/1/50369/files/4363/2\\_NetherlandsCidefpaper\\_2003.pdf](http://www.alexandrobarrros.com/media/users/1/50369/files/4363/2_NetherlandsCidefpaper_2003.pdf)
- [4] Luijff, H., Dunn, M., "Working Group 1 report", in CiSP Proceedings on the NATO EAPC/PfP workshop on Cyber Security & Contingency Planning, 25-27 September 2003, Zürich, Switzerland, Center for International Security Policy, Bern, Switzerland, 2004, pp 96-104.
- [5] SAIV 2006, Sectors of Activity of Vital Importance, France, 2006.
- [6] Canada-US Action Plan on Critical Infrastructure Protection, 2010.  
Online: [http://www.dhs.gov/xlibrary/assets/ip\\_canada\\_us\\_action\\_plan.pdf](http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf)
- [7] European Commission, Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 567 Final, Brussels November 2005.



## 4 Dependencies

### 4.1 General description and issues

#### *The need for dependency analysis*

Today, critical societal functions are highly interconnected and mutually dependent in complex ways. This is largely due to a number of social changes, of which technical development has created the most dependencies between different CI. These societal changes mean that we can work more efficiently but also mean that we have become more vulnerable. New dependencies have also been created as an increasing proportion of functions are outsourced to third parties, also outside national borders. New dependencies have been created due to a growing degree of specialisation and the ‘just-in-time’ principle that is increasingly applied to production and transportation. Dependencies should therefore be viewed as a specific type of vulnerability that every CI should be aware of and is able to handle.

Dependencies are therefore important in several aspects of CIP. During the *identification of CI*, dependencies may cause some infrastructures to be identified as critical, not because of the first order effect of disruptions, but based on the cascading effects that their disruption may have on other infrastructures. In the determination of CI in different MS, *cross-border dependencies* are an important factor, since disruptions of an infrastructure in one nation may have serious effects in other nations.

#### EXAMPLE: POSSIBLE EFFECTS OF CROSS-BORDER DEPENDENCIES

Research and policy analysis have put a lot of effort into the study of dependencies. The increased level of interconnectedness of infrastructures led to the concern that small disturbances might easily lead to large scale effects due to cascading effects. The fact that those effects can occur with EU-wide cross-border effects, was shown for example by the blackouts that occurred Europe-wide and even in Morocco on November 4, 2006. Over 15 million people lost their power as well as other CI services for minutes to hours.

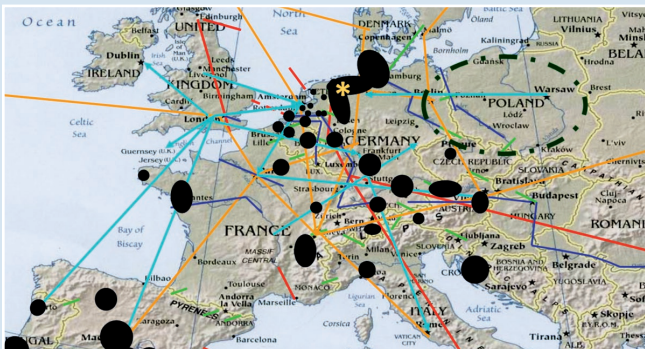


FIGURE 5: Power blackouts hitting 12 European nations including Morocco on November 4, 2006.

Dependency analysis can be used as a foundation for *(business) continuity planning* as it gives a good understanding of the capability – or lack thereof – of the function(s) analysed. In addition, it provides the possibility of conducting *aggregated analysis* of risk, vulnerabilities and capabilities. At the same time, it enables *prioritisation* in the allocation of resources, countermeasures, mitigation strategies and it helps to enhance operational support and decision making. And lastly, it gives incentives for *co-operation* between various players in society (and across borders).

#### EXAMPLE: USE OF DEPENDENCY ANALYSIS IN CRISIS SITUATIONS

Early 2010, the ash cloud emitted by the Icelandic Eyjafjallajökull volcano affected a major part of the European air traffic for weeks. The Swedish emergency management agency MSB used their VisualMSB tool and dependency database to assess the dependency consequences for other infrastructure services. For MSB it was easy to gain insight into the possible effects on all relevant sectors and to contact them.

#### Concept of (inter)dependency

Dependency is the relationship between two products or services in which one product or service is required for the generation of the other product or service. Interdependency is defined as the mutual dependency of products or services. (from<sup>[5]</sup>)

#### Types of (inter)dependencies

Though dependencies vary widely, one way to characterise them is the method by Rinaldi and Peerenboom<sup>[1][2]</sup>:

- Physical dependency - the state of one infrastructure is dependent on the material output(s) of the other infrastructure;
- Cyber dependency - the state of an infrastructure is dependent on information transmitted through the information infrastructure;
- Geographic dependency - an infrastructure is geographically dependent if a local environmental event can create state changes in it;
- Logical dependency - one infrastructure depends on the state of another infrastructure via a mechanism that is neither a physical nor a cyber dependency.

Physical and cyber infrastructure (inter)dependencies transcend individual infrastructure sectors (by definition) and generally transcend individual public and private-sector companies. They vary significantly in terms of scale and complexity (local, regional, national, international linkages). Failures affecting (inter)dependent infrastructures can be described in terms of three general categories <sup>[1][2]</sup>:

- Cascading failure (disruption in one infrastructure causes disruption in a second infrastructure).
- Escalating failure (disruption in one infrastructure exacerbates an independent disruption in a second infrastructure).
- Common cause failure (disruption of two or more infrastructures at the same time as a result of a common cause, e.g. by an earthquake or flooding)<sup>[1]</sup>.

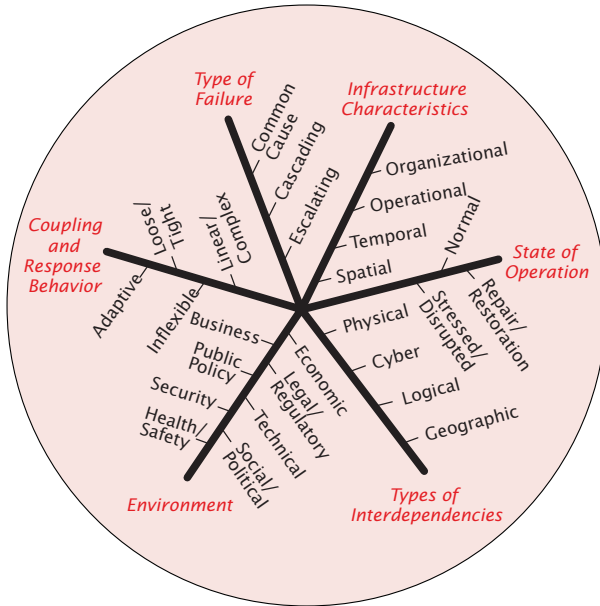


FIGURE 6: Dimensions within the Dependency Concept, Rinaldi (2001)<sup>[1]</sup>

### *Time effects and recovery time*

The degree to which the infrastructures are coupled influences operational characteristics and determines for example the time frame for responsive actions<sup>[1]</sup>. When infrastructures are tightly coupled, disturbances tend to spread more rapidly. The degree of coupling (tightness or looseness) and other characteristics such as buffers and the requisite recovery time determine whether infrastructures are adaptive or inflexible when perturbed or stressed. Tight coupling is characterised by time-dependent processes that have little slack. Loose coupling means that infrastructures are relatively independent of each other and the processes are not nearly as time dependent as in a tightly coupled system.

### *Mode of operation and dependencies*

One complicating factor when identifying dependencies, is that these can vary with the mode of operation of CI. An example of shifting dependencies would be a hospital: when in normal operation this does not require diesel fuel for its operation. However, when electricity fails, the emergency power generator does require timely refuelling. Four states of operation can be distinguished<sup>[6]</sup>:

- The Normal state, in which the CI operates under normal conditions.
- Stressed state: This is the state in which special measures are required to keep CI operations under control, e.g. due to maintenance or non-critical failure.
- Crisis state: This is the state in which CI operations are out of control.
- Recovery state: This is the state in which CI operations are under control but have not (yet) been restored to normal conditions.

In order to acquire a complete overview of dependencies between CI, all four states should be considered.

#### *Methods for mapping CI dependencies*

Approaches to mapping CI dependencies vary across nations. An example of a pragmatic approach is to encourage *intersectoral networking*. By bringing relevant partners together, raising awareness on (mutual) dependencies can be created. This is most often done based on risk scenarios.

Another approach is to *conduct dependency analyses* based on (mathematical) modelling. This can vary from conducting analyses for individual functions up to analyses for the cross-sector societal level. Within these analyses direct but as well as indirect impacts are taken into account. Most often, special attention is given to the verification of anticipated dependencies (electricity, electronic communication and transport) as they represent a significant vulnerability.

Good examples of qualitative and quantitative modelling can be found in Sweden and Finland. Modelling helps to obtain insight into possible cascading effects. Detailed modelling gives good insight into complex dependencies and relationships. However, the more detailed the modelling, the more information is needed. Operators might not always want to share this information. Another example of detailed modelling can be found in Australia. The Australian Critical Infrastructure Protection Modelling and Analysis Program (CIPMA) is building up a catalogue of infrastructure sector simulation models, databases, geospatial information systems (GIS) and economic models which in combination are used for CI dependency analysis.



### EXAMPLE: ANALYSIS OF CI DEPENDENCIES AND INCIDENTS

In order to get more of a handle on dependencies and the risk of cascading effects, an analysis has been made on data collected on large-scale CI disruption incidents. The analysis of this data showed that energy and ICT are the sectors with most disruptions and cascading effects.<sup>[6]</sup>

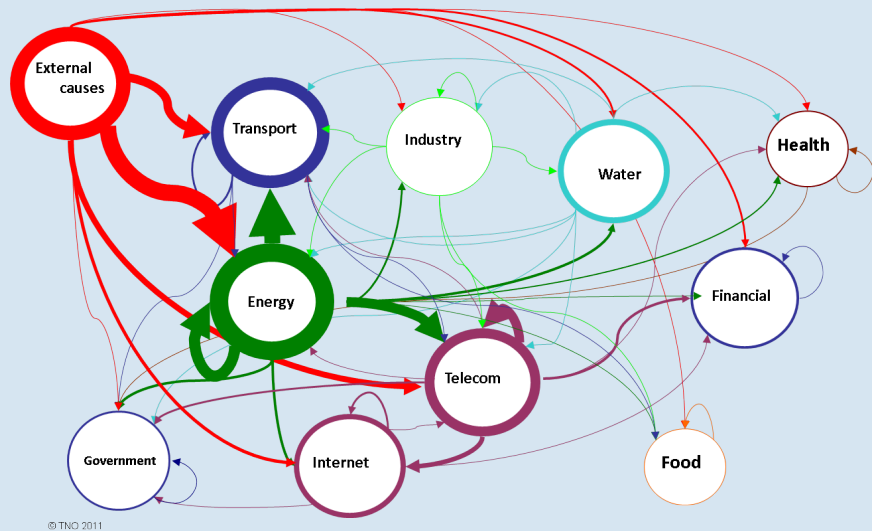


FIGURE 7: CI outage relations and cascading statistics in the EU (TNO, 2003-2011)

## 4.2 Good practices

The following good practices for dependency analysis have been highlighted:

- Organising intersectoral workshops (example: the Netherlands) is a method which does not require detailed modelling knowledge;
- Qualitative analysis (example: Sweden) requires some knowledge on qualitative modelling approaches;
- Quantitative analysis (example: Finland) requires specific and detailed modelling knowledge.

## Intersectoral workshops

PPP ▼

MANDATED

CIP MATURITY

### Background

A good example of the application of intersectoral workshops can be found in the Netherlands. Within the Dutch CIP programme an analysis was made of intersectoral dependencies. This enabled the CI sectors to gain insight into the consequences of (mutual) dependencies as well as into the effect of measures taken. The parties involved aimed to identify and clarify the technical and organisational networks in which critical sectors operate and enable these public and private parties to prepare together for possible threats to their business continuity.

### Description

The subject of dependencies within the CIP programme has been dealt with by the Dutch government from a pragmatic point of view. In the Dutch approach, no specific models were used for conducting dependency analyses. The main focus is on knowledge exchange. The idea here is that through networking and sharing expertise, sectors themselves become more aware of their dependencies and how to reduce their vulnerabilities. The parties involved will be more acquainted with each other and with each other's possibilities so when problems arise they will be better able to work together.

CI sectors were brought together in workshops that were based on two scenarios from the Dutch National Risk Assessment (pandemic flu and flooding), to discuss:

- Effects of CI disruptions, e.g. direct/indirect, supply chain, access/scarcity/integrity, time period of disruption, sector characteristic, and human factors;
- Dependencies, redundancies and recovery;
- Measures to reduce vulnerabilities.

### Experiences / Lessons learned

The first lesson is that it is necessary to prioritise in order to deal with the huge variety of CI products and services, as well as the enormous amount of related parties and relations. Certain CI sectors deliver the preconditions for other CI sectors to function. When one of these CI sectors (e.g. electricity, transport and ICT) is not functioning, most other CI sectors will be affected as well.

A second lesson that became clear from the workshops is that possible measures are mostly not assessed in terms of their reliability. Although dependencies generally are taken into account, most businesses do not know whether the measures taken will be sufficient during a crisis. Often the assumption is made that supporting infrastructures will continue to provide an uninterrupted supply of their goods and services, regardless of any disturbance in the supported infrastructure. To enhance insight into what one critical sector can expect from other critical sectors or partners, two points of particular interest were mentioned: (1) the relationship between CI sectors and (2) expectations between CI sectors and government services.

The first relation (between CI sectors) is considered by parties to be an important point of concern. Most CI sectors have insufficient insight into possible consequences of the breakdown of the delivery of their products or services on other sectors. Neither do they have sufficient insight into the consequences of fallout of others in relation to their own business continuity, especially during a crisis. How possible cascading effects would look like is therefore not clear.

