Risk assessment of multi-order dependencies between critical ICT infrastructures

Panayiotis Kotzanikolaou[1], Marianthi Theoharidou[2], and Dimitris Gritzalis[2]
[1]Dept. of Informatics, University of Piraeus,
85 Karaoli & Dimitriou, GR-18534, Piraeus, Greece
pkotzani@unipi.gr
[2]Dept. of Informatics, Athens University of Economics & Business,
76 Patission Ave., GR-10434, Athens, Greece
{mtheohar,dgrit}@aueb.gr

ABSTRACT

Assessing risk in information and communication infrastructures is a challenging topic due to the complexity of critical infrastructures (CIs) and of the various dependencies between such infrastructures. This chapter discusses the basic concepts of risk assessment for CIs. Moreover, it describes a recently proposed methodology for criticality assessment. The main goal of this methodology is to assess the risk of an infrastructure (or a sector of critical infrastructures), taking into account the dependencies between CIs and/or sectors. The methodology is compatible with current information systems practices. The basic characteristic of the presented methodology is that it attempts to capture both organization-oriented and society-oriented consequences of possible security events, a feature which is not always embedded in mainstream information security risk assessment methodologies.

INTRODUCTION

Although assessing security risk in critical information and communication infrastructures (CI) has similarities with risk assessment in traditional information systems, it also requires an extended approach, in order to capture CI complexities (Bialas, 2006). The process of assessing the impacts and the likelihood of occurrence of security incidents affecting CIs, is closely related to traditional information security risk assessment methods. It is also a basis for estimating which infrastructures are more critical than others, and, respectively, which sectors present higher criticality and require more sophisticated protective mechanisms. In the case of a potential threat affecting availability, but also information integrity or confidentiality of a CI, apart from the consequences to the infrastructure itself, a risk assessment methodology should mainly focus on possible impacts to the society. Risk assessment in CIs requires that the policy makers and security experts do consider possible societal impacts, which are external to the organization hosting a critical infrastructure (Theoharidou et al. 2010). An additional difficulty in risk assessment for CIs is the fact that these infrastructures are generally connected with many others and thus the effects of a disruption or failure may spread both geographically and across multiple sectors. The identification of 1st-order dependencies may be sufficient in order to assess the risk of a particular infrastructure; however, capturing 1st-order dependencies may fail in some cases to capture cascading risk to other infrastructures. For example, one or more relatively minor, security incidents on one CI may cause cascading and escalating impacts to a second or third dependent CI. Identifying multi-order dependencies leads to a more accurate assessment on the overall criticality level of an infrastructure or a sector, especially if we consider the social implications caused by the failure of a CI.

In this chapter, we describe the basic goals and outcome of a recent risk assessment methodology which aims to capture multi-order dependencies, and at the same time consider both organizational and societal effects, while assessing the risk of critical infrastructures (Theoharidou et al., 2009, 2010; Kotzanikolaou et al., 2011). The goals of the chapter are two-fold: (a) to assess the risk that a CI is exposed to, taking into account the presence of dependencies between infrastructures, and (b) to assess the risk of n–order dependencies between CIs. The aim of this method is to provide useful projections of the consequences of major security events, to security experts responsible for the protection of CIs. Since it also assesses the overall risk due to CI dependencies, it can be a useful tool for policy makers or national representatives to organizations dealing with CI protection. The ultimate goal is to provide a way to reduce the cumulative risk of security incidents and to avoid catastrophic cascading failures, by reducing threat, vulnerability, and/or impact levels, in the most appropriate and cost-efficient steps of a chain of dependent infrastructures.

ASSESSING RISK AND DEPENDENCIES

Traditional risk assessment methodologies for ICT systems, i.e. the ISO27005 standard, assess information risk only within the system or organization in question. They do not assess parameters such as the potential effect of a failure or disruption to dependent infrastructures or the impact to society. This is natural in the context of a single organization, since the management is interested to know what are the possible consequences (economical, business, legal or other) for the organization in question, in case of a security incident. Recent research on targeted to CIP risk assessment methodologies however, has indicated the need to also consider external effects. From a macroscopic view, what makes an infrastructure "critical" is the fact that it affects many others connected with it, who are mostly outsiders for the organization operating the CI. Thus, the criticality of an asset depends not only on the potential impact of a security incident on the operator of a CI, but also on the outgoing societal risk caused to other dependent organizations (Theoharidou et al., 2009).

A review on generic risk assessment methods for CIs (Theoharidou et al., 2009) indicates that such approaches assess risk in terms of threat, vulnerability and impact, with a high emphasis on the societal impact of a CI failure or disruption. However, they fail to model and assess the risk caused by the multi-order dependencies of CIs. Any modeling and simulation attempt faces several challenges, namely data accessibility, model development, and model validation. In the case of CI dependency, such a task is further complicated by the detailed and disparate cross sector analysis which is required (Pederson et al., 2006). The lack of reliable real-time data makes the identification of dependency related failures even worse (Andersson et al., 2005).

Dependencies and Failures

According to (Rinaldi et al., 2001; De Porcellinis et al., 2009), the dependencies may belong to the following categories:

- Physical (the state of a CI depends upon the material output(s) of the other CI),
- Cyber/Informational(the state of a CI depends on information transmitted through the other CI),
- Geographic (the state of a CI depends on an environmental event on another CI),

- Logical (the state of a CI depends upon the state of another CI via a non-physical, cyber, or geographic connection) or
- Social (the state of a CI is affected by the spreading of disorder to another CI related to human activities).

Also, while assessing the dependencies, one should not assume the complete availability or unavailability of a CI, as these may be available on different levels of quality (Nieuwenhuijs et al. 2008).

Rinaldi et al. (2001) classify dependence-related disruptions or outages in three types:

- A *cascading failure* is defined as a failure in which a disruption in an infrastructure A affects one or more components in another infrastructure, say B, which in turn leads to the partial or total unavailability of B.
- An *escalating failure* is defined as a failure in which an existing disruption in one infrastructure exacerbates an independent disruption of another infrastructure, usually in the form of increasing the severity or the time for recovery or restoration of the second failure.
- A *common-cause failure* occurs when two or more infrastructure networks are disrupted at the same time: components within each network fail because of some common cause. This occurs when two infrastructures are co-located (geographic interdependency) or because the root cause of the failure is widespread (e.g., a natural or a man-made disaster).

As summarized by Zio and Sansavini (2011), a more recent empirical study (Van Eeten et al., 2011), shows that events can been classified as "cascade initiating" (i.e., an event that causes an event in another CI), "cascade resulting" (i.e., an event that results from an event in another CI), and "independent" (i.e., an event that is neither a cascade initiating nor a cascade resulting event). The empirical findings indicate that: i) "cascade resulting" events are more frequent than generally believed, and that "cascade initiators" are about half as frequent; ii) the dependencies are more focused and directional than often thought; and iii) energy and telecommunication are the main "cascading initiating" sectors.

