Original Article

Consequence-, time- and interdependency-based risk assessment in the field of critical infrastructure

Iztok Prezelj* and Aleš Žiberna
Faculty of Social Sciences, University of Ljubljana, Kardeljeva ploščad 5, SI-1000 Ljubljana, Slovenia.
E-mail: Iztok.Prezelj@fdv.uni-lj.si

*Corresponding author.

The article was presented in 2011 at the twentieth SRA-Europe Meeting in Stuttgart.

Abstract The disruption of any critical infrastructural sector has the potential to create significant direct consequences and cross-sectoral effects in a short period of time. In this article, we suggest a consequence-, time- and interdependency-based risk assessment approach that seeks to identify which direct consequences and intersectoral effects are likely to emerge in what time frame. We argue that critical infrastructures with the capacity to cause the greatest societal consequences and strongest intersectoral negative effects in the shortest time represent the most risky infrastructures. Such a direct risk assessment was further improved by a network-based risk calculation that takes not only first-order effects into account, but also the *n*-order intersectoral cascading effects. Applying this model to 17 infrastructural subsectors in Slovenia shows that the network transfer of effects among critical infrastructures can considerably and unpredictably change their initially calculated risk. The riskiest subsectors at the maximal level of network effects turned out to be those on which other subsectors heavily directly and indirectly depend: electricity, ICT, road transport and financial instruments. Risk management in the critical infrastructure protection field and related defence in depth should focus its limited resources on those infrastructures with the biggest network-based risk.
Risk Management (2013) **15,** 100–131. doi:10.1057/rm.2013.1

Keywords: critical infrastructure; risk; risk assessment; network; interdependency

Introduction

Critical infrastructure encompasses a broad spectrum of vital sociotechnical sectors such as transport, energy, ICT, health services, water, food, financial services and so on. Their partial or complete failure could threaten the societies they support and create various kinds of crises related to the interruption of basic services and other outputs (for example, shortage of electricity, oil or food, disrupted medical care and so on). The malfunction of any such sector can create significant damage that affects other infrastructures in a short period of time. The question is how to assess infrastructural risk related to the dynamic interaction of multiple consequences, cross-sectoral effects and time. Our consequence-, time- and interdependency-based (CTI) risk assessment approach (a three-dimensional CTI model) aims to diagnose which direct consequences and intersectoral effects would likely emerge in what time frame after the malfunction of particular critical infrastructures. We argue that critical infrastructures with the capacity of causing the greatest societal consequences and strongest intersectoral negative effects in the shortest time period represent the riskiest infrastructures. This argument and our model were based on a combination of the existing quantitative approaches to risk assessment, studies of critical infrastructure and (social) network analysis theory (see Freeman, 1979; Borgatti, 2005; Borgatti *et al*, 2009), as will be explained below. The goal of this article is to present two possible measures of risk, incorporating the variables of consequences (c), time (t) and interdependency (i), and to show their usefulness in the development of risk management strategies.

The consequences of an infrastructural disruption are a typical variable in risk assessment as they show predictable direct or indirect effects and reflect the societal importance of particular infrastructure (see Luiijf *et al*, 2003; Dunn, 2004; Willis *et al*, 2005). The role of interdependencies in relation to infrastructural risk has also become widely recognized (see Perrow, 1999; Rinaldi *et al*, 2001; Boin *et al*, 2003; Le Grand *et al*, 2003; Zimmerman, 2004; Lewis, 2006; van Asselt and Renn, 2011). Cascading failures can spread cross-sectorally from one infrastructure to another, potentially causing compound and complex disasters. Risk has obviously become a borderless phenomenon, transcending different kinds of structural and other borders (Smith and Fischbacher, 2009). Approaches to studying cross-sectoral interdependencies have been developed, such as the Inoperability Input–Output model for estimating how the system of interdependent infrastructural sectors can be adversely affected in terms of economic damage as a result of initial perturbations to other sectors through willful attacks or natural disasters (Santos and Haimes, 2004; Lian and Haimes, 2006). In addition, the role of time is important because risks materialize in certain regions of space during particular time intervals. Only rare examples of risk assessment in the field of critical

infrastructure have included this variable directly (see Rinaldi *et al*, 2001; Bradley, 2007; Haimes, 2009; Barker and Santos, 2010), and even they show that different time variables can be considered (for example, the timing of the adverse event, temporal accumulation of events, speed of events, duration of their effects, time to recovery and so on). The above brief overview of the infrastructural relevance of consequences, interdependency and time shows that there are enough good reasons to build our risk assessment approach on these variables.

Although there is no universally accepted definition of risk, the prevailing quantitative approaches to risk assessment understand risk as a function of the probability of an escalation of a particular threat or adverse event that would bring some dangerous consequences. For example, Lowrance (1976) defined risk as a measure of the probability and severity of adverse effects. Kaplan (1997) later defined it as a triplet of scenario, likelihood and consequences. Many other authors used similar definitions of risk (see Ben-Ari & Or-Chen, 2009; International Risk Governance Council, 2006), whereas some added the dimension of vulnerability (see Dunn, 2004; Haimes, 2004; Willis *et al*, 2005; Willis, 2007; Aven, 2011a). In addition, the ISO 31000 standard recognizes the use of risk as a combination of the consequences of an event and the associated likelihood of its occurrence (Standards Australia & New Zealand, 2009). Aven's (2011a, b) assessment of risk characterizations has further shown that risk can be understood as a result of threatening events (initiating events, scenarios – A), consequences of A (C), and the associated probabilities (P) or uncertainties (U) (an A-C-P or A-C-U understanding of risk). He found out that probability is only a limited tool used to represent the uncertainties and that some models can define risk as *uncertainty about* and the *severity of* the consequences of an activity with respect to something that humans value. Aven (2011b, p. 1082) also suggested that for some applications one can drop the A component (no adverse events are defined) and focus on consequences alone. In our risk model, we have two risk measures using three basic variables (expected consequences, time effects and interdependencies) determined by groups of experts based on the scenario of a complete disruption or malfunction in various infrastructural subsectors (the probability of such a worst-case scenario equals 1).