The second relation (between CI sectors and government services) yielded a degree of uncertainty regarding responsibilities. CI sectors do not know what to expect from the government. Companies expect that the government will take action during a crisis, but do not know what the government will do, which priorities are made, and whether they will be informed and when. How government and business activities influence each other is something that needs special attention. Making clear the responsibilities and expectations of different parties is of vital importance.

## Qualitative analysis

PPP ▼

MANDATED

CIP MATURITY ▼

### Background

The Swedish Emergency Management Agency identified and analysed critical dependencies as a government assignment from 2006 to 2008. In the dependency analysis, critical societal functions are considered instead of infrastructures, as the latter only support certain functions in society. The results of the dependency analysis are used for decisions regarding the prioritisation of measures, resource distribution and the focus of studies and research.

### Description

The method consists of three stages: selecting and describing critical societal functions, identifying and evaluating the individual function's dependencies, and ultimately analysing the dependencies between functions at an aggregate level (see Figure 8).

In the first stage, a selection is made of the critical societal functions that are to be examined. The functions selected are then also described based on what they should supply, to what extent, and to whom.

In the second stage, each critical societal function's external dependencies are identified and evaluated. To facilitate this step a tool, called the 'Dependency Wheel', is used. This interactive tool describes what a critical societal function needs in order to function as described in the first stage of the method.

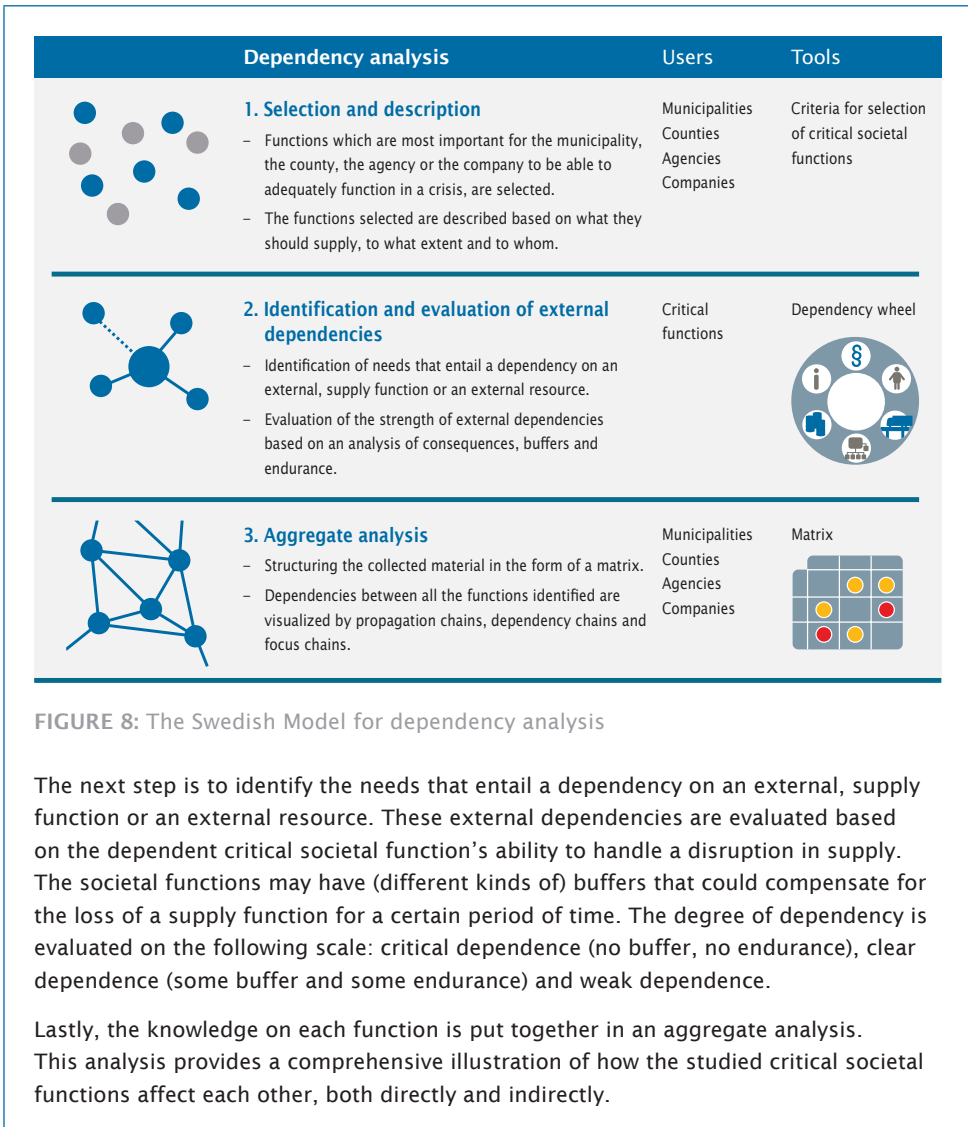


FIGURE 8: The Swedish Model for dependency analysis

The next step is to identify the needs that entail a dependency on an external, supply function or an external resource. These external dependencies are evaluated based on the dependent critical societal function’s ability to handle a disruption in supply. The societal functions may have (different kinds of) buffers that could compensate for the loss of a supply function for a certain period of time. The degree of dependency is evaluated on the following scale: critical dependence (no buffer, no endurance), clear dependence (some buffer and some endurance) and weak dependence.

Lastly, the knowledge on each function is put together in an aggregate analysis. This analysis provides a comprehensive illustration of how the studied critical societal functions affect each other, both directly and indirectly.

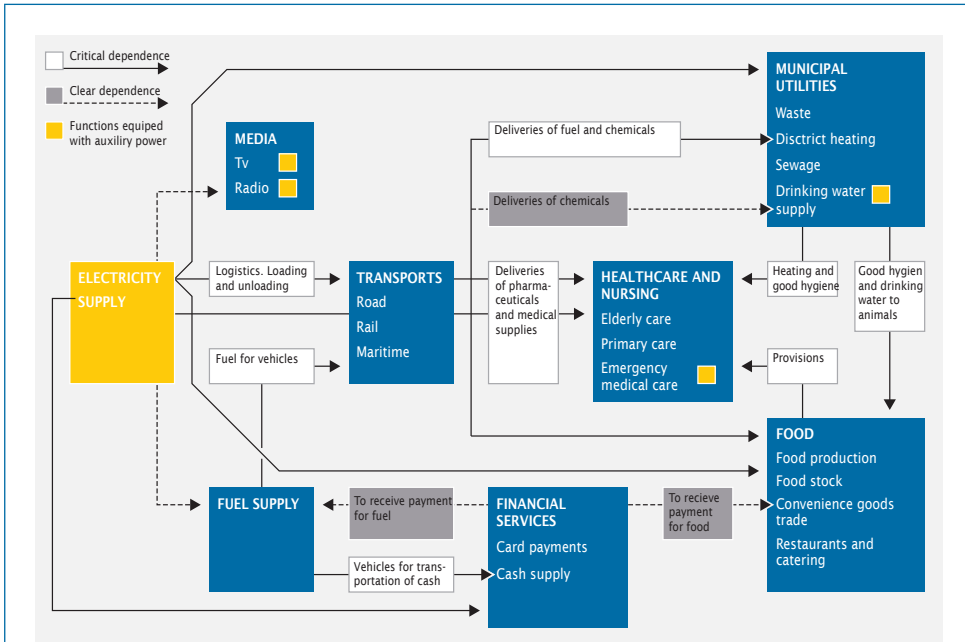


FIGURE 9: Focus chain: are functions with auxiliary power secure?

### Experiences / Lessons learned

- In order to analyse how a function is affected during a crisis, it is not enough to consider the direct functions. It is also necessary to investigate the indirect consequences: how can functions be affected by their dependencies on others' dependencies? This provides a more realistic picture of, for example, how a disruption in electronic communications affects a function.
- Many functions have a distinct dependence on qualified personnel that can take care of functions and repairs. They comprise a strategic resource that is 'under-dimensioned' relative to the needs that may arise in a crisis situation.
- Several of the sectors studied show clear intra-sector dependencies. Examples of such sectors include health care and nursing, international protection and security and the financial sector. There is a clear risk that the strain within the sector would shift to other functions in a crisis, which would then have problems fulfilling their function.
- End users are affected (more) often as private persons are often affected in a crisis even if critical societal functions manage to maintain their capacity. For example, banking consumers cannot use internet banking during a power outage because there is no power for their router even though electronic communications and financial services may have succeeded in withstanding the disruption of the power supply.
- It turned out that the method is not only useful for the purpose of preparation, but also during a crisis (see example on page 28).

## Quantitative analysis

PPP ▼

MANDATED

CIP MATURITY ▼

### Background

CIP is a well established policy domain in Finland and is given high priority. Therefore, the Finnish government and public and private partners have a lot of experience in developing both policies and useful instruments to protect CI. In 2008, a government decision on the targets pertaining to security of supply (21.8.2008/539) was published which states that “nationally networked co-operation, as well as understanding of international dependencies and the development of the means of preparation based on them, must be invested to a greater extent in security of supply work”.

### Description

To map CI dependencies, a linear mathematical model is used to rank the risk involved in different societal functions. It ranks these functions according to the effects and risk pertinent to the dependencies. The calculation of relative effects and risk caused by failures is based on expert assessments on three factors pertinent to each infrastructure, basic service, and outside threat:

1. Dependency,
2. Mean time between failures,
3. Duration of failure.

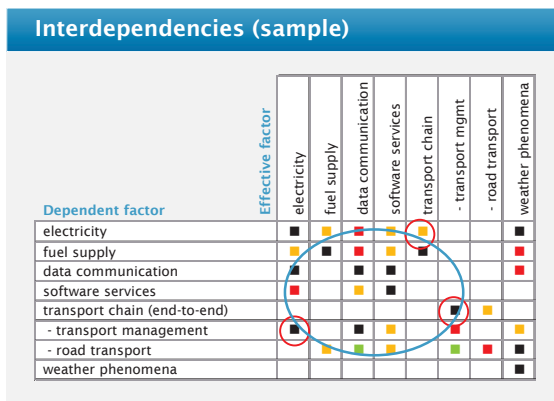


FIGURE 10: Sample of the 60\*60 matrix of dependencies of critical functions and threats in Finland

The method helps to understand the dependency structure. The results of the first analysis showed different areas of ICT to be most critical. Subsequently, the method was used to analyse ICT more in detail by breaking it down to 66 sub-functions.

This analysis resulted in a set of agreed recommendations for subcontracting and business partnerships in order to minimise service disruptions.

#### Experiences / Lessons learned

- The identification and strength of dependencies is the most important step in using the model. A separate group of experts is needed to estimate each horizontal line of cells in the dependency matrix. This is fairly easy for them, because they are the best people to know on which functions their own area of expertise depends and how critically. Furthermore, the rough scale, only four steps, facilitates the assessment. The linear model calculates the basic ranking. The model that was used in ranking the CI and critical production in 2005 had 60 items (functions and threats) to be considered. Therefore, there were  $60 * 60 = 3,600$  dependency estimates to think of.
- The methodology requires extensive and quantifiable reliable input from various public and private partners in order to be effective.
- The method is quite time consuming: before starting one should carefully assess costs vs. benefits.

### 4.3 References and further reading

- [1] Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly , Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, December 2001
- [2] James P. Peerenboom and Ronald E. Fisher, Analyzing Cross-Sector Interdependencies, in: Proceedings of the 40th Hawaii International Conference on System Sciences; 2007.
- [3] H. Sivinen, Assessing security of supply – three methods in Finland, in: ‘Food chain security’, Springer, ISBN: 978-90-481-9557-2.  
Online: [http://www.nesa.fi/documents/3/Sivonen\\_Assessing\\_security.pdf](http://www.nesa.fi/documents/3/Sivonen_Assessing_security.pdf)
- [4] Swedish Civil Contingencies Agency, “if one goes down – all goes down?” A final report from SEMA’s assignment on Critical Societal Dependencies.  
Online: [http://www.msb.se/Upload/Produkter\\_tjanster/Publikationer/MSB/0001\\_09\\_Bilaga\\_Faller\\_en\\_ENG\\_sammanfattning.pdf](http://www.msb.se/Upload/Produkter_tjanster/Publikationer/MSB/0001_09_Bilaga_Faller_en_ENG_sammanfattning.pdf)
- [5] ACIP consortium, Analysis and Assessment for Critical Infrastructure Protection (ACIP) final report, EU/IST, Brussels, Belgium, 2003.
- [6] Nieuwenhuijs, A.H., Luijff, H.A.M., Klaver M.H.A., “Modeling Critical Infrastructure Dependencies”, in: IFIP International Federation for Information Processing, Volume 290, Critical Infrastructure Protection II, eds. P. Mauricio and S. Shenoi, (Boston: Springer), October 2008, pp. 205-214, ISBN 978-0-387-88522-3.



## 5 Public-Private Partnerships

### 5.1 General description and issues

#### *The need for PPPs for CIP*

In many nations, more than 80% of the CI is owned and operated by private companies. In order to achieve community resilience it is important that public and private CI owners work together in a co-ordinated way in protection of the CI, before, during, and after a disaster. So, with the current majority of CI in private hands and the responsibility for civil protection and emergency preparedness in public hands, PPPs are essential for meeting contemporary threats.

Although multiple definitions of PPP are in use around the world, we will use the term to mean collaboration between a government agency and a private entity with the purpose of ensuring the continuous functioning of the CI services.

Traditionally, the label PPP is used in the context of *contractual* relationships between governments and the private sector. One example of a traditional infrastructure PPP project is the Channel Tunnel project, which involves a mix of public sector support and private sector funding. This kind of PPP means that the (parts of) financing, management, and risk of certain infrastructure projects would be transferred to the private sector.

However, it should be realised that PPPs in CIP can be much more than a delegation of public tasks to private players.<sup>[1]</sup> A broader concept of collaboration embraces the pooling of resources, mutual support, and joint decision-making. They not only involve contracting-out schemes but also inter-organisational networks of collaboration. The objective is to grant the continuity of services or infrastructures that have been considered critical from a national and local perspective. National and local first-responders, emergency managers and others frequently interact via established networks with CI owners and operators to plan for and respond to natural and man-made hazards. This is the core principle that distinguishes ordinary contracting out PPP schemes from PPP in CIP.