Related work in identifying and modeling dependencies includes the use of sector-specific methods, e.g. gas lines, electric grid or ICT, or more general methods that are applicable in various types of CIs. Interdependency models fall into six broad categories (Rinaldi, 2004; Zio and Sansavini, 2011; Kröger and Zio, 2011): (i) aggregate supply and demand tools, which evaluate the total demand for infrastructure services in a region and the ability to supply those services (ii) dynamic simulations, which examine infrastructure operations, the effects of disruptions, and the associated downstream consequences; (iii) agent-based models, which allow the analysis of the operational characteristics and physical states of infrastructures; (iv) physics-based models, which analyze physical aspects of infrastructures with standard engineering techniques (e.g., power flow and stability analyses for electric power grids or hydraulic analyses on pipeline systems); (v) population mobility models, which examine the movement of entities through geographical regions; and (vi) Leontief input-output models, which in the basic case provide a linear, aggregated, time-independent analysis of the generation, flow, and consumption of various commodities among infrastructure sectors.

Dependencies also vary according to the level of analysis selected. Different approaches have been used to examine dependencies under a *microscopic* or *macroscopic* view. De Porcellinis et al. (2009) refer to reductionistic and holistic approaches. A reductionistic approach identifies "elementary" components within a CI and then describes the evolution of the entire system based on the aggregated behavior of these components. For example, Svedsen and Wolthunsen (2007) focus on the components of a CI and they demonstrate several types of multi-dependency structures for both linear and particularly cyclical dependencies among multiple infrastructure types. Min et al. (2009) focus also on the component level, but they model two types of vulnerability: (a) structural and (b) functional. This approach calculates the interdependent effect and the effect of interdependence strength. The method is applied on power grid and gas pipeline models. Holistic examples include the study dependencies between different CIs (Nieuwenhuijs et al., 2008), within the same or different sectors of a country (Aung and Watanabe, 2009). A method to map dependencies with a workflow enabling the characterization of coupled networks and the emerging effects related to their level of dependency is presented by Rosato et al. (2008). This work aims at mapping the dependency between electrical and related communication nodes. Many holistic approaches apply Leontief's Inoperability Input-Output model (IIM), which calculates economic loss due to unavailability on different CI sectors based on their interdependencies (Aung and Watanabe, 2009; Santos and Haimes, 2004; Haimes et al., 2007; Setola et al., 2009). The same model is also applied by Crowther (2008), so as to include elements of business continuity and the cost to recover from an event.

A relevant risk management approach (Utne et al., 2011) follows six steps in order to model dependencies: (1) Identify the initiating event, (2) Identify interdependencies and Perform qualitative analysis, (3) Perform semi-quantitative assessment of the scenario, (4) Perform detailed quantitative analysis of interdependencies (optional), (5) Evaluate risk and measures to reduce interdependencies, and (6) Perform Cost/benefit analysis(optional).

Risk vs. Criticality

An extensive review on national strategies and risk assessment approaches for CIs (Theoharidou et al., 2009) indicates that these mainly focus on the *impact assessment* of an incident or threat, which usually results on the unavailability of a single CI. Impact is assessed under various terms, such as consequences, criticality, or vitality, and expressed with various criteria or factors. The potential effect usually takes the form of:

- Public Health & Safety
- Economic effect
- Environment
- Political effect or Governance or Mission
- Psychological or Social effect or Public Confidence
- Concentration of people
- Scope or Range
- Service Delivery or Recovery time
- National or Territorial security

Criticality assessment however seems to have a more broad scope than risk assessment, since it attempts to capture the external, societal impacts. In (Theoharidou et al., 2010), a method for assessing the criticality level of a CI is presented. It contains the following phases:

1. Identification of CI Components

2. Selection of Incidents - Threats
3. Partial Impact Assessment
4. Overall Criticality Assessment

Therefore, the Criticality of an infrastructure *I* can be assessed as the total Impact for every applicable combination of a component *c*, an incident-threat *th* and a resulting effect *e* to the infrastructure (*c,th,e*).

$$\text{Criticality}_I = \text{Impact}_I = \Sigma_{\forall(c,t,e)}\text{Impact}_I(c,t,e).$$

The sum operator is a generic operator and does not represent a numerical sum per se. Other possible operators may include max, average, median etc. This represents the common practice in most current criticality assessment approaches and it does not take into account the likelihood of incidents.

A more precise representation of the impact would be the following:
$\text{Impact}_i(t) = \alpha\text{Severity}_i(t) \text{ x } \beta\text{Scope}_i(t) \text{ x } \gamma\text{Time}_i(t)$, where $\alpha, \beta, \gamma \in [0,1]$, $\alpha + \beta + \gamma = 1$, and × is a generic multiplier (for example the use of Cartesian product).

These three attributes have all been included in existing approaches and can defined by various qualitative assessment criteria like the following (Theoharidou et al., 2009):

- Severity: Economic, Dependency, Public Confidence, International Relations, Public Order, Policy and Operations of Public Service, Safety, Defense.
- Scope: People affected, Concentration of people, Range.
- Time: Recovery Time, Duration.

Although these criteria are also used in risk assessment methodologies, in the case of CI assessment these criteria mainly refer to the *societal impact* of an incident. Thus they require significantly higher scales. We also observe that these three types of factors can be dependent on the time that an incident occurs. There may be points of time or time frames where the impact appears to be higher. Such time frames also need to be evaluated separately, since the risk deriving from the same event may be significantly different for different time periods. Thus, the security management plan should take into account different security risk which is time-dependent. As a consequence, different security controls must be considered for different time periods. However, if such time points or frames cannot be identified, then the above attributes are not time-dependent.

Many of the approaches discussed earlier (Aung and Watanabe, 2009; Santos and Haimes, 2004; Haimes et al., 2007; Setola et al., 2009) place the emphasis of an incident mainly on the potential impact, adopting the assumption that the likelihood of an event is less important when we deal with CIs. This means that we usually expect harmful incidents of relatively low likelihood, but significant impact to occur in CIs (Kröger, 2008; DHS, 2009). This also reflects the innate difficulty of assessing the likelihood of a threat/incident due to the lack of statistical data or previous incidents and due to the existing dependencies between CIs. A more complete approach would assess the overall Risk of an infrastructure *I* as follows:

(a) $\text{Risk}_I = \Sigma_{\forall(c,t,e)}(\text{Likelihood}(c,t,e) \text{ x } \text{Vulnerability}(c,t,e) \text{ x } \text{Impact}(c,t,e))$

(b) $\text{Risk}_I = \Sigma_{\forall(c,t,e)}(\text{Likelihood}(c,t,e) \text{ x } \text{Impact}(c,t,e))$

The approach (b) assumes that the assessment of likelihood takes into account the presence of vulnerabilities as well (ISO/IEC, 2008), in the sense that the presence of a vulnerability affects the occurrence likelihood of a threat. In this chapter we will adopt the second option, which means that the point of focus is the societal impact of an incident/threat and the effect of dependencies in risk assessment.

RISK ASSESSMENT METHODOLOGY FOR CI DEPENDENCIES

We observe that despite extensive research on the subject there is a lack of risk assessment methodologies which focus on critical information and communication infrastructures. The existing ones do not assess the risk that is based on the dependencies between them. The approach that follows attempts to identify the risk caused due to dependencies between different (Theoharidou et al., 2009, 2010; Kotzanikolaou et al., 2011). We adopt an holistic approach (De Porcellinis et al., 2009) meaning that we view each infrastructure as a single entity with well-defined boundaries and functional properties.