Direct risk (R_d) attributed to an infrastructural subsector is a function of the expected direct societal consequences, intersectoral effects and time, given the scenario of its complete malfunction. Its value shows the amount of consequences and intersectoral effects per time (according to time). Network-based risk (R_n) attributed to an infrastructural subsector is a function of consequences, time and not only first-order intersectoral effects as in case of R_d, but the *n*-order network effects of its complete malfunction and related consequences and time. It reflects the unpredictable effects of both direct and indirect transfers of consequences per time across infrastructural sectors. These transfers are a consequence of cascading failures or the propagation of

malfunctions across the network. This means that infrastructural risk should grow with the increased diffusion of consequences through the network of interdependent sectors. Such a cross-sectoral process of the transfer of consequences per time can be labeled 'risk transfer', and network-based risk (R_n) is its better estimate. The term risk transfer has been used by other authors to reflect the passing on of some or all consequences of a risk to a third party (see International Risk Governance Council, 2006), thereby decreasing the initial risk for the first party (for example, in the insurance business). However, in our case, the cross-sectoral transfer of malfunctions (consequences per time) is only used for an improved estimation of risk and not a reduction of risk in the initial subsector. Vulnerability was not an express focus in our approach, but can be traced in the varying levels of susceptibility of critical infrastructural subsectors to the effects of a malfunction of others (see Table 3 and the related interpretation). Knowing the unknowns related to direct and network-based risk created by the malfunctions of large infrastructures can contribute to the existing critical infrastructure protection policy and related risk assessment approaches. A better understanding of the cross-sectoral network propagation of risk can also contribute to cross-sectoral defense in depth.

This article is organized as follows. In the next section, we explain the CTI risk assessment method, its three variables and both risk calculations. The third section presents the results of the tested model for the case of Slovenia. In the conclusion section, we summarize the results, discuss their relevance and identify the limitations of our approach.

The CTI Risk Assessment Method

Extreme events can create serious adverse consequences in a relatively short period of time with strong intersectoral negative effects. Our risk assessment approach therefore incorporates three basic variables: consequences, time and interdependencies. The units of our analysis are subsectors of critical infrastructure. Each subsector refers to a group of infrastructures performing a similar function. Figure 1 shows the variables, subsectors and outputs of the risk assessment process, which are further explained in the rest of this section.

The variables

The CTI risk assessment is based on an expert assessment of the basic variables. Each variable in each subsector was to be assessed on the hypothetical *assumption (scenario) of a complete subsectoral breakdown and no countermeasures*. All subsectors thereby faced exactly the same simple scenario, and the consequences of this scenario were measured in a way that allows further cross-sectoral comparability. Some critics might argue that it is artificial to separate the cause and related consequences (CTI variables in our case).

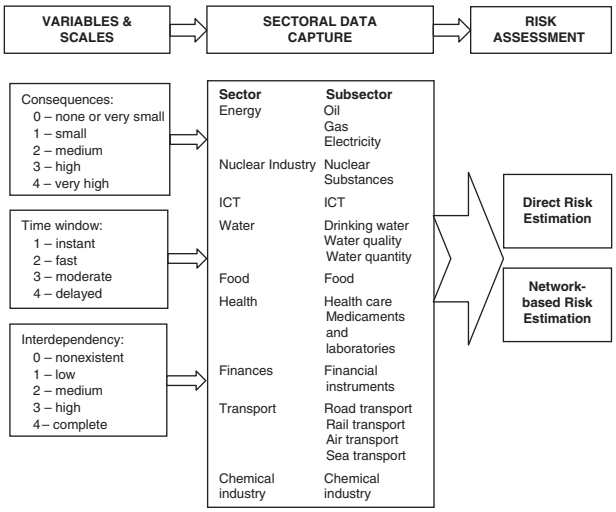

Figure 1: CTI risk assessment model.

We concur that assessing variables under this scenario is somewhat artificial, although it can be demonstrated that this approach has been used by several other scientists to reduce the cognitive complexity of numerous possible scenarios (see Di Mauro *et al*, 2010, p. 281), several potential countermeasures and their complex interactions when assessing the variables at the subsectoral workshops. Only such a simplification enables us to acquire the 'pure' consequences, interdepencies and time windows that determine the absolute subsectoral risk. For example, the assessment assumption of complete subsectoral failure has been used in cross-sectoral scanning in the Netherlands to assess the variable of interdependencies without any countermeasures, meaning no back up, no redundancy, no alternative buffers or supplies (Luiijf *et al*, 2003). A similar approach to assessing variables without considering countermeaures was used in the United States by Barker and Santos (2010, p. 969) where it was labeled the 'do nothing strategy'. Swiss and German approaches have also employed a scenario of a complete infrastructural malfunction without specifying the threat or its nature that might cause such a malfunction (Bundesamt für Sicherheit in der Informationstechnik, 2008; Fischer, 2010, p. 31). A similar logic when assessing the consequences (complete malfunction – no countermeasures) has been used by all EU member states to determine the European critical infrastructure in the subsectors of oil, gas, electricity, road, air, rail and water transport (see Council of the European Union, 2008). Such inoperability scenarios have also been used to assess the cascading financial effect of an infrastructural malfunction on other infrastructures (see Anderson *et al*, 2007) and in the HAZOP methodology that has been used widely to predict deviations from the normal system operation (see Kletz, 1997; Dunjo *et al*, 2010).

Our scenario is the worst of all scenarios considered in the HAZOP approach and is applied to the whole infrastructural subsector. In reality, such scenarios are less probable but not completely impossible, as demonstrated by several past blackouts and information security threats. For example, the Northeast blackout in the United States and the blackout in Italy in 2003 were the largest blackouts in the history of those countries, with each affecting more than 50 million people in a time period lasting from 12 hours to 4 days.[1] These wide-area blackouts were the result of a cascade of failures originating from the loss of one line (the Sammis-Star line in the case of the US blackout and the line connecting Switzerland and Italy) (U.S.–Canada Power System Outage Task Force, 2004; North American Electric Reliability Council, 2004; Buldyrev *et al*, 2010). The cascade of failures and interruptions in this subsector affected all related and dependent infrastructures, such as mobile telephone networks, the Internet, water supply systems (lost pressure due to the malfunction of water pumps), electric rail transport, air transport (flights canceled), road transport (cars could not refuel because gas stations were unable to pump fuel, no traffic lights, traffic jams, inoperable road electronic toll systems and so on), financial markets and industry (many facilities shut down or at least had supply problems) and so on (see Sophie, 2003; Gorman, 2005, p. 16; Anderson *et al*, 2007). Various ICT security events (such as information warfare, cyberterrorism, cybercrime and so on) created by states, criminal and terrorist organizations or individuals could in the case of an extreme scenario incapacitate a country and create serious cross-sectoral effects on financial systems, air transport, water control systems, nuclear power plants, government, electricity, rescue services and so on. Digital Pearl Harbor scenarios have been contemplated and exercised (Mandel, 1999, pp. 80–86; Gorman, 2005, p. 11; Ashmore, 2009, p. 4; Shackelford, 2009, p. 195; Biedleman, 2011, p. 58), although the cyberattack on Estonia in 2007 was the first case to threaten the national security of an entire state and aimed to bring the country to a virtual standstill in a time of political conflict. Estonia was brought close to a complete digital collapse that would have shut off many vital services and caused massive social disruptions (Ashmore, 2009, p. 7; Shackelford, 2009, p. 204; Biedleman, 2011, p. 57). Another cyber-threat that could completely disrupt the ICT subsector was the so-called millennium bug or Y2K. A pure technical detail of having two digits instead of four in computer processors brought the whole world in 1999 to the edge of a digital darkness with serious cascading effects. The threat was labeled in apocalyptic terms such as 'a digital time bomb', 'a millennium meltdown', 'a doomsday scenario', 'a simple problem with catastrophic consequences' (Reeve and McGhee, 1996, pp. 1, 15, 178), 'a global ticking time bomb' (CSIS Conference, 1998) and as 'the end of the world as we know it' (Quiggin, 2005). Scenarios of cascading and domino effects predicted the effect on all computerized date-dependent systems, such as road transport regulation, electric rail transport, civil and military aviation, radars, food supply,