PPP are found in many different forms, varying from very informal types of cooperation to more formal partnerships. The degree of formality is often associated with the amount of control the governmental bodies aim to exert. This spectrum is illustrated in Figure 10.

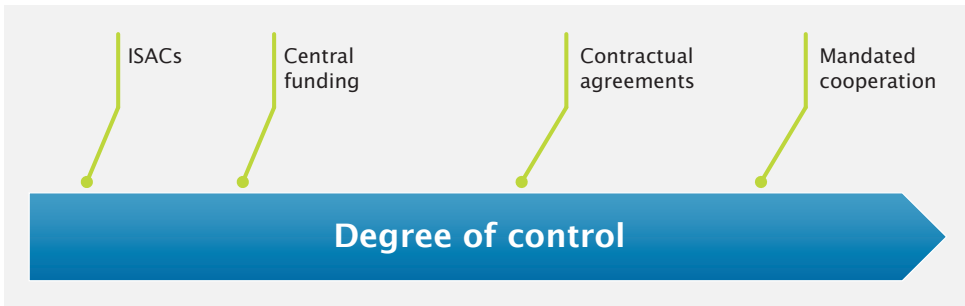


FIGURE 11: Degree of control in PPP

*The use of PPP in CIP*

Some of the benefits PPP can bring to CIP are:

- a) Stronger PPP will positively influence the capability of CI operators participating to manage consequences of disaster.
- b) Improvements in the resilience of CI will positively improve supply chain resilience.
- c) A higher capacity to maintain business continuity, resulting also in higher levels of service and trust between service providers and clients.
- d) A higher level of understanding on how dependencies among sectors affect responses to emergencies leads to better levels of preparation and response to disruptions, and shortens the duration till full recovery.
- e) Co-operation can lead to reduced risk for all parties involved.
- f) Co-operation can lead to lower costs for all parties involved.

The National Incident Management System (NIMS) in the USA indicates that community resilience is influenced by the relationships government agencies develop with private sector partners and the resilience of relevant supply chains and CI <sup>[3]</sup>:



FIGURE 12: Chain of CIP strengthening by PPP<sup>[2]</sup>

As Figure 12 indicates, one of the main issues of PPP is to find and embrace the public-private interfaces that can improve the ability of a community to manage the response and recovery phases of disaster response.

### *Critical factors for success*

While a format for success in establishing a PPP is non-existent, there are certain factors that are of the utmost importance for a successful PPP. These factors are:

- Trust: as PPP in CIP often concern touchy subjects (commercially, security wise or in terms of established structures), it is essential to create an atmosphere of trust in which both parties show awareness of each other's need for discretion and consistently act accordingly.
- Respect: both parties have to recognise and respect the added value the other party brings to the collaboration. This can be reached by 'selling' your own added value (in your partner's terminology) while actively looking for the added value of your partners.
- Transparency: the openness of procurement policies and practices is an important factor. The general principles of contracts, procurements, etcetera, should be made public.
- Clear legislative and regulatory framework: clear framework of legislation and regulation sets out the PPP framework. It is recommendable to have fewer and simpler laws (avoid duplication).
- Neutrality: it is necessary to have clear, specific and predictable rules that do not provide scope for discretion and prevent any conflict of interest.
- Common interest: the partnership between the public and private CI sectors should be based on a common interest in order to establish a basis for co-operation.
- Awareness of each other's possibilities and restrictions: this prevents conflict through misjudgement of the cause of a negative response and allows for an optimum return on the efforts of the alliance. This implies that both parties should know each other's business. A good way to attain this is to have worked together for a longer period of time, preferably years.
- Realistic expectations: both parties have to take into consideration affordability of resources, development budget, etcetera, to be able to form realistic expectations of the PPP.

## 5.2 Good practices

Many forms of PPP are possible. Presenting a complete list would be impossible, therefore we will try to outline this spectrum by examples that vary in the degree of formality and control involved.

- An example of a more informal kind of PPP would be an Information sharing and Analysis Centre (ISAC) where the government facilitates the information sharing between concerned parties on a specific (CIP) subject.  
The good practice "CIP board at the strategic level" gives an example of a public-private information sharing at the strategic level (the Netherlands);
- A more formalised PPP can be established by making centralised government support (funding or free expertise and/or manpower) available for CIP initiatives. This form of PPP

is presented in the good practices 'Providing common funds for CIP measures' and 'Exchange of expert knowledge';

- Even more formal would be the inclusion of CIP conditions in (regular) contracts established between private partners and public authorities;
- The most formal example would be to introduce CIP obligations in legal acts. More details on this form of PPP can be found in the good practice 'Compelling cooperation'.

## CIP board at the strategic level

PPP ▼

▼ MANDATED

CIP MAJORITY

### Background

The basis of public-private collaboration is the enhancement of mutual understanding, as supported by information sharing. Information sharing communities are established to stimulate the flow of information concerning threats and vulnerabilities, undesirable effects, possible measures and policies, etcetera among CI operators (in or between sectors) and sometimes also with public organisations (see Section 5).

Some of the most practical and useful outcomes of such experience are probably the information sharing at the strategic level (e.g. the SOVI in the Netherlands) and information sharing communities at the operational and tactical level, such as ISACs as discussed in more detail in Section 5.

### Description

The SOVI (strategic consultative body for CI) is a public/private consultation body that was established in April 2006 by the Dutch Ministry of the Interior and Kingdom Relations and the Confederation of Netherlands Industry and Employers (VNO-NCW). The objective of the SOVI is establishing a structural consultation platform between government and businesses within the Dutch CIP framework.

The SOVI takes the form of a regular series of meetings, where a permanent representative of each of the CI sectors and VNO-NCW is invited to discuss issues concerning the protection of their own CI sector, and cross-sector issues. Participation in the SOVI is on a voluntary basis, but requires a commitment to participate. The sessions are facilitated and chaired by a permanent representative of the government. The agenda is determined by the CI sector representatives themselves. This ensures that only issues that are of concern to the CI sector representatives are put on the agenda and that even issues that oppose government interests can be put on the agenda.

### Experiences / Lessons learned

The SOVI meetings have brought a number of concrete results:

- Enhanced understanding and trust between the CI sectors.

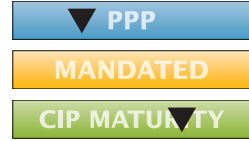
*The opportunity for different CI sectors to meet and share cross-sector and CIP relevant information has led to better insight into each other's possibilities and limitations.*

- A better understanding on the part of the government of the issues in the CI sectors.
- A direct channel running from the CI sector to the government.

*This was instrumental in creating understanding of existing and intended CIP policies with the CI sectors.*

- A common frame of reference.  
*By sharing knowledge and experiences, a common frame of reference of CIP related activities within and outside the various CI sectors has been created and maintained.*
- A better understanding of dependencies.  
*By sharing vulnerability information, shared bottlenecks are considered and made debatable. Exchange of such information will also help to give each other insight into each other's dependencies. It provides insight into and conditions under which such dependencies form a risk.*
- Fostering a culture of direct accountability.  
*In the meetings, parties can make each other directly accountable for sticking to agreements and achieved goals.*
- A better understanding of one's own role in CIP.  
*By discussing the interests of other sectors for CIP, the need for CIP measures in one's own CI sector is made very clear.*
- Improved preparedness.  
*Access to a trusted forum to share problems and solutions, as well as raising your awareness of CI threats. In a number of cases this has lead to concrete bilateral agreements mitigating vulnerabilities.*

## Provide common funds for CIP measures



### Background

Providing common funds for CIP measures is an important and widely discussed topic in PPP. In most nations, the CI owners must guarantee the continuity of critical services at their own expense. Finland is one example where some measures for CIP are also covered by common funds. This kind of financial tool is managed by a co-operative network: the National Emergency Supply Agency (NESA). The participants are various sectors of the public administration and business, as well as branch organisations. The network of committees consists of more than one thousand leading experts. The partnership organisation exchanges information within sectors and across sectors, follows the business environment and threats to it, supports individual business continuity management, arranges exercises, and carries out surveys, research and development projects with the help of consultants and academia.

### Description

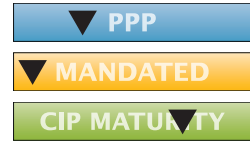
The expenses resulting from maintaining security of supply are financed centrally by the security of supply fund which is external to the state budget and which is managed by the NESA. The PPP members are not paid for their time, but NESA finances exercise arrangements and the permanent secretaries of the pools.

Usually the market mechanism provides sufficient security of supply. However, in some cases special measures are needed. The NESA Fund finances stockpiles for oil and medical products. In addition, selected redundancy and protection measures for the critical information infrastructure are financed by the NESA fund. A security of supply fee is levied in conjunction with energy taxes. Its amount is approximately half a per cent of retail prices.

### Experiences / Lessons learned

- The markets usually provide security of supply, but special arrangements (common funds) certainly help to provide the operators with protection measures for CI and thus raise the risk thresholds.
- NESA unifies various public sectors of administration and business – they can jointly decide on the need for CIP funding.

## Attaining voluntary co-operation through providing expertise



### Background

An effective way of realising many of the critical factors for establishing successful PPP, can be attained by the government providing expert knowledge to private partners. The added value of this information for the private partners is rooted in the fact that the government independently visits many companies, and reaches an all-encompassing view of the CIP status of a sector or multiple sectors. When this information is combined with threat information from intelligence, this can be translated into operational information that can be acted on. In this way the government can become a valued partner for CI operators.

### Description

Many nations have set up governmental non-profit bodies in order to provide integrated security advice (combining for instance information about threats and risk, personnel and physical) to the businesses and organisations that make up the national infrastructure. Probably one of the best examples is the Centre for the Protection of National Infrastructure (CPNI) in the UK which is an interdepartmental organisation with resources from industry, academia, and a number of government departments and agencies. CPNI deals with delivering advice for businesses and organisations thus helping to reduce the vulnerability of the national infrastructure to terrorism and other threats. Support to companies also encompasses the development and dissemination of relevant standards.

### Experiences / Lessons learned

- Greater level of awareness and involvement of the industry for CIP.
- By means of personal visits, government agencies gain insight into strategic and daily tactical and operational security aspects of CI operations.
- Government may promote conversion of CIP lessons learned by CI operators are converted into national (de facto) standards.
- By means of personal contact with CI operators, government agencies are able to more easily convey the national interest aspects of CIP.
- Fusing information from multiple CI operators and combining that with current threat information from open and classified sources gives government agencies quid-pro-quo information that is valued by the CI operators.
- Building trust with CI operators at the tactical/operational level builds a foundation for collaboration at the strategic level.



## Compelling co-operation

PPP ▼

MANDATED ▼

CIP MATURITY ▼

### Background

It is understood by some nations that the necessary preconditions for securing their CI and fostering PPP is a clear framework provided by regulations and legislation. Good examples can be found in France and Estonia, where certain and quite far-reaching provisions about CIP and PPP have been introduced in legislation. The Example of France is discussed in more detail in Section 7 “Risk Management”.

### Description

In Estonia, the Emergency Act provides the legal bases for crisis management as well as for CIP. The Minister of the Interior has established by regulation the general guidelines for risk assessment and continuity plan according to which CI operators and owners have to prepare the aforementioned plans every two years and submit the information (including dependencies and proposals to improve the system) to the state agency organising the respective critical service.

The state agencies responsible have to perform the analysis at a higher level to derive at an overview of the CIP status across sectors. Failing to perform the obligations leads to legal sanctions for the CI service providers. The integral overview of the continuity of CI services and proposals to improve the system is presented regularly in the government crisis management committee presided over by the Minister of the Interior. To those ends a solid co-operation, interaction, and close contact between the state agencies and private owners is required – in concordance with the national organisational structure of the Estonian government.

One form of such co-operation can be found in for example the framework of Estonian local and regional crisis management committees. In close co-operation with the local authorities and emergency managers regular exercises are organised to test the continuity of CI services. It is important to mention that CIP operators have to mitigate the risk and guarantee the continuity of critical services at their own expense, no additional funding is set up. The obligation for the state is also to set up the minimum standards for providing the critical service. The requirements of the Emergency Act are also well in line with the EPCIP directive.

### Experiences / Lessons learned

- CI owners are more aware of threats and risk because they are obliged to regularly analyse the continuity of critical services.
- Better understanding of dependencies and knowing and engaging with their safety partners (public and private).

- Better awareness at State level about the problems and deficiencies – CI owners and operators are obliged to exchange information with the relevant government authorities.
- The need to set up clear rules on how to handle the sensible information in order not to disturb the market situation.
- The need to provide CI operators with the minimum requirements/standards on which level the continuity of critical service must be guaranteed.
- The need for the state to set up and regularly update the list of sector specific threats to be submitted to critical service providers.

### 5.3 References and further reading

Developments can be seen in different kinds of national CIP strategies, also involving the principles of PPP.<sup>[3][4]</sup> Some nations have introduced relevant provisions and starting points for PPPs in legal acts.<sup>[5]</sup> Some good examples of national PPP strategies can be found in <sup>[4][7][8]</sup> <sup>[9][10][11]</sup> or, at a European level, <sup>[12]</sup>.