The method assesses risk in two stages. First, it attempts a more detailed -yet less complicated- assessment of *1st-order dependencies* between CIs. These means we examine pairs of infrastructures and their relationship. The analysis of 1st-order dependencies is performed in three levels of abstraction: (a) infrastructure level, (b) sector level, and (c) national/intra-sector level. The ultimate goal of this stage is to assess the dependency risk for each pair of infrastructure and then to assess the overall risk of an infrastructure or a sector, based on the dependency risk identified earlier. We then proceed in the assessment of the *n-order dependencies*, which allow the assessment of risk in chains of infrastructures and may highlight hidden information or dependencies that the initial assessment could not identify.

Some preparatory steps include the scope definition of the assessment. The decision maker needs to select (a) the sectors to be included in the assessment process (i.e. Finance, Government Services, ICT, Emergency, Energy, Health, Food, Transport, and Water) and (b) the CI which are considered important and, thus, should be included in the initial set. For each sector, an entity needs to act as sector coordinator, which will coordinate sector representatives, e.g. governmental agencies, expert groups, infrastructure representatives, etc. The use of experts for identifying dependencies between sectors has also been proposed by Setola et al. (2009). Since the criticality of the infrastructures has not yet been assessed, the initial selection is based on the assumptions and initial assessments of the representatives. For this reason, this initial set of infrastructures needs to be flexible and to be enriched and modified, if needed, in future steps.

Risk Assessment of 1st-order Dependencies

We examine the relation between two infrastructures ignoring the potential effect of a failure that affects multiple CIs or the effect of a chained reaction to an event. The methodology assesses risk in three layers: the infrastructure level, the sector level and, finally, the national/intra-sector level. We refer to infrastructures on an organizational level, which means we do not initiate the analysis at the component level, following the holistic perspective.

Infrastructure level

We assume that risk assessment results and security plans of CIs (based on standards, e.g. ISO (2008), NERC (2009)) are already available. This hypothesis means that the CI has identified all the assets, potential threats, and impacts and has calculated the risk for the particular infrastructure. Another assumption is that the CI has performed some form of vulnerability analysis for the ICT components. This assumption means that risk will be calculated as the product of threat likelihood and impact (ISO, 2008) in the following steps.

This level tries to identify potential points of dependency, where risk is transferred between infrastructures. It assumes that the 'owner' or the 'operator' of a CI has a better knowledge of the infrastructures he is dependent on for his function (these are called requisite CIs). All the dependencies are identified and then assessed in the following way:

Step 1: Identify all the requisite CIs and the corresponding dependencies. For each dependency the following elements need to be identified:

a) Dependency type (physical, cyber, geographic, logical and social),
b) Source impact of the dependency (unavailability, disclosure, modification), i.e. the impact caused to the requisite organization due to a security incident,
c) Incoming impact (unavailability, disclosure, modification), i.e. the impact caused to the CI in question, due a source impact realized in a requisite CI,
d) Type of incoming impact (financial loss, safety, loss of service, legal consequences etc.),
e) Scale of incoming impact (very low, low, medium, high, very high), and
f) Likelihood of incoming impact (very low, low, medium, high, very high).

The types (d) and scale (e) provide a qualitative assessment of the incoming impact, which combined with the likelihood (f), allow the assessment of the *incoming dependency risk* in step 2.

Step 2: Estimate the incoming risk. For each infrastructure CI$_j$ estimate the incoming risk that CI$_i$ is exposed to, due to its dependency from each possible requisite infrastructure CI$_i$, i.e. $r_{i,j} = I_{i,j} \times L_{ij}$. The following risk matrix is used for the computation of $r_{i,j}$.

		Likelihood				
		Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Impact	Very Low	1	2	3	4	5
	Low	2	3	4	5	6
	Medium	3	4	5	6	7
	High	4	5	6	7	8
	Very High	5	6	7	8	9

Table 1: Incoming risk matrix (Theoharidou et al., 2009)

Step 3: Create the incoming dependency risk matrix for each CI.
This risk matrix is called an incoming dependency risk matrix, because it is risk that arises as a consequence of impact external to the examined CI.

In the case of multiple dependencies, then the total incoming dependency risk DR$_{i,j}$ for CI$_i$ from CI$_j$ needs to be calculated. There are two simple approaches in regards of assessing overall risk: (a) average risk or (b) maximum risk. Adopting the first approach allows us to perform better cost benefit analysis, but we may lose important information when large variations occur. Alternatives include assessing the median risk. Contrary, the second approach focuses on a worst case scenario, which usually leads to more expensive risk treatment plans, but high valuations of risk are not omitted. We adopt the second approach (worst-case principle); the total incoming dependency risk DR_j of an infrastructure CI_j is calculated as the maximum of all incoming dependency risk factors $r_{i,j}$, for each requisite infrastructure CI_i of the examined infrastructure CI_j, i.e.:

$$DR_{i,j} = \max \{r_{i,j}\}, \forall (i,j)$$

Sector level

At this level, the input is provided not only by CIs but from sector representatives as well, who have a better overview of potential dependencies. At this stage, dependencies, which (a) have been identified at the previous level and (b) new ones that may be highlighted by sector representatives, are assessed, but the main difference is that the risk does not refer to the infrastructure itself but to the society in general. Here we assess the outgoing risk of an infrastructure, meaning that we estimate the societal impact of an incident or threat on other infrastructures (dependent CIs) and the society.

Step 1: Identify the dependent CIs and the corresponding dependencies.

For each dependency the following elements need to be identified:

(a) Dependency type (physical, cyber, geographic, logical and social),
(b) Source impact of the dependency (unavailability, disclosure, modification), i.e. the impact caused to the CI in question due to a security incident,
(c) Outgoing societal impact (unavailability, disclosure, modification), i.e. the impact caused to the dependent CI, due to the above source impact,
(d) Type (Economic, Public Confidence, International Relations, Public Order, Policy & Operations of Public Service, Safety, Defense etc.) of outgoing societal impact,
(e) Scale of outgoing societal impact (very low, low, medium, high, very high), and
(f) Likelihood of outgoing societal impact (very low, low, medium, high, very high) due to dependencies

The types (d) and scale (e) provide a qualitative assessment of the outgoing societal impact, which combined with the likelihood (f), allow the assessment of the outgoing societal risk in step 2.

Step 2: Estimate the outgoing societal risk of an infrastructure.

For each infrastructure CI_i estimate the *outgoing societal risk $sr_{i,j}$* that CI_i causes to its dependent CI_j, i.e. $sr_{i,j} = I_{i,j} \times L_{ij}$.

One should note that the incoming dependency risk and the outgoing societal risk are two complementary variations of the same concept, i.e. the risk exhibited due to a connection between two CIs. Their basic difference is the different perspective in the target of the impact. The estimation of the incoming dependency risk is computed by each organization that is in the right side of a dependency and its main purpose is to capture incoming risk for an infrastructure. It is natural to assume that each CI will be able to assess its potential risk from its requisite organizations. On the other hand the societal outgoing dependency risk is computed not by the organization in question, but from sector-wise experts. Again, it is natural to assume that governmental or regulatory bodies will be more capable to focus on potential risks deriving from CI dependencies that will impact the society and not each particular CI. Such risk factors are usually out-of-the-scope of organization-wide risk assessments, where each CI would be interested in estimating its own risk and not the risk it may cause to others.

The computation of the societal risk uses a different risk matrix that the one used on the infrastructure level, as the impact does not refer only to the examined infrastructure but to the society as well and thus the potential impact is of higher level (see Table 2).