electricity supply, the financial and banking sector (for example, tax collection instruments, electronic funds transfer), industry production and supply services, governmental departments, national and international fixed and mobile telecommunications, weapons systems and missile control systems, satellites, including GPS, nuclear power stations and so on (Reeve and McGhee, 1996; CSIS Conference, 1998; Hansen, 1999). Another case of complete subsectoral disruption that lasted several days took place in 2010 in the air transport of many European states due to volcanic eruption in Iceland.

Consequences

This variable refers to societal damage or effects in the case of a subsectoral malfunction. Because of difficulties with measuring indirect effects (such as symbolic, psychological, moral and other effects), the variable only measures direct consequences that can be assessed by 'hard metrics' (Quirk and Fernandez, 2005, p. 13). We used the four typically measured categories of direct consequences, namely, fatalities ($c1$), economic losses ($c2$), political or public effects ($c3$) and environmental effects ($c4$) (Luiijf *et al*, 2003, p. 9; Dunn, 2004, p. 287; Willis *et al*, 2005, p. 599) on the adapted scale proposed by the European Commission for identifying European Critical Infrastructure (see Appendix A). The experts in each infrastructural subsector had to consensually answer the question: 'What would be the direct consequences in the case of a subsectoral malfunction and no countermeasures?' The reasons why such a situation would happen are not important in such an assessment. After obtaining estimates in each subsector for all four damage categories ($c1$–$c4$) on a scale from 0 to 4 (from none or very small to very high effects), the average consequence estimate (c) can be calculated using equation (1). Two multidimensional categories (political or public effects ($c3$) and environmental effects ($c4$)) contribute only their maximal dimensional value to this calculation. The value of average damage also ranges from 0 to 4 (minimal to maximal average consequences). All further calculations in this text use the c values for each subsector.

$$c = \frac{c1 + c2 + \max(c3.1, c3.2, c3.3, c3.4, c3.5) + \max(c4.1, c4.2)}{4}$$

For example, the calculated subsector's average societal damage would amount to 2.5 in the case of the following attributed values: 2 for fatalities (6–15 dead or badly wounded), 4 for direct economic effects (between €50–150 million), 4 for public effects (maximal effect from the following estimates: 2 for effects on public services, 4 for effects on public trust, 3 for effects on public order and 1 for geopolitical effects) and 0 for environmental effects (maximal effect from 2 estimates: 0 for useless territorial area and 0 for share

of homeless population). In such a case, the equation would therefore be $(2+4+4+0)/4=2.5$.

Time

Infrastructural malfunctions and failures take place in some regions of space during some intervals of time. The importance of time was frequently neglected in risk studies. Rinaldi *et al* (2001, p. 21) acknowledged that infrastructural dynamics span a vast temporal range: from milliseconds to years and that modeling interdependencies strongly depends on time scales. In his recent conceptualization of risk, Haimes (2009, pp. 1647–1652) stressed the importance of time in all system-based risk assessments. He found out that all risks to a system and all the consequences of adverse events are also functions of time, especially the time frame and the timing of an adverse event. Experience from various past breakdowns of critical infrastructures indicates that time matters not only in terms of the timing of adverse events (which hour, day, season), but also by the temporal accumulation, speed and duration of their effects. Theoretical simulations have also shown that a risk assessment on the same system in different time periods might result in different calculations of risk (Bradley, 2007). The above-mentioned Input–Output Inoperability Model also uses time in terms of the time to recovery of an affected sector (Barker and Santos, 2010, p. 963). Other studies, for example, use the reaction time to malfunctions, the time lags between the attack on critical infrastructure and the effects of the attack and so on (Dunn and Mauer, 2006, pp. 18–21).

In line with our initial assumption in this article, we measured the time variable that indicates how fast the complete disruption of an infrastructural subsector would create a major societal crisis, defined as the cumulation of threats, urgency and uncertainty by Rosenthal *et al* (1989, p. 10). The experts from each subsector had to jointly assess in what time the malfunction of their subsector would predictably create a societal crisis. The word 'predictable' refers to their expert and consensual perception of how long after the malfunction a crisis would actually appear. The malfunctioning of some subsectors would almost immediately create a serious stress on society and a related crisis, whereas the effects of other subsectors would appear more slowly. To estimate such time windows in each subsector, one should ideally use the classic numerical scale, but it turned out that the experts were unable to assess the time effects with such precision. Instead, we looked into studies that used 'simpler' categories of time windows to assess the impacts of critical infrastructure failures (for example, Luiijf *et al*, 2003). For the purposes of our study, we developed and applied a time scale that is meaningful from the crisis management perspective: 0–12 hours (1 – instant effect), 12–48 hours (2 – fast effect), 2 days–1 week (3 – moderate effect) and more than 1 week (4 – delayed effect). This time scale has enabled us to distinguish between the subsectors that

require an instant crisis reaction from those with delayed effects and time to prepare a reaction.

Interdependencies

The consequences of adverse events and malfunctions in one infrastructural subsector more or less affect others (dependency as a unidirectional relationship) and vice versa (interdependency). According to Perrow (1999, pp. 89–92), failures can interact in anticipated and unanticipated ways (hidden interactions of failures). Both are a reflection of tight or loose coupling or the degree of system interconnectedness. It was further found that a cascading transfer of consequences and failures from one subsector to another may lead to 'escalatory network breakdowns' and 'compound disasters' (Boin *et al*, 2003, pp. 99–100; Koubatis and Schonberger, 2005, p. 202). Such a correlation among the states of each infrastructural subsectors is possible because, for example, infrastructure *i* depends on *j* through some links, and *j* likewise depends on *i* through other links (Rinaldi *et al*, 2001, pp. 12–14).