- [1] CRN Focal Report 2. Critical Infrastructure Protection, Centre for Security Studies (CSS), ETH Zurich, 2009.  
Online: [http://kms2.isn.ethz.ch/serviceengine/Files/CRN/105884/ipublicationdocument\\_singledocument/E1E2BF81-36FD-4407-95B3-50CF2655BEEB/en/CRN-Report-Focal-Report-2-CIP.pdf](http://kms2.isn.ethz.ch/serviceengine/Files/CRN/105884/ipublicationdocument_singledocument/E1E2BF81-36FD-4407-95B3-50CF2655BEEB/en/CRN-Report-Focal-Report-2-CIP.pdf)
- [2] Stewart, G., Kolluru, R. and Smith, M. (2009) Leveraging public-private partnerships to improve community resilience in times of disaster. *International Journal of Physical Distribution & Logistics Management*, 39 (5), 343-364.
- [3] “The Strategy for Securing the Functions Vital to Society”, Government Resolution, Finland, 2006.  
Online: [http://www.defmin.fi/files/858/06\\_12\\_12\\_YETTS\\_\\_in\\_english.pdf](http://www.defmin.fi/files/858/06_12_12_YETTS__in_english.pdf)
- [4] National Infrastructure Protection Plan, 2009. USA.  
Online: [http://www.dhs.gov/xlibrary/assets/NIPP\\_Plan.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf)
- [5] Emergency Act, 15 June 2009, Estonia.  
Online: <https://www.riigiteataja.ee/akt/13201475> (in Estonian language)
- [6] The National Plan for the Protection of Information Infrastructures, 2005 (NPSI) Germany.  
Online: [http://www.en.bmi.bund.de/cln\\_028/nn\\_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National\\_\\_Plan\\_\\_for\\_\\_Information\\_\\_Infrastructure\\_\\_Protection,templated=raw,property=publicationFile.pdf/National\\_Plan\\_for\\_Information\\_Infrastructure\\_Protection.pdf](http://www.en.bmi.bund.de/cln_028/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National__Plan__for__Information__Infrastructure__Protection,templated=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.pdf)

- [7] The Hungary Information Society Strategy, 2006. Hungary.  
Online: [http://plone.itc.nl/agile\\_old/Conference/2006-Visegrad/papers/detrekoi\\_agile\\_welcome.pdf](http://plone.itc.nl/agile_old/Conference/2006-Visegrad/papers/detrekoi_agile_welcome.pdf)
- [8] National Guidelines to Strengthen Information Security, 2007-2010, Norway.  
Online: <http://www.oecd.org/dataoecd/56/40/41671072.pdf>
- [9] The National Strategy and Action Plan for Critical Infrastructure, Canada, 2009.  
Online: [http://www.dhs.gov/xlibrary/assets/ip\\_canada\\_us\\_action\\_plan.pdf](http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf)
- [10] Sector Resilience Plan for Critical Infrastructure 2010, UK.  
Online: <http://www.icpem.net/LinkClick.aspx?fileticket=r-0z5QGqqW4%3D&tabid=107&mid=588>
- [11] Strategy for Securing the Functions Vital to Society 2006, Finland.  
Online: <http://www.finlandnato.org/public/download.aspx?ID=31784&GUID=%7B7644AF36-AE50-41EF-ADDA-778E0080B49E%7D>
- [12] European Council, Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Brussels, December 2008.  
Online: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF>



## 6 Information sharing

### 6.1 General description and issues

#### *The need for information sharing*

The interconnectedness of large and complex CI requires collaboration across organisational boundaries in order to improve the protection of these networked CI. Information sharing is one of the key elements in providing this collaboration.

Information sharing between both public and private organisations provides a basis for common understanding of threats, risk, dependencies, and shared knowledge on possible countermeasures. It allows for stronger protection of CI, both at the national and international level.

Information sharing will contribute to a common understanding of threats, risk factors and measures. It improves the quality of *risk management* across the set of participating CI, and may thus raise their level of protection. The CIP policymaker will have a better understanding of the level of protection and possible contingencies. This common understanding will prove to be essential in case major incidents occur and *crisis management* is required.

Public-private information sharing platforms have the following benefits:

- They can raise awareness of the need to perform CIP and related topics such as business continuity management and risk management;
- They can improve the level of education/knowledge about these subjects;
- By sharing experiences, they can increase the skills of community members;
- By following the topics discussed within the communities, they can serve as a channel to keep the government involved in the concerns of the community;
- By using the private community, the government can directly address all or part of the community with specific information. If the community uses a secure communication channel, this can even include restricted information.

#### *What information to share*

In support of CIP, all parties need to have a basic understanding of the protection level of their respective CI and of possible (often imminent) threats and risk factors. For that reason, parties may share information on the following topics:

- *Threats, vulnerabilities, and risk factors*: sharing this type information allows for a better understanding of risk and threats throughout the technical and organisational network of CI. This may include information on new threats or types of attack disseminated by intelligence and security services, police services, and private entities.
- *Measures and good practices*: sharing information on possible countermeasures and CIP good practices strengthens the level of protection of CI. This information may be both of a technical and organisational nature.
- *Incident data*: in some nations, CI sector enterprises, government bodies, and intelligence and police services share information on actual incidents that have occurred. This type of information is only shared within a secure and, above all, trusted environment. Sharing

incident data allows lessons to be derived from earlier incidents which may prevent these incidents from happening again elsewhere in the same or other CI, and which may enhance the effectiveness and efficiency of incident response and recovery actions.

- *Weak signals*: CI operators may have noticed some vague abnormality which on its own is too weak to raise an alarm. By sharing such information, a pattern of reconnaissance activities may be unearthed.

#### *Which organisations to involve*

Information sharing can take place at several levels:

- Between CI organisations within a critical sector;
- Between CI organisations of different sectors;
- Between government organisations and CI operators of a single sector;
- Between government organisations and CI operators from all CI sectors;
- Between CI provisioning and support organisations (e.g. manufacturers, system integrators, resellers) and CI operators from all CI sectors.

#### *Main success factors*

Experiences of successful information sharing show that trust is the main key success factor. Experience has shown that trust is best built-up in small sized face-to-face meetings.

In general, there are some basic dos and don'ts. As a general rule, information sharing can be best initiated at a level that is not too detailed. It is not always necessary to share information that is too specific, for instance knowledge on critical objects and their location, or specific information on vulnerabilities or incidents. Several successful information exchanges stress that starting small will help to establish the required level of trust.

For establishing *trust*, there should be continuity in the people attending the information exchange meetings. The participants should be appointed at a personal level with enough mandate and responsibility in their own environment. Generally, no substitutes are allowed.

*Information sharing meetings* focus on the exchange of information: all organisations involved should (in principle) contribute information.

The information provider shall ensure that the information provided is of the right level of content and background. Based upon the information, the recipients of the information should be able to take appropriate actions in their respective organisations or be alerted about the new threat. Above all, the information provider remains the owner of the shared information and its sensitivity classification.

Most examples of successful information sharing are on a voluntary basis, built on trust.

However, there are also some mandatory examples, in which information on risk assessments and incidents has to be shared, e.g. the reporting on large disturbances to public communications networks according to article 13a of the EU telecommunications package<sup>[10]</sup>. In the mandated approach it is often hard to guarantee quality of the exchanged information. Even mandated approaches therefore emphasise that a key to the success of their scheme is still to build trust and a spirit of voluntary co-operation<sup>[5]</sup>.

### *How to organise information sharing in a secure and trusted way*

One of the key success factors for information sharing is to use a set of clear rules to ensure the confidentiality of the information exchanged. One of the most widely used protocols to protect the *confidentiality* of shared information is the Traffic Light Protocol or TLP (see good practice Traffic Light Protocol). Another protocol that can be used to protect the *anonymity* of shared sensitive information is the Chatham House Rule. Under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.<sup>[9]</sup>

Currently, a new ISO industrial standard for information sharing is being developed in terms of security techniques for intersectoral and inter-organisational communications.<sup>[6]</sup>

Some organisations also use electronic tools for secure information sharing, e.g. by using a protected extranet for (for example) minutes of the meetings, and references to interesting documents.

Sharing of national classified information is based upon formal regulations, accreditations, and clearances (vetting of staff).

### *Cross-border information sharing*

International communities may share information based upon trust and a protocol, e.g. the traffic light protocol<sup>[8]</sup> (TLP) or the Chatham House Rule<sup>[9]</sup>.

Sharing of national (and EU) classified information across national borders is based upon formal regulations, accreditations, and clearances (vetting of staff), and formal international agreements on equivalency schemes. Due to the formalities and sets of regulations involved, it is often less easy to share such information with private parties.

In an international environment, it also proves to be more difficult to build the trust needed for effective information sharing. Again, there are some examples of cross-border information sharing in relatively small communities on a regional basis (e.g. the Visegrad nations) or on information sharing for a specific topic (e.g. the European information exchange on security for SCADA and control systems EuroSCSIE).

### *CIIP and information sharing*

Many of the examples of information sharing include information exchanges on ICT related vulnerabilities and threats (e.g. CPNI.nl in the Netherlands).

Especially the community of Computer Security Incident Response Teams (CSIRTs) is well organised and interconnected and use information sharing on a regular basis. There exists an accreditation scheme to build a network of trust between these CSIRTs (Trusted Introducer).

## 6.2 Good practices

This section will provide you with good practices on some of the main issues of information sharing:

- Established and tested initiatives for building trusted communities for information exchanges are found in the United Kingdom and the Netherlands;
- Two ways to facilitate achieving trust in sharing sensitive information across public and private parties:
  - The Traffic Light Protocol (TLP) – an easy and practical procedure.
  - Electronic information exchanges;
- An example a regional governmental initiative supporting cross-border information sharing is found in the Visegrad 4 example.



## Building trusted communities for information sharing

POP

MANDATED

CIP Maturity

### Background

There is an increasing amount of information on threats and risk factors and on protective measures. It is hard for individual organisations to analyse all of this information and to derive good practices for dealing with new risk factors.

In order to support CI organisations in selecting the right information and establishing good practices for protection, some nations have established small trusted communities in which information can be shared in a secure and trusted way.

This good practice discusses the information exchanges facilitated by the Centre for the Protection of Critical Infrastructure (CPNI) in the UK and by CPNI.nl in the Netherlands.

### Description

The information exchanges share information on the risk facing the CI in a small and trusted community. The communities can be built on a sectoral basis or around a special topic (e.g. SCADA security).

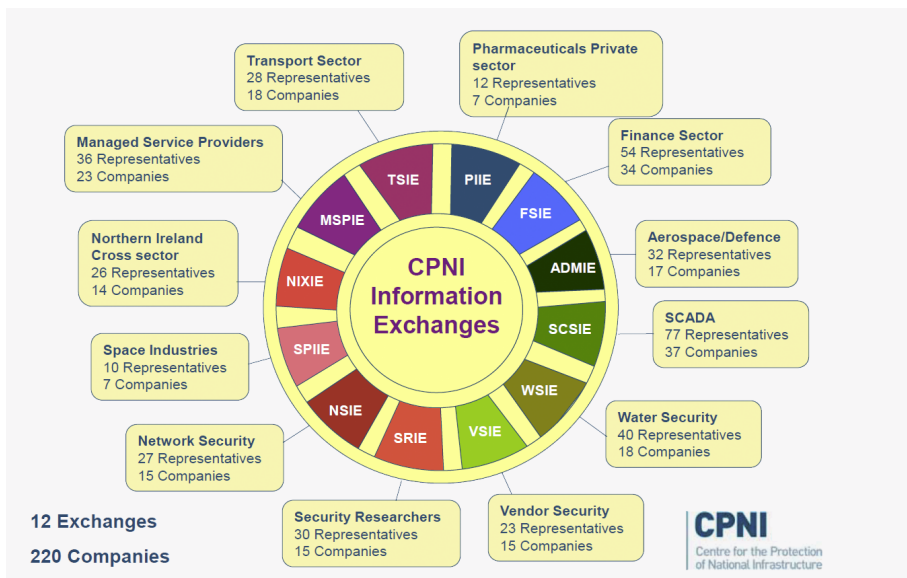


FIGURE 13: CPNI model of information exchange

(source: <http://www.cpni.gov.uk>)

The information exchanges bring together representatives from a specific CI or across multiple CI. They may also include relevant public organisations like law enforcement or intelligence services.

The information sharing is based upon the personal trust of representatives and information is shared in a secure and confidential way (see good practice Traffic Light Protocol).

Building on this trust, information is shared on threats, vulnerabilities and incidents, and on CIP good practices. This allows the organisations to learn from each other's good practices and lessons learned, and thus raise the level of understanding and protection within the whole network of CI.

#### **Experiences / Lessons learned**

- One of the key success factors for the information exchange is to establish a high level of trust within the community. Experience shows that trust can best be built in regular face-to-face meetings. This may take time; CPNI states that it may take up to two years to establish trust.
- The membership of an information exchange is on a personal basis and should provide continuity and trust. Therefore, it is often not allowed to send different representatives for each subsequent meeting.
- All information exchanged should be dealt with in a confidential and secure way.
- Organisations will only share information on incidents or risk factors if they can be sure that no sensitive information will come out into the open, or will be used against them by (for example) competitors or public agencies (such as a regulator).
- The *Traffic Light Protocol* (described below) has proven to be a very easy and practical tool for establishing the right level of confidentiality for the information exchanged.

## Traffic Light Protocol

PPP

▼ MANDATED

CIP MATURITY

### Background

In order to establish the level of trust needed for information sharing, it is necessary to establish procedures on how to deal with sensitive information in a trusted way.

The Traffic Light Protocol (TLP) provides a very easy method for establishing the required level of confidentiality for the information exchanged.

### Description

The TLP provides an easy method to achieve the confidentiality of sensitive information. One of the key principles of the TLP is that whoever contributes sensitive information also establishes if and how widely the information can be circulated.

The originator of the information can label the information with one of four colours<sup>[8]</sup>

- **RED - personal for named recipients only.** In the context of a meeting, for example, RED information is limited to those present at the meeting. In most circumstances, RED information will be passed verbally or in person.
- **AMBER - limited distribution.** The recipient may share AMBER information with others within their organisation, but only on a 'need-to-know' basis. The originator may be expected to specify the intended limits of that sharing.
- **GREEN - community wide.** Information in this category can be circulated widely within a particular community. However, the information may not be published or posted publicly on the Internet, nor released outside of the community.
- **WHITE - unlimited.** Subject to standard copyright rules, WHITE information may be distributed freely, without restriction.

### Experiences / lessons learned

The TLP is used widely, both by several European nations and by multinational working groups, e.g. in the information exchanges of the United Kingdom and the Netherlands, in the European SCADA and Control Systems Information Exchange (EuroSCSIE). Its strength is that it is very easy to use and that the responsibility of both the originator and receiver of the information are very clear.

## Electronic information exchange

PPP ▼

MANDATED

CIP MATURITY ▼

### Background

Sharing information on risk requires a trusted environment. Most information sharing initiatives are based on regular face-to-face meetings. If the information on vulnerabilities, threats and incidents has to be shared in a wider community a secure electronic environment can be useful. There have been several initiatives that have tried to create a secure and trusted electronic platform for electronic information sharing.