		Likelihood				
		Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Impact	Very Low	2	3	4	5	6
	Low	3	4	5	6	7
	Medium	4	5	6	7	8
	High	5	6	7	8	9
	Very High	6	7	8	9	9

Table 2: Societal risk matrix (Theoharidou et al., 2009)

In the case of multiple dependencies, then the total societal risk SR_i for each examined infrastructure CI_i is calculated as the maximum of all outgoing societal risk factors $sr_{i,j}$. for each possible dependent infrastructure CI_j, i.e.:

$$SR_{i,j} = \max \{sr_{i,j}\}, \forall (i,j)$$

This risk can be represented in a graph, like the following.

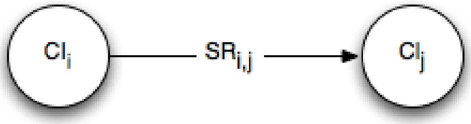

Figure 1. Graph representation of Societal Risk

An infrastructure is denoted as a circle. An arrow from CI_i → CI_j denotes a risk dependency, i.e. a dependency risk from the infrastructure CI_i to the infrastructure CI_j. A bi-directional arrow CI_i ←→ CI_j denotes a dependency risk from CI_i to CI_j and another one from CI_j to CI_i. The number on each arrow refers to the level of the societal risk from CI_i to CI_j due to the dependency, i.e. the likelihood of a disruption from CI_i to cascade to CI_j, as well as the impact in the case of such an event, not to the infrastructure $CI_{j,}$ but to the society. This is why this assessment cannot be performed solely but the 'owner' or 'operator' of the particular CI, but the participation of sector coordinators or multiple CI 'owners' is needed.

Step 3: Estimate the inherent societal risk of each CI.
The disruption of an infrastructure may pose risk to the society regardless of dependencies. We refer to the inherent societal risk for each CI_i, i.e. SR_i.

Step 4: Estimate overall incoming, outgoing societal risk (ISR_i, OSR_j).
Based on the results of step 2, the sector coordinators can calculate the overall incoming and outgoing societal risk for each CI. In order to calculate the overall societal risk that

occurs due to dependencies, there are many operators that can be used, i.e. max, average, median, standard deviation etc. If we select the average operator and n is the number of CIs studied, r_{max} is the maximum valuation of $SR_{i,j}$ (in our example risk ranges from 2 to 9, see Table 2), then the average incoming societal risk ISR_i for CI_i is calculated as follows:

$$ISR_i = \frac{1}{(n-1) * r_{max}} \sum_{\forall i \neq j}^{n} DR_{i,j}$$

Similarly, the average outgoing societal risk OSRj is calculated as follows:

$$OSR_j = \frac{1}{(n-1) * r_{max}} \sum_{\forall j \neq i}^{n} SR_{i,j}$$

National/ Intra-sector level

During this layer, the sector coordinators will re-examine all the results of the previous layers in order to identify and confirm the dependencies between CIs and form a more macroscopic view than the one in the sector level. Ultimate goal is to identify which sectors are more critical than others.

Step 1: Calculate overall risk for each CI.

We consider that a CI is critical for the society, when the CI has high societal risk:

(a) due to inherent societal risk (SR_i) or

(b) due to outgoing societal risk that occurs due to dependencies (OSR_i).

The overall risk of a CI_i is calculated as a function of these two parameters: R_i = f(OSR_i, SR_i). The function f can vary. For example, if the decision makers do not consider both parameters as equally important, they can use a weighted sum to represent function f.

Step 2: Calculate overall risk for each sector.

In order to calculate the risk of each sector, we need to calculate the overall societal risk for each one of them. If we adopt the worst case scenario principle and l, k are CIs belonging to the sectors S_i and S_j respectively, then the overall societal risk from sector S_i to sector S_j is:

$$SR_{S_i,S_j} = \max_{\forall k \in S_i, \forall l \in Sj, Si \neq Sj} \{SR_{k,l}\}$$

If m is the number of sectors, then the average incoming and outgoing societal risk for sector Si are:

$$ISR_{S_i} = \frac{1}{(m-1) * r_{max}} \sum_{Si \neq Sj} SR_{S_i,S_j}$$

$$OSR_{S_i} = \frac{1}{(m-1) * r_{max}} \sum_{Si \neq Sj} SR_{S_j,S_i}$$

Similarly, other operators can be considered. If n_i is the number of the CIs of the sector Si, then the average overall inherent societal risk is:

$$SR_{S_i} = \frac{1}{n_i} \sum_{\forall j \in S_i} SR_j$$

This way, we can identify which sectors are more critical for the society. A sector's risk depends on the societal risk of its members, and on the societal risk of its dependencies. Therefore, the overall risk R_{Si} of a sector S_i, is calculated as a function R_{Si}= f (OSR_{Si}, SR_{Si}).

Example

An example of 5 infrastructures belonging to 4 sectors (Finance, ICT and Energy, Government) is presented:

- CI$_A$: a banking institution, which belongs in the finance sector. It provides a full range of financial products and services for corporate customers and private individuals, including investment banking services, brokerage, insurance, asset management, leasing and factoring.
- CI$_B$: an electric energy provider (energy sector). This infrastructure produces and transfers energy for a significant portion of the national market (>90%).
- CI$_C$: an information and communication infrastructure which offers network services in a national level for all public organisations (ICT sector).
- CI$_D$: a provider which offers communication services (landline, mobile, internet) and belongs to the ICT sector.
- CI$_E$: a health and insurance institution, which belongs in the government sector. This information and communication infrastructure offers e-services and transactions for citizens.

During the infrastructure level, the operators of the 5 CIs identified the dependencies between them. On the sector level, sector experts and representatives of the operators assessed the following societal risks deriving from each identified dependency (see Table 3). For each dependency, the case of an unavailability incident affecting the availability of another CI was examined.

CI	Dep. Type	Description	Societal Impact	$I_{j,i}$	$L_{j,i}$	$SR_{j,i}$
CI$_A$ (Finance Sector)						
CI$_E$	C	Provides payment services	Public Confidence	L	L	4
CI$_B$ (Energy Sector)						
CI$_A$	P	Provides power services	Economic Impact	VL	L	3
CI$_C$	P	Provides power services	Public Confidence	H	VL	5
CI$_D$	P	Provides power services	Economic Impact	VH	VL	6
CI$_E$	P	Provides power services	Public Confidence	L	L	4
CI$_C$ (ICT Sector)						
CI$_E$	C	Provides network services	Public Confidence	L	VL	3
CI$_D$ (ICT Sector)						
CI$_C$	P	Provides network connectivity	Public Confidence	H	VL	5

Table 3: Societal risks due to dependencies

The dependencies are also graphically depicted in Figure 2.

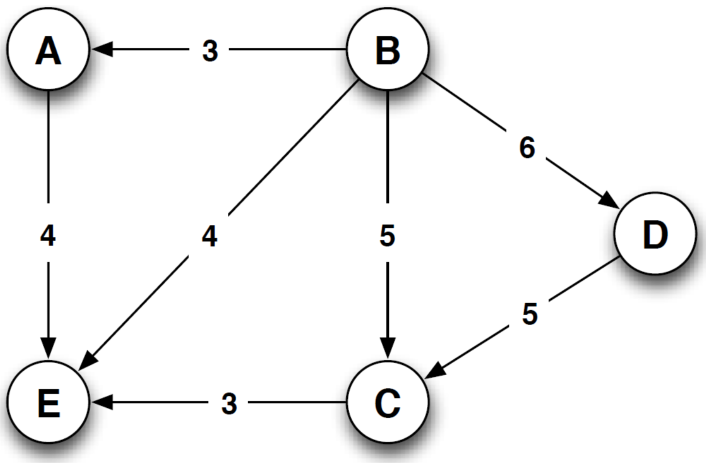

Figure 2. An example of five dependent infrastructures.