Interdependency relations are also to some extent hierarchical due to differences in dependence and influence. Zimmerman's (2004) database of critical cross-sectoral incidents in the United States in the period from 1990 to 2004 showed that ICT and electricity are more frequently and vitally affecting others than being affected by others. This was confirmed by Lewis (2006, p. 57) who differentiated three levels of sectors according to their influence and dependency. The first level of the most influential sectors (or 'key sectors' by Barker and Santos, 2010, p. 962) consists of ICT, energy and water, the second level embraces transportation, chemical industry and banking and finances and the third level of the most dependent or vulnerable sectors entails public health, food, defense industry and emergency and postal services. This means that the riskiness of infrastructures can also be interpreted in relation to their structural position within the whole system of interdependent infrastructures.

The experts from each subsector assessed dependencies for their subsector from all other subsectors in the case of their malfunction and without consideration of any countermeasures. To assess these dependencies, we used the following scale already applied by Luiijf *et al* (2003): 0 – nonexistent (0–1 per cent), 1 – small (2 – 33 per cent), 2 – medium (34–66 per cent), 3 – high (67–98 per cent), 4 – complete (99–100 per cent). These categories of dependence were needed in order to simplify the assessment for the experts, and percentage figures were only used as an orientation for the experts to determine the categories of dependence. Nonexistent dependence in this case means that a malfunction of another subsector does not affect the functioning of the assessed subsector, whereas complete dependence refers to the complete inoperability of the assessed subsector created by the complete inoperability of another subsector. The medium dependence refers then to a situation where the assessed

subsector has serious problems with functioning, but still manages to provide some services to a limited extent.

Direct and network-based risk assessment method

The variables described above give us an estimate of the expected social consequences (c), intersectoral effects (i) and time effects (t) in the case of a subsectoral malfunction (that is, complete failure irrespective of a reason). By following the main argument of this article on the riskiness of those infrastructures that have the capacity to cause the greatest negative societal consequences and intersectoral effects in the shortest time, we used the following equation to compute direct risk:

$$R_d = \frac{c + i}{t}$$

where:

R_d – direct risk of a subsector
c – consequences
i – interdependency
t – time

Direct consequences and intersectoral effects are both kinds of consequences. That is why they were summed in the numerator. Time in the denominator reflects the rapidity of effects of the summed consequences. Ordinal variable t as a denominator was a result of a compromise between the researchability of time effects and mathematical flexibility. Our pilot discussion of the variables and scales at a joint preparatory workshop and also with sectoral representatives in the interagency CIP body from the country of our case study showed that the experts could not accurately assess the time windows (before the subsectoral malfunction creates a crisis) on a classical numerical scale. However, they were able to rank subsectors in the broader time categories described above. Although the use of ordinal variable t represents a limitation of our approach, we believe that the R_d index provides a useful (although approximate) 'risk score' (Copas, 1999, p. 38) based on CTI variables.

R_d values extend on the interval from 0 to 8. The maximal value (8) is calculated in the case where very high consequences ($c = 4$) and intersectoral effects ($i = 4$) emerge and instantly ($t = 1$) create a major societal crisis. The minimal value (0) could be calculated in the case of no consequences and intersectoral effects ($c = 0$, $i = 0$) being created by a complete subsectoral disruption, which is almost impossible. All other R_d values represent more realistic and unique combinations of the interactions among the three variables. The calculated R_d values were categorized into four risk levels by splitting the scale into four

equally wide intervals ('very low' (0–2), 'low' (2–4), 'high' (4–6) and 'very high' (6–8)).

Our calculation of direct subsectoral risk up to this point has not considered all network effects of destructive dependencies. However, network analysis theory allows an improvement of the risk calculation for a single subsector by also including the *c* and *t* variables of all other subsectors that are directly or indirectly dependent on the subsector being assessed. In this way, the risk of a specific subsector becomes a function of its own *c* and *t* variables and the *c* and *t* variables of other directly and indirectly dependent subsectors. Rinaldi *et al* (2001, pp. 11–20) introduced the degree of dependency among infrastructures, or a 'coupling order', that indicates whether two infrastructures are directly connected to one another or indirectly coupled through one or more intervening infrastructures (subsectors in our case). The indirect linkages and state changes are commonly referred to as *n*th-order interdependencies, respectively, where *n* is the number of linkages. Of particular note is that feedback loops can also exist through *n*th-order interdependencies. For example, infrastructure *i* is coupled with *j*, *j* is coupled with *k* and *k* is coupled through another route with *i*, then a feedback loop exists through the chain $i-j-k-\ldots-i$. Disturbances rippling through and across the interconnected infrastructures create *n*th-order effects.

Our direct risk calculation only included the first-order effects and even here we did not take the *c* and *t* variables of dependent subsectors into account. Thus, in calculating the network-based risk for each subsector, we considered the 'base risks' ($R_b = c/t$) of all directly or indirectly dependent subsectors and the strength of that direct or indirect dependence. These were taken into account by assuming that if subsector *i* is dependent on subsector *j* then at least some part of the risk of subsector *i* should also be attributed to *j*. If *j* were to malfunction, *i* would also be unable to function to the fullest extent due to its dependency. Further, those subsectors that depend on *i* could also not function to their fullest extent, thus part of their risk should also be added to the risk of *i* and consequently *j*. In this way, we have taken first- and second-order dependency into account, although there is no reason why we should stop here (or any other point).

To take all direct and indirect dependencies into account when estimating network-based risk, we used α centrality by Bonacich and Lloyd (2001) as a centrality measure for asymmetric (directed) networks. Numerous other measures of centrality (or power, status, influence, even coreness) can be found in the network analysis literature (Bonacich, 1972; 1987; Freeman, 1979; Borgatti and Everett, 1999; 2006; Bonacich and Lloyd, 2001; Borgatti, 2005). However, most of these measures are inappropriate for measuring network-based risk. We chose α centrality as it is applicable to directed networks (such as our network of dependencies) and takes into account the 'base risks' (endogenous risks) of subsectors and the nature of risk as the 'thing' that flows (Borgatti, 2005) through the network of dependencies.

The risk is transferred from the subsector where it occurs to the subsectors on which that subsector depends. Obviously, risk can be simultaneously transferred to all subsectors on which a given subsector depends and the 'original' subsector still retains its risk. Risk is not only transferred through the shortest paths, but takes all possible paths. This also means that the length of the path is not limited. Moreover, as so-called feedback loops are possible, the risk can pass again through the same subsector or dependency (a link of dependency between two subsectors). This means that, in Borgatti's (2005) terms, the risk flows through 'walks'.