The most successful initiatives are used as an extra tool in support of communities that also attend face-to-face meetings.

### Description

In support of information sharing on CIP, many initiatives have tried to create electronic tools for information sharing, e.g. CIWIN, NEISAS<sup>[7]</sup> and CIRCA.

Most successful initiatives are used in support of regular face-to-face information exchanges, e.g. in the United Kingdom participants of the CPNI Information Exchanges and all Category 1 and 2 responders (see Section 8) have access to an extranet portal (National Resilience Extranet or NRE) with additional information, e.g. security advice documents.<sup>[11]</sup>

The EU project NEISAS has created a framework and a prototype platform in support of information sharing.

### Experiences / lessons learned

Experience shows that tools for electronic information exchange are best used as an additional tool for existing trusted information sharing communities. If no level of trust exists, then it is very hard to create a high level of trust in the electronic environment.

## Cross-border information sharing

PPP

MANDATED

CI MATURITY

### Background

In defining the CI it is important to analyse cross-border dependencies and determine whether citizens and critical services are highly dependent on infrastructure in another nation. For information exchange on these cross-border dependencies, collaboration on a multi-national regional basis may prove to be very valuable.

### Description

The Visegrad 4 is a collaboration between the Czech Republic, Slovakia, Hungary, Poland and Austria. Informal meetings are organised to exchange views on different approaches to common CI problems. This provides an overview of possible approaches and the opportunity to reflect on one's own approach. The Visegrad meetings are organised to exchange information on methods used for the identification of CI and for more detailed exchange per sector on CI identified and on important cross-border dependencies. Thus CI in a neighbouring nation can be designated as being critical for one's own nation.

Besides these direct results, the collaboration also helps in the effort towards a more common understanding of CI concepts and terminology within the region.

### Experiences / lessons learned

In sharing information, the different concepts and terminology used in different nations can provide a challenge for successful information sharing. Successful cross-border information sharing therefore also requires the building of trust and a common framework in face-to-face meetings.

## 6.3 References and further reading

- [1] CPNI information exchange membership guidelines, April 2010.  
Online: <http://www.cpni.gov.uk>
- [2] Warning Advice and Reporting Point (WARP) - United Kingdom.  
Online: <http://www.warp.gov.uk/benefits.html>
- [3] Public Private Partnership in the Cybercrime Information Exchange - NICC brochure, The Hague, the Netherlands.  
Online: [http://www.samentgencybercrime.nl/UserFiles/File/NICC%20brochure\\_uk.pdf](http://www.samentgencybercrime.nl/UserFiles/File/NICC%20brochure_uk.pdf)
- [4] Good Practice Guide Network Security Information Exchanges, ENISA, September 2009  
Online: <http://www.enisa.europa.eu/media/press-releases/guide-to-mitigate-vulnerabilities-threats-cyber-attacks>

- [5] Good Practices on Reporting Security Incident, ENISA, December 2009  
Online: <http://www.enisa.europa.eu/act/res/policies/good-practices-1/incident-reporting-mechanisms/reporting-security-incidents-good-practices>
- [6] Information technology — Security techniques — Information security management for inter-sector and inter-organisational communications, ISO/IEC CD 27010, November 2010.
- [7] <http://www.neisas.eu>
- [8] [http://en.wikipedia.org/wiki/Traffic\\_Light\\_Protocol](http://en.wikipedia.org/wiki/Traffic_Light_Protocol)
- [9] <http://www.chathamhouse.org.uk/about/chathamhouserule/>
- [10] EU Telecommunications Package, - regulatory framework for electronic communications 2009.  
Online: [http://ec.europa.eu/information\\_society/policy/ecomm/doc/library/regframeforec\\_dec2009.pdf](http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf)
- [11] National Resilience Extranet.  
Online: <http://www.resilience-extranet.co.uk>
- [12] CIRCA  
Online: <http://circa.europa.eu>



# 7 Risk management and CIP

## 7.1 General description and issues

### *The need for risk management in CIP*

CIP is primarily directed at strengthening the resilience of the assets that are of essence to the functioning of society. Therefore, knowing where and in what way that functioning may be disrupted and what can be done to prevent this is extremely important. Identifying weaknesses and their possible consequences and subsequently reducing the risk to acceptable levels is the core of risk management. CIP can therefore profit from risk management efforts in the sense that these can indicate which risk is already being addressed, provide possible risks to which the CI is still subject, provide insight into the relative significance of the risks and provide possible measures to reduce these risks.

### *Possible levels of aggregation for risk management*

Risk management (RM) can be performed on various levels, ranging from a very detailed, very specific RM process for a single machine to an all-encompassing RM effort concerning all risks potentially threatening a nation or a transnational infrastructure. This is graphically depicted in Figure 14. As we will show, RM policies can strengthen CIP at all these levels.

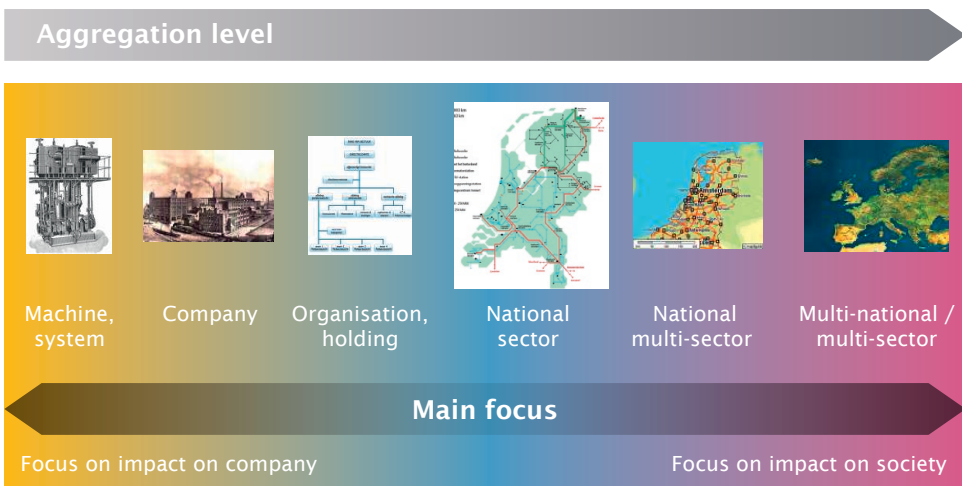


FIGURE 14: levels of aggregation in risk management

By and large, for the use of risk management in CIP three levels of aggregation can be distinguished which we will call the company level, the sector level and the national level. The use of RM on these levels is slightly different:

- The *company* will primarily use RM to manage the possible risk that can harm the company business objectives. The focus is on protecting the company itself. Sometimes this process will include the management of threats that the company exerts on the environment (e.g. for a chemical plant), but this is mostly done only if prescribed by legislation.
- RM at a *sector* level will primarily focus on the resilience of the sector, taking into account the individual measures taken by the constituents, but national and EU policies will to some extent enforce the consideration of societal impact.
- A *National Risk Assessment* (NRA) will primarily focus on the risk with societal impact, and take a wider range than just CI. It will for example consider the risk of pandemic flu. In general, CI will be involved in the NRA, as these CI can play an important role in the course of an incident (e.g. for pandemic flu: will electricity supply still be reliable in the event of mass illness and what could be the consequences for the public?). An NRA is the first step in a national risk management process, where risks identified by the NRA are managed consecutively in a policy-making process.

### *Applications for the various levels of RM in CIP*

#### *Company level risk management*

Although the goal served by a company level RM process is focussed on business continuity, when worked towards within a company that is part of the CI, is still directly beneficial to CIP. As one of the most important company business objectives is providing the main product or service, a company level RM process will identify possible threats to the continuity of 'production' and measures for mitigation of the associated risk. If the RM process is performed cyclically (as is the norm), the regular update of the RM process will show whether the measures were effective. This establishes a more resilient organisation, which is a prime concern of CIP.

#### *Sector level risk management*

RM at sector level aims to assess and mitigate remaining risk for the sector in spite of RM efforts already made in the constituent organisations. This delivers direct input for CIP as this indicates which risk is not covered by the different CI sectors. It generates an overview of the level of resilience of the CI and gives indications as to which risk remains to be addressed. Uniformity of RM efforts in the constituent organisations will greatly ease the assessment of efforts already made and will help to identify the remaining risk.

#### *National level risk assessment (NRA)*

An NRA is a centrally co-ordinated effort to survey the risk to which the nation is subject. This delivers a broad overview of potential risk for the community. This overview will typically include the CI, as they can have a profound effect on the way a crisis will propagate or be suppressed. This result will provide valuable insights into the role the CI plays at times of crises and the level of preparedness of the CI sectors. Furthermore, in such an assessment, the interconnectedness between CI sectors will be clarified, which is rarely exposed in company or sector level assessments. This effort can be integrated with a long-term policy exploration (horizon scanning) or serve more immediate goals, but in any case, the results should be fed back directly to the national policymakers to enable them to act on the outcome.



## *Approaches for furtherance of CIP by way of risk management*

### *Supporting of risk management within companies*

Although RM in CI organisations is not uncommon, there is no common standard of performing it. This leads to different levels of quality and incompatible results, which, from a CIP point of view undermines the reliability (completeness and correctness) of the efforts being made. A way to overcome this is to support the companies in doing RM by providing common tools with a common frame of reference. This facilitates the adaptation of an RM process for organisations not previously doing so (by ‘peer pressure’). It creates a basis for a common baseline level of protection and by creating a common frame of reference it will facilitate the exchange of information about RM. Another advantage of government provision of tools is that this way the content of the method can be influenced by the government. In this way, for example, some degree of societal impact could be explicitly included in the risks being considered. Additionally, by providing tools and a common framework a more concrete basis for introducing legislation, incentives or penalty systems is established.

### *Enforce risk management in companies and sectors*

Another way to further CIP by encouraging the use of RM is a system of legislation that enforces certain (or all) organisations or sectors that are part of the national CI to comply with an RM method. This policy is only attainable if it is accompanied by a standard and tools (see above).

It requires a national structure in which a strongly directive approach towards the CI organisations is accepted.

### *Integrate CI risk into the NRA process*

A third way to further CIP is to integrate CI within the NRA process. By closely involving CI representatives in an NRA and assessing the risk of CI dependencies, a better quality of results is reached. At the same time the contact between CI representatives and government is improved. Joint insight is gained in the interoperability of CI and the preparedness of CI organisations and CI sectors (or the lack of means to do so).

## **7.2 Good practices**

This section provides you with three good practices in the field of using RM for CIP:

- A good practice on strengthening risk management for CI operators through by supporting private initiatives and providing uniform risk related tools.
- A good practice on the use of legislation to enforce risk management in CI companies and CI sectors;
- A good practice on including CI operators in a central, government led initiative for long term strategic planning and CIP.

## Provide guidelines and tools for risk management

PPP
MANDATED
CIP Maturity

### Background

Providing tools and guidelines for risk management may foster the use, enhance the quality and, by providing a common frame of reference, facilitate information exchange about risk or risk management. The method can also introduce elements that specifically enhance CIP, such as explicitly including dependencies from other infrastructures as a threat and taking into consideration different kinds of impact that surpass the interests of the organisation. Ultimately this should lead to an enhanced resilience of the CI.

To this end, the method can be limited to risk assessment or cover the wider subject of risk management. Figure 15 illustrates the relationship between these concepts. In this text, we will concentrate on the full cycle of RM.



FIGURE 15: Relationship between risk assessment and RM

### Description

There are a large number of nations who have developed RM guidelines and tools. Among the nations that provide methods and/or tools are the United Kingdom<sup>[1]</sup>, Germany<sup>[2]</sup>, Denmark<sup>[3]</sup>, and others. Although these differ considerably, they have some elements in common that contribute to their success.

A uniform method for risk assessment should form a coherent system of steps that can be used as guideline by the target group and ideally, should by its very nature prove its added value. Each step should be sufficiently clear for the target group to be easily applicable. Steps that are commonly included in such a method, are:

1. determination of the context of the analysis;
2. identification of potential risk;

3. assessment of threats, vulnerabilities (sometimes integrated into determination of threats) and impacts;
4. determination of ensuing risks (and analysing them).

Elements that are of foremost importance for inclusion in the method to make it practically applicable, are:

- clear, uniform definitions and terms,
- which (types of) threats to include,
- which (type of) impacts to include,
- an objective scoring mechanism for probability and impact and ultimately risk.

Finally, one of the most important properties of the method is that it should be in line with the expectations and needs of the target group.

#### **Experiences/lessons learned**

- In order get the method accepted, it should conform as much as possible to current practices. A clear and not overly complicated method supported by simple and effective tools further enhances the level of acceptance. The Danish RVA method<sup>[3]</sup> is a prime example of a method that offers simple support tools.
- Starting such a method within a limited context, such as established crisis management structures or public organisations with an existing and clear chain of command significantly improves the likelihood of success.
- One should be aware that trying to enforce a risk assessment method on private organisations will likely result in a high level of resistance. A voluntary approach, if possible supported by incentives or penalties is more likely to succeed in the private domain.
- A successful implementation of a common risk assessment method can lead to a distinctly positive impact on the amount and ease of information exchange among the concerned parties and to a raised level of risk awareness.
- The development of a common method for risk management requires a high level of expertise and inside knowledge of the intended target group. Developing such a method in close co-operation with the target group and experts in risk assessment is therefore highly advisable.
- As getting lost in details is always a big pitfall, setting realistic and limited goals is an important factor in the likelihood of success. Limitations can be found in the width of the target group (such as limiting it to serve the needs of emergency services), or the extent of the method (such as initially limiting it to risk assessment only and not including other aspects of risk management).

## Enforce risk management in CI companies and CI sectors

PPP ▼

MANDATED ▼

CIP MATURITY ▼

### Background

The enforcement of risk management processes in CI organisations serves the goal of making RM standards to which they have to comply, thereby assuring a basic level of risk protection for these organisations.