The overall incoming and outgoing societal risks were calculated by using the avg and max operator (see Table 4).

CI		CI_A	CI_B	CI_C	CI_D	CI_E	ISR_i	
							AVG	MAX
	CI_A		3				0,083	0,333
	CI_B						0,000	0,000
	CI_C		5		5		0,278	0,556
	CI_D		6				0,167	0,667
	CI_E	4	4	3			0,306	0,444
OSR_i	AVG	0,111	0,500	0,083	0,139	0,000		
	MAX	0,444	0,667	0,333	0,556	0,000		

Table 4: Overall societal risks due to dependencies

The sector representatives also assessed the inherent societal risk of each infrastructure in the case of unavailability. The results are presented in the table that follows.

CI	Societal Impact		Likelihood	Inherent SR_i
CI_A Banking services to 10% of the population	Economic Impact	L	VL	3
CI_B Energy to the 99.7% of the population	Public Confidence	VH	L	7
CI_C Network services to all public organizations	Public Confidence	H	L	6
CI_D Landline telecommunication services to 60% of the citizens	Public Confidence	VH	VL	6
CI_E Insurance services to 50% of the population	Economic Impact	M	L	5

Table 5: Inherent societal risks

At a national level, for the outgoing societal risk (OSR_i) and the inherent societal risk (SR_i) of each infrastructure, the average operator was selected. The decision maker considered these two parameters as equally important and he evaluated the risk of a CI as $R_i = αOSR_i + βSR_i$, where $α= β = 0,5$.

CI	CI_A	CI_B	CI_C	CI_D	CI_E
OSR_i (AVG)	0,111	0,500	0,083	0,139	0,000
SR_i	0,333	0,778	0,667	0,667	0,556
R_i	0,222	0,639	0,375	0,403	0,278

Table 6: Overall risks of each infrastructure

Note that, although the overall risk gives us insight of the importance of a CI, it is also important to assess the partial risk values. For example, CI_E has the least outgoing societal risk but due to its high level of inherent societal risk (SR_E), it should not be considered as the least important CI.

Similarly, aggregated results can be derived for each sector. The table that follows presents (a) the average and maximum incoming and outgoing risk of each sector (ISR_{Si}, OSR_{Si}), i.e. the risks that occur due to dependencies,
(b) the inherent societal risk of each sector.

Sector	Finance	Energy	ICT	Government	ISR_{Si}	
					AVG	MAX
Finance		3			0,111	0,333
Energy					0,000	0,000
ICT		6			0,222	0,667
Government	4	4	3		0,407	0,667
OSR_{Si} AVG	0,148	0,481	0,111	0,000		
MAX	0,444	0,667	0,333	0,000		
SRSi	0,333	0,777	0,666	0,666		

Table 7: Overall sector risks (incoming, outgoing, inherent)

Based on the outgoing societal risk and the inherent societal risk of each sector, its overall risk can be also calculated, following an equivalent procedure as the one depicted in Table 4.

Summary

At the infrastructure level, dependencies are identified. At the sector level, the expected incoming and outgoing societal risk associated with each CI belonging to the sector, are estimated by the sector coordinator. Finally, at the intra-sector/national level, the dependency and societal risk of all sector members are considered, in order to compare the criticality between sectors. It should be highlighted that a decision maker is responsible for (a) selecting the infrastructures and sectors to include in the assessment set, (b) assessing the risk parameters, i.e. defining the risk matrices, (c) selecting the scales to be used for the assessment.

Risk Assessment of N-order Dependencies

During this phase, the goal is to assess the second-order and more generally, n-order dependencies of a CI_i.

In the previous stage, we have already identified all the incoming societal risk of CI_i. For simplicity, and without loss of generality, we assume that the incoming societal risk $CI_j \rightarrow CI_i$ has risk value $R_{j,i} = L_{j,i} \times I_{j,i}$, where $I_{j,i}$ is the societal impact and $L_{j,i}$ is the likelihood of this impact to occur.

For example, as shown in Figure 2, the infrastructure E has an incoming dependency from A and another one from B.

Preliminaries and Definitions

Let **CI**= (CI_1,...,CI_m) be the set of all the examined infrastructures. In the example it would be **CI**= (CI_A, CI_B, CIc, CI_D, CI_E).

Definition 1: (Probability of the unavailability event) Let E_U^j be an event realized to the infrastructure $CI_j \in$ **CI** that causes unavailability to CI_j. If $\Pr\left(E_U^j\right) = p_j$ then the probability that the infrastructure CI_j will remain available, denoted as $Pr(CI_j)$, is computed as:

$$Pr(CI_j) = 1 - p_j \qquad (1)$$

Obviously, an infrastructure CI_j will become unavailable, if $Pr(CI_j) = 0$. Let CI_i, CI_j be two infrastructures that are directly connected as $CI_i \rightarrow CI_j$. Since the infrastructures are directly connected and we examine cascading effects, the events E_U^j and E_U^j are statistically dependent.

Definition 2: (Probability of 1st-order cascading events) The probability that CI_j is unavailable due to an unavailability event realized in CI_i, denoted as $Pr(CI_{i,j})$ is computed by the conditional probability:

$$Pr\left(CI_{i,j}\right) =(Pr\left(CI_j\right) =0 \,/\, Pr(CI_i) =0) \qquad (2)$$

Computing such probabilities is not easy, since usually it is not possible to quantify unavailability events (e.g. by having access to creditable statistical data). However, it is more practical for each infrastructure CI_j to provide a qualitative *conditional degree of belief*, in order to assess the likelihood of a cascading unavailability event caused in its directly connected infrastructure CI_i, to eventually cause unavailability to CI_j.

Definition 3: (Likelihood of 1st-order cascading events) The likelihood $L_{i,j}$ is defined as the conditional degree of belief that CI_j will become unavailable, due to the unavailability realized in CI_i.

The likelihood $L_{i,j}$ can take one of the following qualitative values {VL, L, M, H, V} (from Very Low to Very High). Note that the likelihood $L_{i,j}$ does not provide any metric of the impact value that CI_j will suffer due to the realization of the joint event. For example, if CI_j depends (for redundancy) on two network providers, then the unavailability of one provider will possibly lead to a partial unavailability impact to CI_j (e.g. service degradation). The incoming impact value of each dependency $CI_i \rightarrow CI_j$ is captured by the value $I_{i,j}$.

Definition 4: (Impact level of 1st-order cascading events) The impact $I_{i,j}$ is defined as the qualitative (societal) impact value that the infrastructure CI_j will suffer, if the joint unavailability event $Pr(CI_{i;j})$ is realized. The impact $I_{i,j}$ takes one of the qualitative values {VL, L, M, H, V}. Note that these values can be assigned to ranges of economic loss or any other loss (e.g. level of affect of public confidence). The incoming societal risk is simply defined as the Cartesian product of the likelihood and the impact level (see Table 2).