α centrality can be seen as a generalization of eigenvector centrality that allows such 'endogenous' effects (base risks) to be taken into account. Therefore, network-based risk can be represented using the following equation (Bonacich and Lloyd (2001)) using matrix algebra:

$$R_n = \alpha N^T R_n + R_b,$$

where:

R_n – network-based risks of subsectors
α – a parameter that determines the weight of the network effects
N – the normalized[2] dependency matrix (or network)
R_b – base risks of subsectors

The solution to that recursive equation can be computed by:

$$R_n = (I - \alpha N^T)^{-1} R_b,$$

where I is the identity matrix.

This means that the network-based risk of a subsector can be obtained by:

1. multiplying the network-based risks of other subsectors by the (normalized) strength of their dependency on a given subsector (the strength is 0 if the subsector does not depend on a given subsector);
2. summing these values;
3. multiplying this sum by parameter α; and
4. adding the base risk.

The network-based risk of a given subsector is thereby determined by the network-based risks of subsectors that directly or indirectly depend on it and its own base risk.

Parameter α determines the relative importance of the risks of the dependent subsectors versus the base risk of the analyzed subsector. The greater parameter α is, the greater the effect of the network of interdependencies and the base risk of those subsectors that are directly or indirectly connected to it.

With $\alpha = 0$, only base risk is taken into account. With a small (but non-zero) α, the network-based risk is predominantly determined by the base risks of the analyzed subsector and the subsectors directly connected to it. As we increase α, more weight is given to the base risk of directly and indirectly dependent subsectors. As we further increase toward its maximum value,[3] the network-based risk is predominantly influenced by the network structure and less by the base risks. While the base risks of 'closer' subsectors (in terms of the interdependency network) always have a greater effect than those 'further away', a lower α penalizes the 'further' subsectors more than a higher α. The choice of α is left to the researcher and should be based on his knowledge of how much inoperability and therefore risk is transferred among subsectors. Where we believe there are important limitations (for example, alternatives) on the transfer of risk among subsectors, lower α values are appropriate. Where we believe there are few limitations then α should be set at its maximum value. Another possibility also taken into account in this article is to compute network-based risk at different α values and through that estimate the effect of different assumptions about the risk transfer on network-based risk. The value of network-based risk should be used in relative terms (compared with network-based risks of other subsectors) and not in absolute terms.

Our formula based on α centrality is quite similar to the Inoperability Input–Output Model suggested by Santos and Haimes (2004, pp. 1441–1443) and Leontief's (1951) Input–Output Model from which the former is derived. However, there are important conceptual and computational differences. First, our approach focuses on supply-side inoperability, whereas their approach focuses on demand-side inoperability. Second, they use economic input–output tables to derive the 'dependency matrix', whereas we use estimates of dependencies reported by the experts. Computationally, due to the way the dependency matrices are obtained and what they represent, the parameter α was needed in our approach to obtain non-negative risks.

Results

Data capture

On the basis of the variables elaborated above, a questionnaire was developed and tested on the case of Slovenia.[4] The data capture process was supported and assisted by the Governmental Interagency Coordination Group for Critical Infrastructure Protection and all relevant national ministries. A joint preparatory workshop was organized for relevant national ministries, agencies and public or private organizations with direct or indirect role in managing and protecting critical infrastructures in the country. Around 200 participants debated the project's empirical aims, its relationship with European trends and

activities, the draft questionnaire and the data collection process. The selection of participant organizations in all subsectors was made in consultation with relevant ministries against the criteria of infrastructural coverage: the bodies that control, regulate or manage major national infrastructures in the researched subsectors were invited. After this, the relevant national ministries organized 17 workshops (one for each subsector) for the experts from the invited institutions to fill out 17 questionnaires. The following subsectors were included: oil, gas, electricity, nuclear substances, ICT, drinking water, water quality, water quantity, food, health care, medicaments and laboratories, financial instruments, road transport, rail transport, air transport, sea transport and chemical industry. In total, 121 experts and managers from the key public and private institutions participated in these workshops (to understand their institutional background and their number per workshop, see Appendix B). Participants were sent the questionnaire and a theoretical definition of each variable in advance. Each workshop was moderated by a researcher and aimed to reach a joint and consensual assessment on the variables. Each participant was initially invited to present own assessment of the variable's value and then a discussion was launched to jointly determine this value. As the focus was on the joint and consensual assessment of the variables, the use of multiple raters and an inter-rater reliability score was inapplicable. This was because many of our experts were only able to assess the direct consequences, cross-sectoral and time effects for their part of infrastructures and not for the whole subsector. In such cases, the subsectoral final estimate was acquired by summing and combining the partial assessments. In order to ensure bias control, the scientific moderator persisted with the principle of a consensual determination of the variable values. The consent of each expert about the variable estimate to a certain extent prevented the institutional bias potentially created by some more influential individuals. The groups generally needed 2–3 hours to debate the proposed scenario and assess the variables.

The above-described use of experts and managers for the consensual assessment of risks (variables in our case) is not new. The utility of experts for eliciting data in risk assessment has been proven in theory (Bier *et al*, 1999, p. 87; Lyall and Tait, 2005) and practice in many countries (Dunn, 2004; 2005). The current literature recommends such a multi-actor approach coupled with a mixed methods design that incorporates both the objective (quantitative) and subjective (value-related) characteristics of risk. Our approach followed the recommended multi-actor approach in modern risk governance, whereby various stakeholders from different backgrounds jointly assess risks at roundtables in the face of scenarios containing uncertainty, complexity and ambiguity (Ben-Ari and Or-Chen, 2009, pp. 866–873; Hansson, 2010, p. 236; van Asselt and Renn, 2011, pp. 440–443). This article then used the estimates so acquired for a more positivistic direct and network risk assessment.

Variable assessment

Consequences of a subsectoral malfunction

The average consequence estimate (c) shows the prevalence of more basic or existence-related subsectors over others. This means that the strongest direct consequences would emerge from the malfunction of food, medicaments and laboratories, health care and water quantity, whereas the weakest would arise from the malfunction of air, sea and rail transport and nuclear substances (see Table 1). This means that a major disruption in the first group of subsectors would have been far more critical than in the second group.

The average consequence estimates are mostly determined by the categories economy and public trust, as indicated by the highest vertical sums. On the contrary, the category environment seems to be almost irrelevant. This could mean that the major failure of a particular subsector of critical infrastructure (considering only its failure and not related causes) would create a greater benefit for the environment than harm.