### Description

A good example of mandatory RM is to be found in France. The traditional national government structure, with the central government being represented locally –with strong links to the local business- in so called ‘prefectures’ and a strong, centrally directed protection of the nation in terms of both defence and security, enabled the French government to adapt this structure to include CIP in 2008. Part of the French National Security Strategy is legislation in which the CI operators are forced to defend themselves from nationally defined threats at their own expense.

The first step in this process was to develop a risk assessment method (RAM) that was applicable to each and every organisation in the CI. This method was developed in the period 2003-2006 and has not changed since then, in order to offer a stable frame of reference to which to comply. Next, the central government (including their local representatives) appoints certain CI operators as ‘critical’. This implies these operators are obliged to produce a high-level Operator Security Plan (OSP). The OSP is based on the RAM and plans security measures and identifies underlying CI Facilities. In turn, these facilities are obliged to develop two plans: an internal CI operator security plan which is basically an internal risk management document and an external security plan in which the relationship with external parties –such as first responders, military, IT security- are described. The latter has to be agreed with those parties. The contents of these plans are communicated back to the government. Here, the results are analysed and assessed in terms of whether they comply with the requirements. If not, the organisation is forced to make the necessary changes. If they do not conform or refuse to do so, they are liable to legal sanctions.

Aside from obligations, the status of being critical also entails incentives: in the external security plan, the relations with external responders are described, and agreed upon. This means that for example a preferential treatment of the CI facilities in case of emergency can be negotiated.

The OSP is directly in line with the EU directive.

### Experiences/lessons learned

- This approach ensures that RM is applied in all organisations where it is deemed necessary at a level of quality that is assured.

- The results are fed back to the government, which gives a high level of control and of mutual insight.
- The fact that being appointed critical not only entails responsibilities, but also gains you rights, has increased the level of acceptance for this approach.
- The explicit inclusion of an external security plan ensures strong integration between CIP and emergency planning.

## Using a national risk assessment for CIP

PPP ▼

▼ MANDATED

CIP MATURITY ▼

### Background

A national risk assessment (NRA) aims to assess the risk that threatens society. The assessment can be limited to the most significant emergencies the nation could face in the future, or provide a wider foundation for the national strategic policy planning process. It should in both cases provide assessments taking into account the interactions between groups, players and infrastructures and provide an assessment of a wide range of possible societal impacts. Because of the importance of CI, CI should be included in NRA, as a possible risk scenario in case of major disruptions of CI, and in assessing the possible consequences on CI of other scenarios (e.g. major flooding, or an earthquake)

### Description

Several European nations have experience with performing an NRA. The United Kingdom (with their yearly National Risk Assessment<sup>[1]</sup>) provides a good example with regard to the frequent update of the NRA with a bi-yearly update of threat information and its direct link with establishing CIP policies and measures for and in CI sectors. Germany<sup>[2]</sup>, Denmark<sup>[3]</sup> and the Netherlands<sup>[4]</sup> also provide good examples of NRAs.

Some common experiences the nations share in the execution of an NRA include:

- Performing an NRA requires the co-operation and support of a wide variety of representatives of CI, emergency services and other governmental bodies.
- Getting an NRA in place is a process, not a unilateral decision. One must be prepared to 'sell' and negotiate the terms of application and method used.
- Transparency of the method and its intended use is an important element to reach acceptance.

Performing a comprehensive NRA is a complicated process that will require expert guidance and a large amount of effort and capacity.

One of the NRAs in use with an extensively and publicly documented method is the Dutch 'Nationale Risico Beoordeling'<sup>[4]</sup>. It is used as the analysis phase of the national security strategy and is used to direct the ensuing strategic planning phase. In this phase, risk is listed, analysed and formulated in the form of scenarios and the associated risk is assessed.

The method used for the risk assessment is an 'all hazard' approach: it enables the comparison of risk factors stemming from different types of threats, with causes lying in natural, deliberate, human or technical error or failure of critical services. The method is therefore by nature rather complicated: execution of the method will require a substantial amount of expertise and a substantial amount of 'field' expertise in order to correctly evaluate the risk.

The result of the method is an up-to-date risk diagram displaying the main risks and, most importantly, the underlying information and reasoning. Some of the CI scenarios that have been studied in this way include a major disruption of the electricity network, and several scenarios involving major disturbances of ICT. In other scenarios, CI operators were involved in determining the adverse effects on CI of the scenario for their infrastructure, e.g. in the event of major flooding.

Based on the risk assessment, public-private capabilities are identified -if required- to enable better handling of the assessed risk.

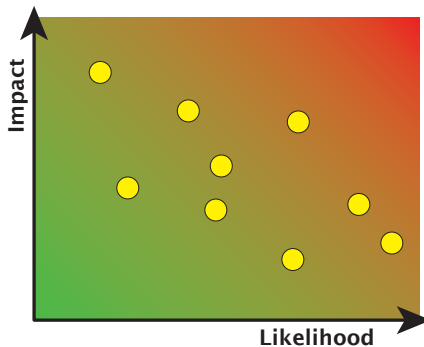


FIGURE 16: Example of a resulting risk diagram

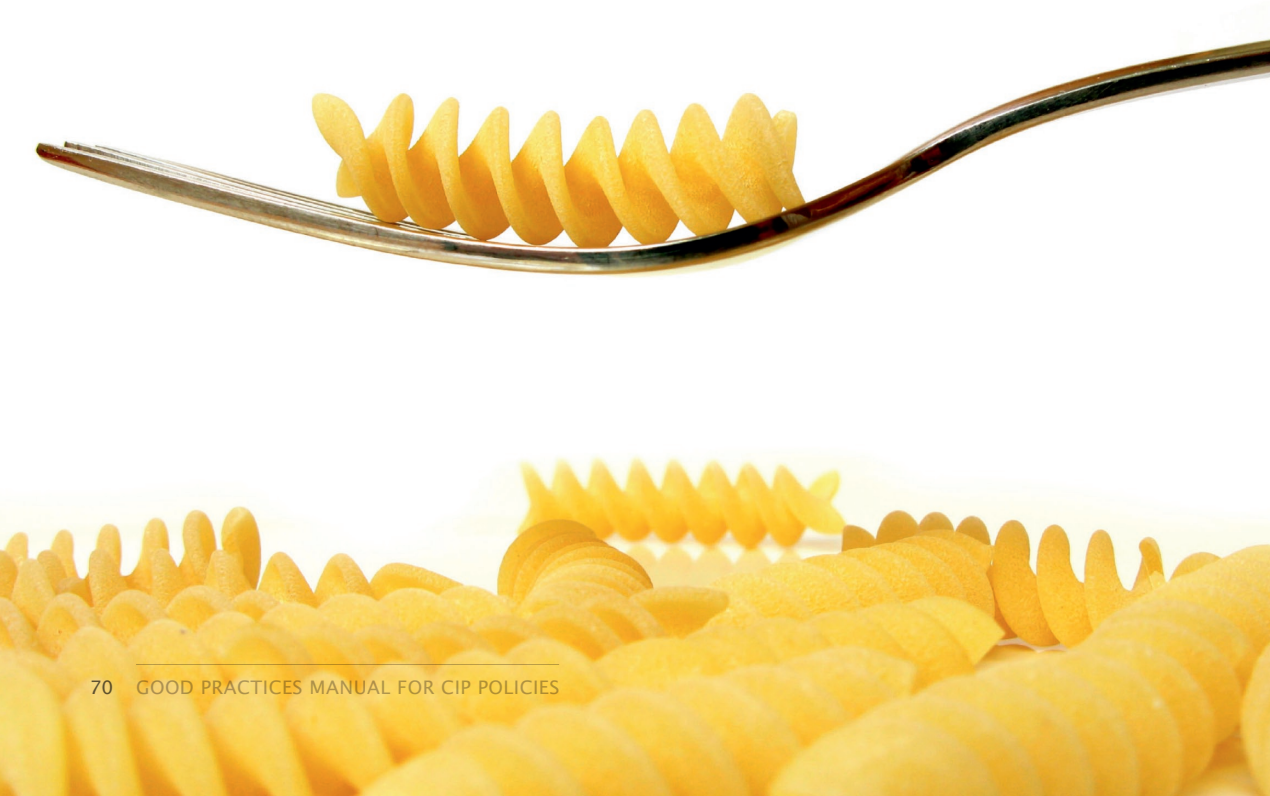
#### Experiences/lessons learned

- Performing an NRA strengthens the awareness in public and private parties of their mutual strengths and weaknesses.
- The co-operation required in an NRA process also strengthens the communication channels between concerned parties.
- The results of an NRA are strong instruments for long term strategic policy planning.
- An NRA will provide policymakers and CI operators with better insight into their interconnectedness.

### 7.3 References and further reading

- [1] Understanding risks and how the UK is preparing for emergencies.  
Online: [http://www.direct.gov.uk/en/Governmentcitizensandrights/Dealingwithemergencies/Preparingforemergencies/DG\\_176587](http://www.direct.gov.uk/en/Governmentcitizensandrights/Dealingwithemergencies/Preparingforemergencies/DG_176587)
- [2] Methode für die Risikoanalyse im Bevölkerungsschutz.  
Online: [http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Wissenschaftsforum/Bd8\\_Methode-Risikoanalyse-BS.pdf?\\_\\_blob=publicationFile](http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Wissenschaftsforum/Bd8_Methode-Risikoanalyse-BS.pdf?__blob=publicationFile)

- [3] DEMA's Approach to Risk and Vulnerability Analysis for Civil Contingency Planning. Online: [http://www.brs.dk/folder/nationalsaarbarhedsrapport2005/Background\\_paper\\_on\\_DEMAs\\_approach\\_to\\_risk\\_and\\_vulnerability\\_analysis.pdf](http://www.brs.dk/folder/nationalsaarbarhedsrapport2005/Background_paper_on_DEMAs_approach_to_risk_and_vulnerability_analysis.pdf)
- [4] Guidance Methodology National Safety and Security Strategy, Ministerie van Binnenlandse Zaken, The Hague, 2009. Online: <http://english.minbzk.nl/aspx/download.aspx?file=/contents/pages/104363/guidancemethodologynationalsafetyandsecuritystrategy2009.pdf>





## 8 Crisis management and CI

### 8.1 General description and issues

#### *The need to integrate CI in crisis management*

Although there are many ways to try to prevent untoward events from happening, there is no way that prevention can eliminate all risk to nations and their citizens. Governmental crisis management (CM) organises and manages all roles, responsibilities and resources to deal with serious incidents, emergencies, and crises<sup>2</sup>. Good CM at the national level, as well as at international and regional levels, takes CI into account as part of its preparedness, response, and restoration phases for the following reasons:

- By definition, the consequences of a CI breakdown can be severe. Avoiding CI disruption and preparations for a fast restoration process is the responsibility of the CI operator. The potential impact of a CI disruption on the functioning of society and on the population may be high. Therefore, CM needs to plan for dealing with disruption of CI and the consequences thereof.
- Joint exercises may enhance CM preparedness of both governmental and CI crisis management to a large extent.
- The continuity of CI services for CM is often critically required to conduct crisis response operations (preparedness, response and recovery phases). This includes both the ability to operate the main national and regional crisis control centre(s) and the base operational centres that support the incident response operations in the field. Examples of such CI are: energy, drinking water, telecommunication, food, financial services, and transport.
- The continuity and – if feasible – fast restoration of certain CI in a disaster area during the response and recovery phases of CM may be an important part of the crisis operation, for instance CI that support the non-evacuated persons. Failing to safeguard such CI services will widen the emergency at hand; more people need to be evacuated, and more lives may be at risk. This requires CM to understand the operation of CI to a certain extent.
- CI services in the disaster area that are still in an operational state during the response and recovery phases of CM can be utilised in CM in innovative ways to its advantage. An example is the use of operational telecommunication services like SMS, cell broadcast and Internet access to communicate with victims and other specific groups of the population in the disaster area.
- For the recovery phase, the earlier CI identification around critical societal functions may help CM to prioritise the restoration of services.

---

<sup>2</sup> A widely accepted definition and delineation of the terms emergency management, disaster response, and crisis management does not yet exist. Various nations use these terms in an interchangeable manner. For that reason this handbook uses the term crisis management to cover the full set of major unpredictable incidents, emergencies, disasters, and other crises. One view is that a crisis is a major incident where an incapable response organisation loses its ability to manage and control the escalating situation. As a result, this subsequently leads to potential consequences for political decision-makers (public) and/or top management (private organisation). In Anglo-American nations emergency management comprises pre-impact risk management, pre-impact response management, and post-impact consequence management [21].

### EXAMPLE: USE OF CI IN CM

Following the tsunami of 26 December 2004, the Sri Lankan mobile telephony operators extracted from their databases the numbers of the international mobile phones that were roaming in their networks in the days before the disaster struck. 10,252 SMS-messages were sent asking the telephone owners to report a sign of life to a call centre using a toll-free number. Using triangular measurements of the signal strength of the mobile phones of those people which reported they were in trouble, the mobile telephony operators were able to pinpoint the location of a number of trapped victims for crisis response teams. In this case, the technical capabilities of CI still in a operational state in a disaster area were used to their fullest extent. <sup>[6]</sup>

From the above, it will be clear that effective and efficient CM requires in-depth knowledge of CI, their operations and their dependencies. Close co-operation and mutual understanding with CI operators is required during incident response planning, emergency preparedness (e.g. joint training and exercises), crisis response and restoration.

#### *Co-operation issues for CM and CI operators*

Depending upon a nation's CM-structure, CI operators may have a formal position or just an advisory role in national, regional and local CM. For an effective CM operation, a set of recommended arrangements to be made with (often private) CI operators and CM functions includes:

- A set of procedures or a legal foundation that specifies that CI operators (or a coordinating representative for their CI sector) may or shall participate in the national and regional CM structure when their CI is or may become disrupted.
- CM and CI operators need to understand the benefits of close cooperation in all phases of incident response and CM. A clear understanding of each other's abilities and capabilities helps to make the most effective use of all available resources to address an incident, emergency or crisis.
- An arrangement of authorities and responsibilities that is understood. CM has to trust CI operators to know best on how to operate and deal with crisis situations in the CI they own and operate. CI operators have to accept that decisions taken by national or regional CM may oppose the advice given to the authorities by the CI operators and may oppose the business interest of a single CI operator.
- At the operational level, it is of the utmost importance to understand each other's processes and specific keywords ('slang') which can be a source of confusion to public, private, military and other players in CM.<sup>3</sup> For that reason, site visits and joint exercises are key to effective and efficient joint CM with CI operators.