Definition 5: (Risk of 1st-order cascading events) Let CI_i, CI_j be two infrastructures that are directly connected, $L_{i;j}$ be the likelihood of the 1st-order cascading event and $I_{i,j}$ be the relative impact. Then the societal risk level of the dependency $CI_i \rightarrow CI_j$ is defined as:

$$SR_{i,j} = L_{i,j} \text{ x } I_{i,j} \qquad (3)$$

For example, as shown in Table 3, CI_A has one dependent CI, the CI_E. The infrastructure CI_E has a Cyber (or Informational) dependency from CI_A, since CI_E has outsourced its payment services to CIA. A possible service unavailability of CI_A will produce an incoming societal impact to CI_E (unavailability of its payment services), denoted as $I_{A,E}$. This would cause loss of public confidence to CI_E, of a relatively low impact, i.e. $I_{A,E}$ = L. The likelihood of an event causing unavailability to CI_A (and consequently a cascading unavailability to CI_E) is considered low, i.e. $L_{A,E}$ = L. Thus, the outgoing risk of this dependency, denoted as $SR_{A,E} = L_{A,E} \text{ x } I_{A,E}$ has a risk value equal to 4, based on the risk matrix of Table 2. The example considers total loss of availability as a source impact, while the incoming impact is given by the value $I_{A,E}$, i.e. in the above example we consider that if the source suffers total unavailability, then the destination will suffer unavailability of a relatively low impact. However, it is easy to construct modified matrices to assess modified levels of service loss at the source infrastructure.

Extending to n-order dependencies

By using the above definitions of 1st-order dependencies, we will extend this model in order to capture the likelihood of n-order cascading events and the relative risk factors. Let **CI** = $(CI_1,\dots,CI_m)$ be the set of all the examined infrastructures. Let $CI_{Y0} \rightarrow CI_{Y1} \rightarrow \dots \rightarrow CI_{Yn}$ denote a chain of connected infrastructures of length n. Since we examine cascading events, the events $E^{U}_{Y_i}$, i= 0,1,…,n are statistically dependent. By extending Definition 2 and equation 2 we have:

Definition 6: (Probability of n-order cascading events) The probability that CI_{Yn} is unavailable due to cascading unavailability events realized in CI_{Y0}, CI_{Y1}, …, CI_{Yn-1} denoted as $Pr(CI_{Y0,Y1,\ldots,Yn})$ is computed by the joint event of the conditional probabilities as:

$$\Pr\left(\mathrm{CI}_{\mathrm{Y}_{0,}\mathrm{Y}_{1,\ldots,}\mathrm{Y}_{\mathrm{n}}}\right) \equiv \cap_{\mathrm{i}=0}^{\mathrm{n}}\{\Pr(\mathrm{CI}_{\mathrm{Y}_\mathrm{i}}) = 0\} = \Pr(\mathrm{CI}_{\mathrm{Y}_0} = 0)\prod_{\mathrm{i}=1}^{\mathrm{n}-1}\{\Pr(\mathrm{CI}_{\mathrm{Y}_{\mathrm{i}+1}}) = 0 \mid \Pr(\mathrm{CI}_{\mathrm{Y}_\mathrm{i}}) = 0\} \quad (4)$$

Following the same approach as in Definition 3, instead of using conditional probabilities, we will use the qualitative *conditional degrees of belief*, computed for each 1st-order cascading event $L_{Yi,Yi+1}$, I = 0, 1, …, n-1.

Definition 7: (Likelihood of n-order cascading events) The likelihood that CI_{Yn} will become unavailable due to cascading unavailability events realized in CI_{Y0}, CI_{Y1}, …, CI_{Yn-1} is computed as:

$$\mathrm{L}_{\mathrm{Y}_0,\ldots,\mathrm{Y}_\mathrm{n}} = \prod_{\mathrm{i}=0}^{\mathrm{n}-1}(\mathrm{L}_{\mathrm{Y}_\mathrm{i},\mathrm{Y}_{\mathrm{i}+1}}) \quad (5)$$

The product of equation 5 is an empirical multiplication value. The heuristic justification of equation 5 stems from the analogy between conditional degrees of belief and conditional probabilities. Since each $L_{Yi,Yi+1}$ is a conditional degree of belief, then the joint event is simply the product of all the conditional degrees of belief. The risk exhibited by CI_{Yn} due to its n-order dependency is defined bellow, based on Definitions 4 and 7:

Definition 8: (Societal risk of n-order cascading events) Let CI_{Y0} → CI_{Y1}→…→CI_{Yn} be a chain of dependencies, $L_{Y0,\ldots Yn}$ be the likelihood of the n-order cascading event and $I_{Y0,\ldots Yn}$ be the impact of the CI_{Yn-1} → CI_{Yn} dependency. Then by combining equations 3 and 5, the cascading societal risk exhibited by CI_{Yn} due to the n-order dependency is computed as:

$$\mathrm{SR}_{\mathrm{Y}_0,\ldots,\mathrm{Y}_\mathrm{n}} = \mathrm{L}_{\mathrm{Y}_0,\ldots,\mathrm{Y}_\mathrm{n}} \cdot \mathrm{I}_{\mathrm{Y}_{\mathrm{n}-1},\mathrm{Y}_\mathrm{n}} = \prod_{\mathrm{i}=0}^{\mathrm{n}-1}(\mathrm{L}_{\mathrm{Y}_\mathrm{i},\mathrm{Y}_{\mathrm{i}+1}}) \cdot \mathrm{I}_{\mathrm{Y}_{\mathrm{n}-1},\mathrm{Y}_\mathrm{n}} \quad (6)$$

The cumulative societal risk should consider the overall risk exhibited by all the CI's within the sub-chains of the n-order dependency. This is defined bellow, based on equations 5 and 6:

Definition 9: (Cumulative societal risk) Let CI_{Y0} → CI_{Y1}→…→CI_{Yn} be a chain of dependencies of length n. The cumulative societal risk, denoted as, is defined as the overall risk produced by an n-order dependency, computed by the following equation:

$$RISK_{\mathrm{Y}_0,\ldots,\mathrm{Y}_\mathrm{n}} = \sum_{\mathrm{i}=1}^{\mathrm{n}}(\prod_{\mathrm{j}=1}^{\mathrm{i}} \mathrm{L}_{\mathrm{Y}_\mathrm{i},\mathrm{Y}_{\mathrm{i}+1}}) \cdot \mathrm{I}_{\mathrm{Y}_{\mathrm{i}-1},\mathrm{Y}_\mathrm{i}} \quad (7)$$

The proposed algorithm

In order to assess the cumulative n-order societal risk factors, we will examine and assess each possible chain of dependencies. For this reason, we define the recursive algorithm described below, which has the following steps: (a) examine each infrastructure as the root of dependency chain(s), (b) construct the chain(s) of its n-order dependencies and (c) assess the societal risk of each chain. Let **CI** = (CI_1,...,CI_m) be the set of all the examined infrastructures. Without loss of generality, we denote as $\mathrm{CI}_{\mathrm{Y}_0}$ the infrastructure which has the role of the examined infrastructure in each round of the algorithm (i.e. it has the role of the root of a dependency chain) and we denote as $\mathrm{CI}_{\mathrm{Y}_{\mathrm{j}}}, \mathrm{j} = 1, \ldots, \mathrm{n}$ an infrastructure which is in the j-th position of a dependency chain with $\mathrm{CI}_{\mathrm{Y}_0}$ as the root.