The time before a complete disruption creates a crisis

The results shown in Table 2 confirm our expectation that the malfunction of some subsectors would instantly impact society, while in some cases this effect would be delayed (see also Prezelj *et al*, 2012). The subsectors with an instant crisis effect on society are:

- electricity, because most societal activities are based on its use;
- gas, because there are no reserves of gas in the country (except for the gas in the pipelines);
- health care, as many people need medical treatment everyday;
- medicaments and laboratories, because the normal daily functioning of an enormous number of people depends on medicaments;
- road transport, due to the complete permeation of society by roads;
- water quantity monitoring, because failures of major dams would immediately directly expose a great number of people to threat; and
- nuclear substances, as radiation affects people instantly.

Failures in food distribution would not affect society instantly due to the presence of some reserves in stores and homes. Further, disturbances to the financial sector would seriously affect society after several days due to the relatively flexible payment deadlines and some cash reserves. It should be noted here that Slovenia is a small Central European market economy with an economic development level (in terms of GDP per capita in 2011) comparable to that of Spain, Italy, Israel and Greece. The most delayed crisis impact of more than 1 week would follow the malfunction of sea and air transport, chemical industry and quality of water.

Table 1: Consequence assessments by subsectors and categories

Subsectors	*Categories*									*C*
	(C1) Population	*(C2) Economic damage*	*(C3) Public effects*					*(C4) Environmental effects*		
			(C3.1) Public services	*(C3.2) Public trust*	*(C3.3) Public/ social order*	*(C3.4) End-users (percentage of affected population)*	*(C3.5) Geopolitical effects*	*(C4.1) Useless territorial area (percentage of national territory)*	*(C4.2) Share of homeless population (in percentage)*	
Oil	0	3	0	4	4	3	2	0	0	**1.75**
Gas	0	3	0	4	2	0	4	0	0	**1.75**
Electricity	2	4	4	4	4	4	3	0	0	**2.5**
Nuclear substances	1	1	0	4	3	0	2	0	0	**1.5**
ICT	0	4	4	4	1	3	3	0	0	**2**
Drinking water	2	4	2	4	1	4	3	0	0	**2.5**
Water quality	1	3	1	3	1	2	2	0	0	**1.75**
Water quantity	2	4	2	4	2	0	3	2	0	**3**
Food	4	4	4	4	4	4	3	0	3	**3.75**
Health care	4	4	1	4	4	1	3	0	0	**3**
Medicaments and laboratories	4	4	4	4	4	2	4	0	1	**3.25**
Financial instruments	0	4	1	3	1	0	0	0	0	**1.75**
Road transport	2	4	0	3	0	2	2	0	0	**2.25**
Rail transport	0	3	1	3	0	0	1	0	0	**1.5**
Air transport	0	1	1	3	0	0	2	0	0	**1**
Sea transport	0	2	0	3	0	0	1	0	0	**1.25**
Chemical industry	2	2	0	4	1	0	2	0	0	**2**
SUM	**24**	**52**	**25**	**51**	**32**	**25**	**40**	**2**	**4**	

Table 2: The time window before a complete disruption creates a crisis (see Prezelj *et al*, 2012)

Subsector	*0–12 hours*	*12–48 hours*	*2 days–1 week*	*More than 1 week*
	1 – Instant	*2 – Fast*	*3 – Moderate*	*4 – Delayed*
Electricity	X	—	—	—
Gas	X	—	—	—
Health care	X	—	—	—
Medicaments and laboratories	X	—	—	—
Road transport	X	—	—	—
Water quantity	X	—	—	—
Nuclear substances	X	—	—	—
Food	—	X	—	—
Drinking water	—	X	—	—
Financial instruments	—	—	X	—
Oil	—	—	X	—
ICT	—	—	X	—
Rail transport	—	—	X	—
Sea transport	—	—	—	X
Air transport	—	—	—	X
Chemical industry	—	—	—	X
Water quality	—	—	—	X

Interdependency (cross-sectoral dependencies)

The interdependency matrix in Table 3 shows the assessed dependencies among subsectors. The cell value shows the degree of dependence of the row subsectors from the column subsectors. The results confirm our expectation concerning the varying levels of dependencies. It is also obvious that there are no absolutely independent subsectors on the one hand and absolutely influential subsectors on the other.

We also computed average dependencies and average cross-sectoral influences by subsectors as row/column averages. The values are reported in the final row/column in Table 3 and also in the parentheses after the subsectors' names in the remainder of the subsection. They can be assumed to be measured on an interval (linear) scale, meaning that absolute differences can be compared: for example, the difference between average dependencies of food and water quality (0.1) is the same as between water quality and drinking water.

Horizontal calculations of the average dependencies (row averages) show the distribution of subsectoral dependence or their varying levels of susceptibility to the effects of a malfunction of others. Those subsectors with a higher average dependence are more susceptible to the cascading effects of malfunctions and,

Table 3: Interdependency matrix

Subsectors	*Oil*	*Gas*	*Electricity*	*Nuclear substances*	*ICT*	*Drinking water*	*Water quality*	*Water quantity*	*Food*	*Health care*	*Medicaments and laboratories*	*Financial instruments*	*Road transport*	*Rail transport*	*Air transport*	*Sea transport*	*Chemical industry*	*SUM of dependencies*	*AVERAGE dependency*
Oil	10	0	2	0	4	1	1	1	1	1	1	4	4	4	0	4	0	28	1.8
Gas	1	10	1	0	3	0	0	0	0	0	0	1	1	0	0	0	0	7	0.4
Electricity	1	1	10	1	3	0	2	3	1	1	0	2	2	2	1	1	3	24	1.5
Nuclear substances	0	0	3	10	4	0	0	1	0	0	0	0	0	0	0	0	0	8	0.5
ICT	4	0	4	0	10	0	0	0	0	0	0	0	0	0	0	0	0	8	0.5
Drinking water	3	0	4	0	3	10	4	3	0	0	4	4	3	1	0	0	3	32	2.0
Water quality	3	0	4	0	2	4	10	1	3	0	4	4	4	1	0	0	3	33	2.1
Water quantity	1	0	2	0	3	1	3	10	1	0	1	4	3	2	0	2	0	23	1.4
Food	4	0	4	0	2	4	4	1	10	1	4	3	3	1	1	1	2	35	2.2
Health care	4	0	4	1	3	4	4	1	4	10	4	3	4	1	3	0	3	43	2.7
Medicaments and laboratories	4	3	4	1	4	4	4	2	2	4	10	4	4	4	4	2	4	54	3.4
Financial instruments	0	0	3	0	4	0	0	0	0	0	0	10	1	0	0	0	0	8	0.5
Road transport	3	0	2	0	1	0	0	1	0	0	0	1	10	3	1	0	0	12	0.8
Rail transport	3	0	4	0	2	0	0	0	0	0	0	1	2	10	0	3	0	15	0.9
Air transport	3	0	4	0	3	0	0	0	0	1	0	3	4	0	10	0	0	18	1.1
Sea transport	3	0	2	0	2	0	0	0	0	1	0	2	2	3	0	10	0	15	0.9
Chemical industry	2	4	4	0	1	4	2	4	1	1	1	3	4	2	1	3	10	37	2.3
Sum of influences (effects)	39	8	51	3	44	22	24	18	13	10	19	39	41	24	11	16	18		
Average influence (effect)	2.4	0.5	3.2	0.2	2.8	1.4	1.5	1.1	0.8	0.6	1.2	2.4	2.6	1.5	0.7	1.0	1.1		

consequently, more vulnerable in the network of critical infrastructure. In this respect, we identified two distinct groups of subsectors:

- Obviously dependent subsectors (very high and high average dependency): medicaments and laboratories (3.4), health care (2.7), chemical industry (2.3), food (2.2), water quantity (2.1) and drinking water (2.0); and
- Relatively independent subsectors: all the remaining ones (with values from 0.4 to 1.8).

More relevant for the risk calculation in this article are the vertical calculations of average cross-sectoral influences by subsectors. The categorization again reveals two groups:

- A group of cross-sectorally influential subsectors (very high and high average influence): electricity (3.2), ICT (2.8), road transport (2.6), oil and financial instruments (2.4); and
- A group of less influential subsectors: all the remaining ones (with values from 0.5 to 1.5).

A further comparison of cross-sectoral influences and dependencies shows there is no subsector that is both among the most influential ones and among the most dependent ones. For a better understanding of the network cross-sectoral dependencies, we include Figure 2, showing the interdependencies among all subsectors as drawn by the computer software Pajek (ver. 2.03, see Batagelj and Mrvar, 2011). The strength of the dependence is reflected by the different shades of grey.

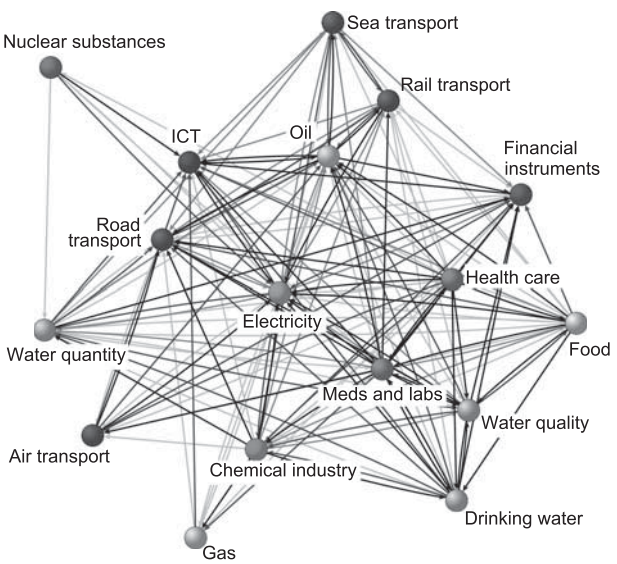

Figure 2: Interdependencies among the critical subsectors (Prezelj *et al*, 2012).

Direct risk

Direct risk for each subsector was calculated using equation (2) based on the *c, t* and *i* values shown in Table 4 and Appendix C. As mentioned above where direct risk was introduced, the values of direct risk were categorized into four categories. The distribution of risk and normalized risk values shows that the majority of subsectors (10 out of 17, or 58.8 per cent) belong to the category of very low risk. Air and sea transport are the least risky subsectors in our case. Surprisingly, drinking water, ICT, oil and financial subsectors are also included here. None of the subsectors belongs to the category of very high risk, whereas four subsectors (23.5 per cent) belong to the category of high risk and three (17.6 per cent) to the category of low risk.

Electricity, road transport, medicaments and laboratories and water quantity subsectors possess the capacity for creating the biggest and fastest effects in Slovenian society in the event of their malfunction. Their malfunction would instantly ($t = 1$ in all cases) create significant societal effects with negative cross-sectoral influences.

The values of the risk index for six subsectors (electricity, road transport, water quality, chemical industry, sea and air transport – 35.2 per cent of subsectors) had been expected due to the extremely high or low values of their CTI categories. All other subsectors represent a unique and not easily predictable

Table 4: Direct risk

Subsectors	*Average consequence estimate – c*	*Time window – t*	*Average cross–sectoral influence – i*	*Direct risk (normalized) – R*	*Risk level*
Electricity	2.50	1	3.19	5.69 (0.71)	High
Road transport	2.25	1	2.56	4.81 (0.6)	High
Medicaments and laboratories	3.25	1	1.19	4.44 (0.55)	High
Water quantity	3.00	1	1.13	4.13 (0.52)	High
Health care	3.00	1	0.63	3.63 (0.45)	Low
Food	3.75	2	0.81	2.28 (0.29)	Low
Gas	1.75	1	0.50	2.25 (0.28)	Low
Drinking water	2.50	2	1.38	1.94 (0.24)	Very low
Nuclear substances	1.50	1	0.19	1.69 (0.21)	Very low
ICT	2.00	3	2.75	1.58 (0.20)	Very low
Oil	1.75	3	2.44	1.40 (0.17)	Very low
Financial instruments	1.75	3	2.44	1.40 (0.17)	Very low
Rail transport	1.50	3	1.50	1.00 (0.13)	Very low
Water quality	1.75	4	1.50	0.81 (0.10)	Very low
Chemical industry	2.00	4	1.13	0.78 (0.10)	Very low
Sea transport	1.25	4	1.00	0.56 (0.07)	Very low
Air transport	1.00	4	0.69	0.42 (0.05)	Very low

combination of two high and one low or one high and two low values. As with all compound indicators, the weight of high values in some categories can easily be diminished by categories with low values (for example, high consequences in the case of food and instant time effects in the case of nuclear substances were diminished by their low average cross-sectoral influence). It also seems that time strongly affects direct risk as no subsector with time higher than 1 is classified as having high risk and all subsectors with time 3 or 4 are classified as having low or very low risk. There might be cases where, apart from high short-term consequences, some very long-term consequences also exist (for example, the long-term consequences of radiation as in the case of Chernobyl). Such situations were not part of our study.