---

<sup>3</sup> As an example: providing cover has a completely different meaning for military personnel than it does to police forces. Different understanding of the same term during EM operations has resulted in unnecessary fatalities.

- Company and personal sensitive information provided by a CI operator to CM shall be protected against and exempted from becoming public knowledge (e.g. Freedom of Information Act) and may only be used and disseminated for the purpose for which it was provided to CM (see for example Section 6 on 'Information sharing' and <sup>[2]</sup>). Sensitive government information disseminated to a CI operator shall be protected by the CI operator according to its classification.
- Under certain circumstances, it may be necessary for CM in one MS to initiate CM actions regarding its CI to help to protect (an)other MS.

Above all, establishing means for direct contact between the public CM function(s) and the operations management / crisis response centres of CI operators is essential for all of the above at regional, national, and international levels. This includes direct crisis communication means, as well as CM structure and contact directories. International examples of the latter can be found in <sup>[3]</sup> and <sup>[4]</sup>.

#### EXAMPLE: USE OF CI KNOWLEDGE IN CRISIS MANAGEMENT

At the end of July 2007, sustained heavy rainfall caused flooding of a large area in central and western England. Local power distribution had to be turned off for safety reasons. In the middle of this disaster area, the national power transmission operator National Grid operates a power station in Walham, Gloucestershire. As the local power distribution grid had no tie lines connected to that substation, they only communicated about the status of their own substations to the emergency management centre. The National local grid, which is part of Gold Command, signalled the urgent need to protect the Walham substation from flooding. An overly high water level would have required a safety shutdown. That would have caused an estimated 350.000 to 500.000 households or some 2 million people to be without power and dependent on CI services for almost a week. The additional draw on emergency management resources would have been tremendous.



**FIGURE 17:** The Walham substation with a temporary flood barrier (photo: UK MOD Crown Copyright (2007))

### *Cross-border aspects*

Crises, especially ones caused by the natural disasters or technological failure, are not confined to one nation and neither are their effects. Also CI may cross European borders and even may be designated as a European CI (ECI)<sup>[2]</sup>. Disruption of such a CI may seriously impact the societies of neighbouring nations, e.g. disruption of a major gas transport pipeline. For that reason, *cross-border CM* shall take cross-border CI into account taking advantage of existing cross-border incident-handling structures and processes from for instance the European Network of Transmission System Operators for Electricity (ENTSO-E).

### *Return on Investment*

Preparedness for CM, especially when involving CI operations, has a cost factor to it. However, the business case is hard as there is only a virtual profit and no tangible product. One should balance between preparing for the worst and 'how good is good enough' by defining acceptable risk versus non-acceptable risk to society.

## **8.2 Good practices**

This section will provide you with four good practices on the relation between crisis management and CI:

- A good practice on the use of legislation as a basis for co-ordinating Crisis Management efforts for CI operators;
- A good practice on the optimal use of the expertise of CI operators and experts by involvement of CI expertise as support function to CM;
- A good practice on creating common knowledge between CI operators and CM organisations by involving CI sectors / operators in joint public-private CM exercises;
- A good practice on the integration of CI operators into CM structures.

## Crisis Management Legislation and CI

POP

MANDATED

CIP MATURITY

### Background

Some nations require a legal framework to oblige CI operators to form a CI sector-specific CM-structure or be formally part of the national or regional CM structure. An Emergency or Crisis Act may serve this function and actively involve CI operators in the preparedness, response, and service restoration phases of CM.

### Description

Legislation for CM can be sector-specific or can cover all CI sectors. In the first case, legislation is made either by the ministry responsible for the sector or by the sector regulator. Such legislation is more finely tuned. Often this is a result of collaborative development with the sector. In the second case, legislation can be a framework within which CI operators are mandated to collaborate with regional CM. It may also provide a framework for CM at the national level.

Examples of CI sector-specific legislation frameworks are often found in the telecom and internet sectors. For example, section 14.2 of the Dutch Telecommunication Act and accompanying ruling establishes the Dutch National Continuity Board for Telecommunications (NCO-T). The NCO-T involves the major fixed and mobile telecom operators and Internet service provision operators<sup>[14]</sup>. The NCO-T is responsible for a sector-wide mutual support in case of major ICT-related crisis based upon an annual audited base level of BCM. This base level standard is based upon sectoral self-regulation.

In the United Kingdom, an equivalent approach has been taken based upon section 32(4)(a) and (b) of the Communications Act 2003, in relation to the Civil Contingencies Act. The Electronic Communication – Resilience and Response Group (EC-RRG), which comprises the major operators established the national response capability to ICT emergencies through the National Emergency Alert for Telecommunications (NEAT)<sup>[15]</sup>. In the same way, the French VIGIPIRATE set of plans incorporates the PIRANET crisis management plan for the information and communication (ICT) sector. PIRANET obliges the French telecommunication operators to participate in the national and prefecture CM structure in case of a major ICT-crisis.

Other CI sectors, such as the financial sector, have established equivalent sector-wide business continuity and crisis response arrangements in various nations based on the ruling of a CI sector-specific regulator or overseer.<sup>[16]</sup>

An example of a legislative framework at the national level for all CI sectors can be found in Estonia, which established a Crisis Act that has a dedicated Chapter ‘Organisation of Continuous Operation of Vital Services’. This act regulates the role and responsibilities of ministries, local and national CM, and CI operators to assure the

continuity of 41 critical services.<sup>[13]</sup> In Slovakia, the acts on Emergency Preparedness and on Crisis Management bind CI Operators in over twenty CI sectors to implementing crisis planning.

#### **Experiences/lessons learned**

- Some European nations distinguish between legal frameworks for dealing with terrorism and other hazards. When the incident cause is obvious, this works. When it is not clear whether CM is dealing with a terror attack or another cause, this distinction may lead to an ineffective CM response.
- One thing that is important to the private CI sector is that the CM-CI acts, regulations and arrangements maintain a level-playing field for all CI operators both nationally and preferably internationally as well. Note that in the event of an ICT crisis, it is possible that an emergency in one MS can only be addressed by CM in another MS, even if that MS is not suffering a crisis directly.
- As some CI infrastructures are nationwide, arrangements by the CI operator need to be harmonised across all regional governmental CM bodies for reasons of efficiency, interoperability and limiting the risk of misunderstandings

## Involvement of CIP expertise as support function to CM

PPP

MANDATED

CIP MATURITY

### Background

For effective decision-making, CM may need to understand the consequences of CI disruption in a certain area including its cascading effects. Help for CM decision-making can be obtained from CI protection (CIP) experts who understand threats to CI, their critical dependencies, their disruption and restoration characteristics, and potential cascading effects. The organisation of CM and CIP may involve distinct parts of government, of the CI operator organisations and other stakeholders. Close co-ordination and common understanding is not a given.

### Description

There are two applications for involving CI knowledge in CM:

- For CM planning purposes various scenarios can be analysed by CIP-experts.
- During an evolving crisis, CIP experts may propose two or more courses-of-action for CM, the consequences of which can be analysed in depth. CM can then make an informed decision valuing the expert analysis results in combination with other decision factors.

Both steps improve the CM actions and may shorten the recovery and restoration process.

An example of such a capability is the US Department of Homeland Security (DHS) Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), which normally operates as an infrastructure-intelligence fusion centre that analyses threats and risk to CI.

During crisis, HITRAC mobilises its Incident Risk Analysis Cell, which taps into the centre's steady-state programmes and capabilities to provide immediate analytical support to CM decision-makers in real time during the crisis. Assistance includes risk analysis, threat analysis, and consequence modelling conducted by the National Infrastructure Simulation and Analysis Center (NISAC). NISAC combines a set of infrastructure models with threat and consequence models.<sup>[17]</sup>

The Australian CI Programme for Modelling and Analysis (CIPMA) has similar objectives to those of NISAC.<sup>[22]</sup> In Europe only some initial steps have been taken in this direction (EU project DIESIS, a UK initiative<sup>[23]</sup>). The added benefit of these activities to CM is significant: sector and threat-specific CIP assessments as well as CI expertise and knowledge are made available to CM.

### Experiences/Lessons learned

- The use of modelling and simulation requires sets of data from CI operators and various models that can be federated into a single model. Obtaining the right level of data from CI operators is a major effort, especially because most such data is company sensitive at the least.
- A good example of CM support is NISAC's CI models and data sets. Shortly after the Hurricane Katrina disaster, NISAC supported the Federal Emergency Management Agency when Hurricane Rita started to threaten the same areas. NISAC's analysis showed where CI restoration teams could best be centred, determined specific areas where the population would be most confronted with disrupted power, drinking water supply, transport and telecommunications, and estimated the need for emergency supplies for each county.
- CIPMA has a set of models but is still busy building data sets. Required data, e.g. about flood plains, often exists at municipal level in a form that requires a lot of effort to convert it to data that can be used in the set of CIPMA models. Experience has also shown that data about CI assets is not always readily available to CM during an emergency. A base set has to be made available as part of preparation ('cold phase').



## Joint public-private CM exercises involving CI sectors / operators

PPP ▼

MANDATED

CIP MATURITY ▼

### Background

Regional, national, and international CM prepares itself for a wide range of hazards and emergencies. CM needs to take CI into account during most emergencies. Rather than dealing with CI operators in an ad hoc manner, there are many reasons for establishing a clear understanding and framework for addressing incidents, emergencies and crises. Failing this, a straightforward incident may evolve into a major crisis. By performing exercises, one learns (often the hard way) about each other's roles, responsibilities, decision-making cycles, capabilities, abilities, and terminology. Last but not least, the 'getting to know each other' is a much quoted important factor in diminishing friction between groups and facilitating co-operation. For this reason it is also important to plan major exercises to also allow for the induction and introduction of new senior level personnel into the overall CM - CI community.

### Description

Joint public-private regional, national and cross-border exercises create the right level of preparedness for emergencies of CM and CI operators. Exercises can be held at operational, tactical, and strategic levels and/or span multiple levels. Increasingly, nations involve CI operators as key partners in regional, national and international exercises.

CI involvement in regional and national exercises can be organised in different ways:

- Some nations, e.g. France, oblige their CI operators to take part in regional and national CM exercises.
- Nations like the Netherlands expect their CI operators to voluntarily play their role in regional and national exercises.
- Slovakia contracts CI operators to take part in their national exercises.

In Europe, some nations organise major national exercises that involve CI or the possibility of disruption of CI with cascading effects. A good example is the German Länder Übergreifende Krisenmanagement-Übung/Exercise (LÜKEX), which exists since 2004. LÜKEX takes CI and their dependencies into account in the development of the scenarios, both at the German Bundesländer (regional) level and the national level. CI operators take part in the exercises<sup>[1][1]</sup>.

Examples of international CM exercises are the worldwide set of Cyberstorm exercises and Cyber Europe 2010 which was organised by ENISA.<sup>[12][13]</sup>

### **Experiences/lessons learned**

- A prerequisite to an exercise is to define the exercise objectives. A 'making errors is allowed - no consequences' policy yields most lessons to be learned for the improvement of CM-CI co-operation.
- One result of exercises is diminishing the chances of friction and misunderstanding during the 'fog of a real crisis'.
- Exchange of sensitive private company data to CM during exercises requires data security safeguards by the CM environment (see Section 6 "Information sharing")

## CI Sector integration into CM structure

PPP ▼

MANDATED

CIP MATURITY ▼

### Background

The threat of international terrorism and the increasing effects of natural disasters have created a growing challenge for national protection, including the protection of CI. The importance of CI has convinced some nations to integrate CI sectors into the national CM structure.

### Description

Some European nations have experience embedding CI operators tightly into their CM chain of decisionmaking, both at the operational, tactical and strategic (national) levels.

Some nations involve specific sectors in the organisation of their national CM, e.g. to take part in the strategic CM decision preparation process in either an advisory role or a formal role. The Swiss strategic level CM structure for major ICT-emergencies called SONIA is an example<sup>[10]</sup>. SONIA (Special Task-Force for Information Assurance) has a strong connection with the Swiss security services, an international contact network, political weight with the Foreign Ministry in case international response is required, and legal response capabilities. SONIA is linked to the Swiss reporting and analysis centre for information assurance MELANI which also acts as the national computer emergency response team (CERT) covering all CI.

The United Kingdom is a good example of where operators from all CI sectors (or the CI sector coordinating representative) are part of the crisis preparedness and response scheme as so-called Category 2 responders at the strategic level (Gold Command), and tactical level (Silver Command). Category 1 and 2 organisations form Local Resilience Forums (based on police areas) which will help co-ordination and co-operation between responders at the local level (a.k.a. Bronze Command). See<sup>[8], [9], and [11]</sup>.

### Experiences/Lessons learned

- The current CM emphasis in most nations is much more focused on a single disruption of CI and its potential consequences, e.g. planning for disruption of drinking water supply, than it is on cascading failure and to common mode failure, such as a major storm disrupting multiple CI at the same time. The recommendation is to prepare for common mode failures and cascading failure effects affecting multiple CI at the same time.
- Hardly any CM planning takes into account the fact that CI dependencies during an crisis may be quite different from CI dependencies recognised during normal CI operation (see Section 4, Dependencies - mode-of-operation ).

- Tight integration of CI operators into CM requires fulfilment of a large set of requirements. Mutual understanding of roles, responsibilities, capabilities and abilities is a lengthy process that requires investment in terms of time, human co-operation, learning each other's 'slang', and above all regular exercises at all levels of command. The reward, however, is high for CM, the private CI, and last not but least the population.
- Crisis communications by national / regional CM and by the CI operators to other CI operators and the public should be aligned to avoid confusion and conflicting instructions.
- Although not yet common practice, planning for creative use of CI that are still in an operational state in an crisis area may yield a lot of benefits to the CM operation as some examples have shown.