Obviously, the algorithm will be run m times, once for each member of CI as the root of dependency chain(s). Without loss of generality, we considered the dependency chain $\mathrm{CI}_{\mathrm{Y0}}$ → $\mathrm{CI}_{\mathrm{Y1}}$→…→$\mathrm{CI}_{\mathrm{Yn.}}$

1. **Identification of the** 1st**-order dependencies of $\mathbf{CI_{Y0}}$.** Identify all the outgoing dependency risk of $\mathrm{CI}_{\mathrm{Y}_0}$. For simplicity, and without loss of generality, we assume that a 1st-order outgoing risk $\mathrm{CI}_{\mathrm{Y}_0} \rightarrow \mathrm{CI}_{\mathrm{Y}_1}$has risk value $\mathrm{SR}_{\mathrm{Y}_0,\mathrm{Y}_1 =} \mathrm{L}_{\mathrm{Y}_0,\mathrm{Y}_1} \cdot \mathrm{I}_{\mathrm{Y}_0,\mathrm{Y}_1}$, where $\mathrm{I}_{\mathrm{Y}_0,\mathrm{Y}_1}$ is the incoming impact for $\mathrm{CI}_{\mathrm{Y}_1}$ (due to its 1st-order dependency from $\mathrm{CI}_{\mathrm{Y}_0}$) and $\mathrm{L}_{\mathrm{Y}_0,\mathrm{Y}_1}$ is the likelihood of this event. For example, if CI_B in Figure 2 is examined as the root infrastructure $(\mathrm{B} \equiv \mathrm{Y}_0)$ then CI_B has four 1st-order dependencies. We examine the dependency CI_B → CI_D and thus, $\mathrm{D} \equiv \mathrm{Y}_1$ (in a real implementation, each 1st-order dependency would be examined as a separate thread). Then, based on Table 3 it holds that $\mathrm{I}_{\mathrm{Y}_0,\mathrm{Y}_1} \equiv \mathrm{I}_{\mathrm{B,D}} = \mathrm{VH}$ and $\mathrm{SR}_{\mathrm{Y}_0,\mathrm{Y}_1} \equiv \mathrm{SR}_{\mathrm{B,D}} = \mathrm{VL}$.

2. **Identification of the** n**-order dependencies of** $\mathrm{CI}_{\mathrm{Y}_0}$**.** During this step, we identify the correlated 2nd and more generally, n-order dependencies of $\mathrm{CI}_{\mathrm{Y}_0}$. For each 1st-order dependency $\mathrm{CI}_{\mathrm{Y}_0} \rightarrow \mathrm{CI}_{\mathrm{Y}_1}$ of the examined infrastructure $\mathrm{CI}_{\mathrm{Y}_0}$, examine the infrastructure $\mathrm{CI}_{\mathrm{Y}_1}$, in order to identify its possible outgoing dependencies $\mathrm{CI}_{\mathrm{Y}_1} \rightarrow \mathrm{CI}_{\mathrm{Y}_2}$.

In the example of Figure 2, for the CI_B → CI_D dependency identified in step 1, we examine the 2nd-order dependency CI_D → CI_C. By examining Table 3, the 2nd-order dependency is marked and we continue by examining possible 3rd-order dependencies. By following the same approach, we can see that CI_E has an incoming dependency from CI_C and thus $\mathrm{E} \equiv \mathrm{Y}_3$. Since no infrastructure has an incoming dependency from CI_E, the examined thread is a 3rd-order dependency. When this thread has finished, the algorithm will continue to examine all the possible n-order dependency threads. In practice, the algorithm can stop in the 4th-order dependency. Recent results (see for example Zio and Sansavini (2011)) have shown that the effect of dependencies grater that 4th-order are negligible. By examining Figure 2 we can continue until all the possible dependency threads of CI_B have been exhausted.

3. **Evaluation of the** n**-order cumulative dependency risk.** Check if a $\mathrm{CI}_{\mathrm{Y}_1} \rightarrow \mathrm{CI}_{\mathrm{Y}_2}$ dependency has been marked in the previous step. In this case, continue until the last marked dependency is found. Then, the cumulative n-order dependency risk of this dependency chain can be computed by using equation 7.

4. **Examine next infrastructure.** Repeat from step one until all the examined infrastructures are exhausted.

5. **Rank cascading risk.** Rank all the examined cascading risk and choose the most critical paths (according to a risk threshold set by the security experts).

6. **Mitigate cascading risk.** Consider risk mitigation controls throughout the path under a cost-benefit analysis, in order to reduce the dependency risk below the threshold, both on a sector and an infrastructure level. The examination of n-order dependencies allows the identification of the most critical infrastructures and their respective sectors in terms of chain effects. The examination of the risk path provides additional options for risk mitigation, in a 'cost-efficient' way. For example, the alternative risk mitigation approaches include:

- Controls to reduce the likelihood of the possible events that may cause the source impact in the source of the examined dependency chain.
- Controls that reduce the likelihood of the possible events that cause the source impact in any intermediate node within the chain.
- Controls that reduce the impact of dependencies by creating alternative paths. Controls that increase the resilience of critical nodes in a dependency chain, thus reducing the impact on individual nodes.

When planning investments for critical infrastructures or sectors, the information provided by the dependency graphs and n-order dependencies can be significant. This is due to the fact that adopting such a macroscopic view permits a more efficient distribution of budget within or across sectors. It also reduces the cost of applying excessive countermeasures on all infrastructures, while it increases their effectiveness, not only in respect of the particular infrastructure, but of the dependent ones as well.

CONCLUSIONS AND FUTURE WORK

This chapter focuses on risk assessment of multi-order dependencies between CIs and presents some recent research results on the field. The methodology described in this chapter examines the risk of dependency in two stages: (a) 1st-order dependencies, where infrastructures and sectors and considered as pairs, and (b) n-order dependencies, where infrastructures are viewed as chains.

The main concept of this method is to first identify the more obvious and easy to capture 1st-order dependencies, and then proceed in their potential multi-order effect. The methodology examines how threats and their impact can be transferred by one infrastructure to another, following the holistic approach (De Porcellinis et al., 2009). This makes the methodology realistic and applicable, as the initial input for identifying dependencies can be based on existing security plans or service level agreements, an approach which is compatible both with the directives of the European Council (2008) and with current best practices (ISO, 2008; NIST, 2008). In terms of the sector level, the methodology emphasizes on the societal risk, which is usually out of scope or underestimated, during traditional organizational-oriented risk assessments. It allows the decision maker to assess the criticality of sectors as well, in a similar way as the various techniques of the IIM model (Aung and Watanabe, 2009; Haimes et al., 2007; Setola et al., 2009).

Then, the dependencies are further examined in order to identify potential cascading effects. The method provides a way to use the dependency graphs created in the first stage, in order to build chains of dependencies for each individual CI and assess the effects in a series of infrastructures. This allows for more knowledgeable risk mitigation, which can be further extended to a sector basis as well.

This methodology can be proved exhaustive, especially as the number of analyzed infrastructures increases. A realistic application of the method would focus on selected number of infrastructures or sectors, which are considered important on a strategic, national level. Like most qualitative risk assessment methods, subjectivity can be introduced during the risk assessment method. Obviously, in our method the accuracy of the result depends on the initial assessments of the CI representatives or the sector coordinators, since their assessments are used for the calculation of the overall risk.