### 8.3 References and further reading

- [1] Luijff, E., Klaver, M., "Insufficient Situational Awareness about Critical Infrastructures by Emergency Management", paper 10 in: Proceedings Symposium on "C3I for crisis, emergency and consequence management", Bucharest 11-12 May 2009, NATO RTA: Paris, France. RTO-MP-IST-086.  
Online: <http://ftp.rta.nato.int/public//PubFullText/RTO/MP/RTO-MP-IST-086//MP-IST-086-10.doc>
- [2] European Council, Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Brussels, December 2008.  
Online: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF>
- [3] UK's Civil Contingencies Act, Information sharing aspects (2004).  
Online: <http://interim.cabinetoffice.gov.uk/ukresilience/preparedness/informationsharing.aspx>
- [4] Civil Emergency Planning Handbook 2009, MSB, Sweden.  
Online: [http://www.msb.se/Upload/Produkter\\_tjanster/Publikationer/MSB/0039-09\\_International\\_CEP-Handbook-2009.pdf](http://www.msb.se/Upload/Produkter_tjanster/Publikationer/MSB/0039-09_International_CEP-Handbook-2009.pdf)
- [5] Von Kirchbach, H-P. et al, Bericht der Unabhängigen Kommission der Sächsischen Staatsregierung Flutkatastrophe 2002, 2003.
- [6] Jansz, M., Disaster Recovery and ICT in Sri Lanka: The day after, Information for Development (I4D), January 2005, p 10.
- [7] International CIIP Directory (For Official Use Only), issued by G8 and Meridian.
- [8] UK's civil contingencies management structure described in [http://en.wikipedia.org/wiki/Gold\\_-\\_silver\\_-\\_bronze\\_command\\_structure](http://en.wikipedia.org/wiki/Gold_-_silver_-_bronze_command_structure)

- [9] UK Cabinet Office/ Civil Contingencies Secretariat.  
Online: <http://interim.cabinetoffice.gov.uk/ukresilience.aspx>
- [10] Federal Strategy Unit for IT – FSUIT. Online: <http://www.isb.admin.ch/themen/sicherheit/00152/index.html?lang=en>
- [11] Emergency Preparedness document, “Co-operation at the regional level in England”, UK Cabinet Office.  
Online: [http://interim.cabinetoffice.gov.uk/media/132011/ep\\_chap\\_17.pdf](http://interim.cabinetoffice.gov.uk/media/132011/ep_chap_17.pdf)
- [12] ENISA: ICT CERT exercise material, ENISA, 2009.  
Online: <http://www.enisa.europa.eu/act/cert/support/exercise>
- [13] Good Practice Guide on National Exercises, , ENISA, 2009.  
Online: <http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises>
- [14] Instellingsbesluit NCO-T 2007, State Secretary of Economic Affairs, The Hague, The Netherlands.
- [15] UK Category 2 Responders - Generic Emergency Planning Arrangements for Telecommunications.  
Online: [http://interim.cabinetoffice.gov.uk/ukresilience/preparedness/ccact/cat2\\_info/telecoms.aspx](http://interim.cabinetoffice.gov.uk/ukresilience/preparedness/ccact/cat2_info/telecoms.aspx)
- [16] Norwegian Financial Services Authority ICT regulation article 11.
- [17] Homeland Infrastructure Threat and Risk Analysis Center (HITRAC).  
Online: [http://www.dhs.gov/xabout/structure/gc\\_1257526699957.shtm](http://www.dhs.gov/xabout/structure/gc_1257526699957.shtm)
- [18] <http://www.denis.bund.de/luekex/Luekex-Flyer-englisch.pdf>
- [19] National Strategy for Critical Infrastructure Protection (CIP Strategy), Bundesministerium des Innern, Berlin, 17 June 2009.  
Online: [http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/cip\\_strategy.pdf?\\_\\_blob=publicationFile](http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/cip_strategy.pdf?__blob=publicationFile).
- [20] Emergency Act, 15 June 2009, Estonia.
- [21] E. Dykstra, ICT, Critical Infrastructure and Emergency Management... Vital Connections?, International Katrina Project, 2011.
- [22] Australian’s CIPMA efforts.  
Online: <http://www.csiro.au/partnerships/CIPMA.html>
- [23] <http://gow.epsrc.ac.uk/ViewGrant.aspx?GrantRef=EP/I01344X/1>



## 9 Definitions

<p><b>Business Continuity Planning (BCP)</b></p> <p>BCP is planning that identifies the organisation’s exposure to internal and external threats and synthesises hard and soft assets to provide effective prevention and recovery for the organisation, whilst maintaining competitive advantage and value system integrity.<sup>[5]</sup></p>
<p><b>Crisis management</b></p> <p>Crisis management is the process by which an organisation deals with a major event that threatens to harm the organisation, its stakeholders, or the general public. <sup>[Wikipedia]</sup></p>
<p><b>Critical infrastructure</b></p> <p>A critical infrastructure is an asset, system or part thereof (located in Member States) that 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>[1]</sup></p>
<p><b>Dependency</b></p> <p>A dependency is a linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other.<sup>[7]</sup></p>
<p><b>Disaster</b></p> <p>A serious disruption of the functioning of a community or a society causing widespread human, material, economic or environmental losses which exceed the ability of the affected community or society to cope using its own resources.<sup>[8]</sup></p>
<p><b>Incident</b></p> <p>Realisation of a risk.</p>
<p><b>Mitigation</b></p> <p>The action of reducing the severity, seriousness, or painfulness of the effects of incidents when they occur. <sup>[derived from Oxford dictionary]</sup></p>
<p><b>Preparedness</b></p> <p>Preparedness is a continuous cycle of planning, organising, training, equipping, exercising, evaluation and improvement activities to ensure effective coordination and the enhancement of capabilities to prevent, protect against, respond to, recover from, and mitigate the effects of all hazards. <sup>[Wikipedia: text emergency management]</sup></p>

<b>Risk</b>
Risk is a combination of the consequences of an event (hazard) and the associated likelihood/probability of its occurrence. <sup>[3]</sup>
<b>Risk management</b>
Risk management refers to a coordinated set of activities and methods that is used to direct an organisation and to control the many risks that can affect its ability to achieve objectives. <sup>[6]</sup>
<b>Threat/hazard</b>
Hazard is a 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. <sup>[9]</sup>
<b>Vulnerability</b>
A vulnerability is the characteristics and circumstances of a community, system or asset that make it susceptible to the damaging effects of a hazard. <sup>[9]</sup>
<b>Mitigation</b>
Structural and non-structural measures undertaken to limit the adverse impact of natural hazards, environmental degradation and technological hazards. <sup>[8]</sup>
<b>Resilience</b>
The ability of a system, community or society exposed to hazards to resist, absorb, accommodate and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions. <sup>[9]</sup>
<b>Measure</b>
A plan or course of action intended to mitigate a risk. <sup>[derived from Oxford dictionary]</sup>



## References

- [1] European Council, Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Brussels, December 2008.  
Online: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF>
- [2] ISO, Vocabulary, ISO Guide 73:2009.
- [3] ISO, Risk assessment techniques, ISO 31010:2009.
- [4] Hubbard, Douglas (2009). *The Failure of Risk Management: Why It's Broken and How to Fix It*. John Wiley & Sons. p. 46.
- [5] Elliot, D.; Swartz, E.; Herbane, B. (1999) Just waiting for the next big bang: business continuity planning in the UK finance sector. *Journal of Applied Management Studies*, Vol. 8, No, pp. 43-60.
- [6] ISO, Risk management – Principles and guidelines, ISO 31000:2009.
- [7] Luijff, E., Burger, H., Klaver, M., “Critical Infrastructure Protection in The Netherlands: A Quick-scan”, In U.E. Gattiker (Ed.), *EICAR 2002 Conference Best Paper Proceedings* (ISBN: 87-987271-2-5) 19 pages. Copenhagen: EICAR.  
Online: [http://www.alejandrobarrros.com/media/users/1/50369/files/4363/2\\_NetherlandsCidefpaper\\_2003.pdf](http://www.alejandrobarrros.com/media/users/1/50369/files/4363/2_NetherlandsCidefpaper_2003.pdf)
- [8] UNISDR, Living with risk, A global review of disaster reduction initiatives, 2004 version.  
Online: [http://www.unisdr.org/eng/about\\_isdr/bd-lwr-2004-eng.htm](http://www.unisdr.org/eng/about_isdr/bd-lwr-2004-eng.htm)
- [9] EU COMMISSION STAFF WORKING PAPER on Risk Assessment and Mapping Guidelines for Disaster Management; SEC(2010) 1626 final, Brussels, 2010.



# 10 Quick reference to good practices

GOOD PRACTICE	THEME	Pg.	PPP	MANDATED	MATURITY	RESOURCES	QUICK WIN
Operator-based approach	Identification of CI	20	PPP ▼	MANDATED ▼	CIP MATURITY	RESOURCES	
Service-oriented approach	Identification of CI	22	PPP ▼	MANDATED	CIP MATURITY	RECOURS	
Asset or "hybrid" approach	Identification of CI	23	PPP ▼	MANDATED	CIP MATURITY	RECOURS ▼	
A bottom-up, cross-border approach	Identification of CI	24	PPP ▼	MANDATED	CIP MATURITY	RECOURS	
Intersectoral workshops	Dependencies	32	PPP ▼	MANDATED	CIP MATURITY	RESOURCES	Quick win
Qualitative analysis	Dependencies	34	PPP ▼	MANDATED	CIP MATURITY	RECOURS	
Quantitative analysis	Dependencies	37	PPP ▼	MANDATED	CIP MATURITY	RECOURS ▼	
CIP board at the strategic level	PPP	43	PPP ▼	MANDATED	CIP MATURITY	RESOURCES	
Provide common funds for CIP measures	PPP	45	PPP ▼	MANDATED	CIP MATURITY	RECOURS	Quick win
Attaining voluntary cooperation through providing expertise	PPP	46	PPP ▼	MANDATED	CIP MATURITY	RECOURS	
Compelling co-operation	PPP	47	PPP ▼	MANDATED ▼	CIP MATURITY	RECOURS	
Building trusted communities for information sharing	Information sharing	55	PPP	MANDATED	CIP MATURITY	RESOURCES	Quick win
Traffic Light Protocol	Information sharing	57	PPP	MANDATED	CIP MATURITY	RECOURS	Quick win
Electronic information exchange	Information sharing	58	PPP	MANDATED	CIP MATURITY	RECOURS	
Cross-border information sharing	Information sharing	59	PPP	MANDATED	CIP MATURITY	RESOURCES	Quick win

GOOD PRACTICE	THEME	Pg.	PPP	MANDATED	MATURITY	RESOURCES	QUICK WIN
Provide guidelines and tools for risk management	Risk management	64	PPP	MANDATED	CIP MATURITY	RECOURCES	
Enforce risk management in CI companies and CI sectors	Risk management	66	PPP ▼	MANDATED ▼	CIP MATURITY	RECOURCES	
Using a national risk assessment for CIP	Risk management	68	PPP ▼	MANDATED ▼	CIP MATURITY	RECOURCES	
Crisis Management Legislation and CI	Crisis management	75	PPP	MANDATED ▼	CIP MATURITY	RECOURCES	
Involvement of CIP expertise as support function to CM	Crisis management	77	PPP	MANDATED	CIP MATURITY	RECOURCES	
Joint public-private CM exercises involving CI sectors / Operators	Crisis management	79	PPP ▼	MANDATED	CIP MATURITY	RECOURCES	
CI Sector integration in CM structure	Crisis management	81	PPP ▼	MANDATED	CIP MATURITY ▼	RECOURCES	

## Legend

PPP	Amount and intensity of public - private partnerships required before adopting good practice
Mandated	Suitability for mandated approach, in favour of voluntary approach
Maturity	Amount of CIP maturity required before adopting good practice
Resources	Amount of resources (time, money, effort) required
Quick win	Suited for beginners and delivers good results with only small investments

# Colophon

## Editors

<p>Marieke Klaver Eric Luijff Albert Nieuwenhuijs</p>	<p>TNO Oude Waalsdorperweg 63 2597 AK The Hague Netherlands Email: <a href="mailto:Marieke.Klaver@tno.nl">Marieke.Klaver@tno.nl</a> <a href="http://www.tno.nl">http://www.tno.nl</a></p>	
---	---	--

## Contributors

<p>Marije Breedveld Samira Lahdahda Pamela van Erve</p>	<p>Ministry of Security and Justice Schedeldoekshaven 100 2511 EX The Hague Netherlands</p>	 <p>Ministerie van Veiligheid en Justitie</p>
<p>Eduard Mračka</p>	<p>Ministry of Transport, Construction and Regional Development Nám Slobody 6 810 05 Bratislava Slovakia</p>	
<p>Alexander Klimburg</p>	<p>OIIP Berggasse 7 A-1090 Vienna Austria</p>	 <p>ÖSTERREICHISCHES INSTITUT FÜR INTERNATIONALE POLITIK AUSTRIAN INSTITUTE FOR INTERNATIONAL AFFAIRS</p>
<p>Kaido Tee</p>	<p>Ministry of the interior Pikk 61 15065 Tallinn Estonia</p>	 <p>SISEMINISTERIUM Estonian Ministry of the Interior</p>

Readers are welcome to translate this manual into another language, provided they notify the editors in advance and receive their express written consent.

An electronic version of this manual is available on <http://www.tno.nl/recipeport>

©TNO 2011

This manual is generated for informational purpose only. The user is allowed to freely copy and/or distribute this manual within the aforementioned purposes and provided the manual and its contents remain in full and unchanged. Without TNO prior written consent it is prohibited to submit this manual for any registration or legal purposes, advertising or negative publicity. Unauthorized or improper use of this manual or its content may breach intellectual property rights of TNO, for which your are responsible. Although TNO has exercised due care to ensure the correctness of the information as stated in the manual, TNO expressly disclaims any warranties on the contents. All content is provided “as is” and “as available”. Decisions which you take on the basis of this information will be at your own expense and risk.