Future steps include the further analysis of the dependency graphs in order to identify cycles and reverse dependencies. The automated analysis of parallel paths can also give insight towards more efficient risk management. Also, we plan to adopt graph analysis algorithms, in order to identify the most critical paths of dependencies, and to provide ways to reduce risk by exploring alternative paths in a dependency graph.

ACKNOWLEDGEMENTS

This work was supported in part by the S-Port (09SYN-72-650) project, which is funded by the Hellenic General Secretariat for Research & Technology, under the Synergasia Programme. We would also like to thank the anonymous reviewers for their helpful comments and suggestions.

KEY TERMS AND DEFINITIONS

Critical Infrastructure (CI): an asset, system or part which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact [in a Member State] as a result of the failure to maintain those functions.

Criticality: the *contribution level* of the infrastructure to the society in maintaining a minimum quality level of vital societal functions, health, safety, security, economic or social well-being of people, or the *impact level* to the society from the disruption or destruction of the CI.

Dependency: A linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other.

Risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the CI.

Risk assessment: the process to determine the value of the information assets, to identify the applicable threats and vulnerabilities that exist (or could exist) and to determine the potential consequences, in order to finally prioritize the derived risk.

REFERENCES

Andersson, G., Donalek, P., Farmer, R., Hatziargyriou, N., Kamwa, I., Kundur, P., Martins, N., Paserba, J., Pourbeik, P., Sanchez-Gasca, J., Schulz, R., Stankovic, A., Taylor, C., & Vittal, V. (2005). Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance. *IEEE Transactions on Power Systems*, *20*(4), 1922-1928.

Aung, Z., & Watanabe, K. (2009). A framework for modeling Dependencies in Japan's Critical Infrastructures. In Palmer C., Shenoi S. (Eds.), *3rd IFIP International Conference on Critical Infrastructure Protection (CIP-2009)* (pp. 243-257). Springer, USA.

Bialas, A. (2006). Information security systems vs. critical information infrastructure protection systems - Similarities and differences. In *Proc. of the Int. Conf. on Dependability of Computer Systems* (pp.60-67).

Crowther, K.G. (2008). Decentralized risk management for strategic preparedness of critical infrastructure through decomposition of the inoperability input-output model. *International Journal of Critical Infrastructure Protection*, *1*, 53-67.

De Porcellinis, S., Oliva, G., Panzieri, S., & Setola, R. (2009). A Holistic-Reductionistic Approach for Modeling Dependencies. In C. Palmer, S. Shenoi (Eds.) *Proc. of the 3rd IFIP Int. Conf. on Critical Infrastructure Protection (CIP-2009)* (pp. 215-227). Springer, USA.

Dept. of Homeland Security (2009). *National Infrastructure Protection Plan*, USA.

European Council (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal L 345*, 0075-0082.

Zio, E., & Sansavini, G. (2011). Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins. *Transactions on Reliability*, *60*(1), 94-101.

Haimes, Y., Santos, J., Crowther, K., Henry, M., Lian C, & Yan Z. (2007). Risk Analysis in Dependent Infrastructures. In Goetz, E., Sheno, S. (Eds.) *Critical Infrastructure Protection*, Vol. 253 (pp. 297-310). Springer Boston, USA.

ISO/IEC (2008). *International Standard 27005: Information technology – Security techniques - Information security risk management*. Ref. No. ISO/IEC, 27005:2008, 1st edition.

Kotzanikolaou, P., Theoharidou, M., & Gritzalis, D. (2011). Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects. In Wolthusen S., et al (Eds.) *Proc. of the 6th International Conference on Critical Infrastructure Security* (CRITIS-2011) (pp. 107-118). Springer, Switzerland.

Kröger, W. (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering & System Safety*, *93*(12), 1781-1787.

Kröger, W., Zio, E. (2011). *Vulnerable Systems*. Springer.

Min, O., Liu, H., Zi-Jun, M., Ming-Hui, Y., & Fei Q. (2009). A methodological approach to analyze vulnerability of dependent infrastructures. *Simulation Modeling Practice and Theory*, *17*, 817-828.

Nieuwenhuijs, A., Luiijf, E., & Klaver, M. (2008). Modeling dependencies in critical infrastructures. In Goetz, E., Sheno, S. (Eds.) *Critical Infrastructure Protection*, Vol. 253 (pp. 205-214. Springer Boston, USA.

National Institute for Standards and Technology (2008). *Managing Risk from Information Systems - An Organizational Perspective*. NIST Special Publication 800-39, 2nd Public Draft, USA.

North American Electric Reliability Corporation (2009). *Standard CIP-002-3, Cyber Security-Critical Asset Identification*. December 16, 2009.

Rinaldi, S. (2004). Modeling and simulating critical infrastructures and their interdependencies. In *37th Hawaii International Conference on System Sciences*, Vol. 2. IEEE, USA.

Rinaldi, S., Peerenboom, J. & Kelly, T. (2001). Identifying, Understanding and Analyzing Critical Infrastructure Dependencies. *IEEE Control Systems Magazine*, *21*(6), 11-25.

Pederson, P., Dudenhoeffer, D., Hartley, S., & Permann, M. (2006). *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*. INL/EXT-06-11464, Idaho National Laboratory, USA.

Rosato, V., Issacharoff, L., Tiriticco, F., Meloni, S., De Porcellinis, S., & Setola, S. (2008). Modeling dependent infrastructures using interacting dynamical models. *International Journal on Critical Infrastructures*, *4*(1/2), 63-79.

Santos, J. & Haimes, Y. (2004). Modeling the demand reduction input-output inoperability due to terrorism of interconnected infrastructures. *Risk Analysis*, *24*(6), 1437-1451.

Setola, R., De Porcellinis, S. & Sforna, M. (2009). Critical infrastructure dependency assessment using the input-output inoperability model. *International Journal of Critical Infrastructure Protection*, *2*(4), 170-178.

Svedsen, N., & Wolthunsen, S. (2007). Connectivity models of dependency in mixed-type critical infrastructure networks. *Information Security Technical Report*, 1, 44-55.

Theoharidou, M., Kotzanikolaou, P. & Gritzalis, D. (2009). Risk-based Criticality Analysis. In C. Palmer, S. Shenoi (Eds.), *Proc of the 3rd IFIP International Conference on Critical Infrastructure Protection (CIP-2009)* (pp.35-49). Springer, USA.

Theoharidou, M., Kotzanikolaou, P. & Gritzalis, D. (2010). A multi-layer Criticality Assessment methodology based on interdependencies. *Computers & Security*, 29(6), 643-658.

Theoharidou M., Kotzanikolaou P., & Gritzalis D. (2011). Risk Assessment Methodology for Interdependent Critical Infrastructures. *International Journal of Risk Assessment and Management*, 15(2/3), 128-148.

Utne, I.B., Hokstad, P., & Vatn J. (2011). A method for risk modeling of interdependencies in critical infrastructures. *Reliability Engineering & System Safety*, ESREL 2009 Special Issue, 96 (6), 671-678.

Van Eeten, M., Nieuwenhuijs, A., Luiijf, E., Klaver, M., & Cruz, E. (2011). The state and the threat of cascading failure across critical infrastructures: The implications of empirical evidence from media incident reports. *Public Administration*, *89*, 381–400.