Network-based risk

We defined the network-based risk of each subsector as a function of the base risks and the subsector interdependencies. These risks rose as we increased the transfer of risk through dependencies (α) as seen in Figure 3 (also see the table in Appendix D). However, the increase is not the same for all subsectors. The increase is largest for those subsectors on which the most subsectors (strongly) depend. Therefore, when the risk does not transfer through the network ($\alpha = 0$, base risks), the most (relatively) risky subsectors are those with the largest consequences in a short time, namely, the health sector (health care and medicaments and laboratories) and water quantity, followed by electricity and road transport. As we increase the transfer of risk through the network, the 'network effect' increases and at the maximal transfer rate (at maximal α) the most risky subsectors are those on which the most subsectors (strongly) depend, regardless of their base risks. These are electricity, ICT, road transport and financial instruments (in order of decreasing risk). Using non-extreme transfer rates (values of α) of risk results in 'in-between' values.

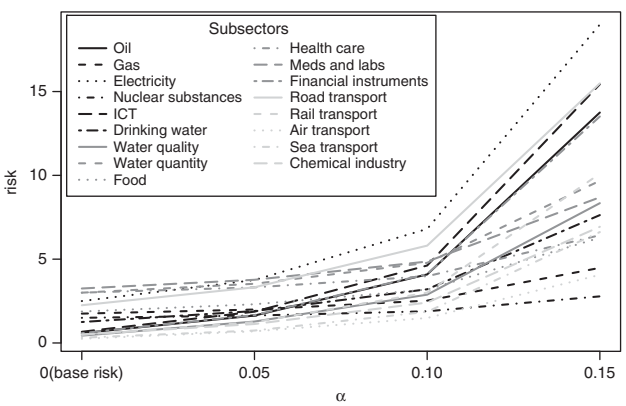

Figure 3: Network-based risks.

To compute the network-based risk, we used a normalized dependency matrix, which is obtained by dividing all values in the original dependency matrix by 4, thus constraining all dependencies between 0 (no dependency) and 1 (total dependency). In this case, the largest permissible value[5] of α equals the largest eigenvalue of the network, which is 0.187 in our case. Although this value might seem small, at this value of α the base risk of a subsector hardly influences its network-based risk. In Figure 3 and Appendix D, we can see the network-based risks computed at α equal to 0.187 (table only), 0.15, 0.10, 0.05 and 0. In the case of $\alpha = 0$, a network is not taken into account so this reduces to base risk.

We can see that the α parameter has a very large effect on the network-based risk and that the network-based risk rises as we increase α (a consequence of the method). The greater the parameter α is, the greater the effect of the network of interdependencies and of the base risk of those subsectors that are directly or indirectly connected to it.

In fact, when α is at its maximum, the values of network-based risk correlate highly (Pearson's correlation coefficient $r = 0.98$) with an average cross-sectoral influence. We have already mentioned that when $\alpha = 0$, network-based risk (although it does not justify this name in such a case) equals the base risk. When α is low (0.05), network-based risk correlates highly with direct risk ($r = 0.97$). The choice of α therefore depends on how much weight is given to base risk versus the base risk of directly dependent subsectors versus the base risk of indirectly dependent subsectors.

As mentioned, at intermediate values of α, the network-based risk highly correlates with direct risk. The correlation is highest (0.97) at $\alpha = 0.05$, although we can notice that the order of the most risky subsectors is not the same. Interestingly, the top four most risky subsectors (and their order) are the same based on direct risk and based on network-based risk with $\alpha = 0.10$. However, in spite of these similarities, we must be aware of the fact that network-based risk and direct risk differ significantly in the way they take interdependencies into account. With direct risk, an index of the influence of the subsector is used to take interdependencies into account, whereas with network-based risk the interdependencies are used to estimate how much risk is transferred from the directly and indirectly dependent subsectors to the subsector being analyzed.

In Figure 4 (and Appendix D), we can observe how the ranks of subsectors (based on their network-based risk) change as we increase α (the network effect). What we can observe is that, by increasing α, mostly the ranks of the subsectors on which a lot of subsectors (strongly) depend increase (for example, ICT, electricity, oil), whereas the ranks of those which have a high-base risk and on which only a few subsectors depend strongly decrease (for example, laboratories and medicaments, health care, food). Not all increases can be explained by the 'local' dependence structure, that is, by looking only at subsectors that directly depend on the analyzed subsectors. One of the more

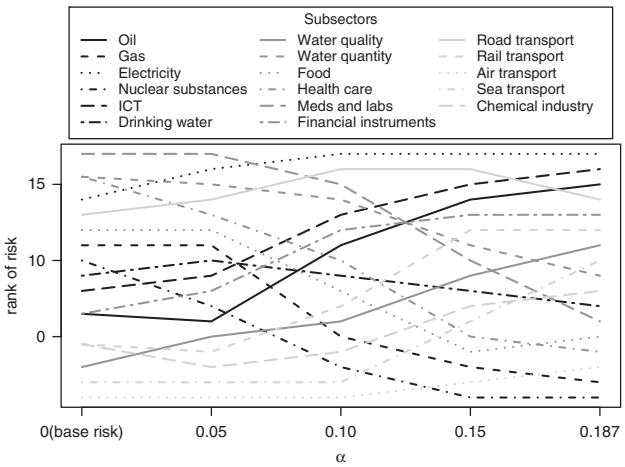

Figure 4: Ranks of subsectors by network-based risk.

noticeable examples is sea transport. Not a lot of subsectors depend on it, although the oil subsector (one of the more influential subsectors) fully depends on it. Consequently, a lot of subsectors indirectly depend on sea transport. As most of these dependencies are therefore indirect, sea transport's rank does not increase at low α values, but it does at higher α values.

Conclusion

In this article, we conceptualized and tested a CTI-based risk assessment approach. The results for the case of Slovenia confirmed our argument concerning the cross-sectoral differentiation of risk based on consequence, interdependency and time estimates. The subsectoral malfunctions create varying direct social consequences and network effects in varying time. The biggest direct risk was calculated for the electricity, road transport, medicaments and laboratories and water quantity subsectors because their malfunction would cause the greatest direct consequences and intersectoral effects in the shortest time. The further network assessment of cross-sectoral direct and indirect risk transfers indicated the increase of risk and an upward and downward change of ranks for all subsectors as a consequence of increasing the levels of network effects. At the maximal level of network effects, the most risky subsectors were electricity, ICT, road transport and financial instruments. These are the subsectors on which other subsectors strongly depend (directly or indirectly). In fact, at this level of network transfer, the network-based risk is practically determined solely by the network structure. This is sometimes undesirable and therefore the appropriate level of network effects should be lower. At small levels of network transfer, the network-based risks are almost the same as those based on direct

risk and highly correlated with base risk, which indicates that the effect of the network is underestimated here. The appropriate α should therefore lie somewhere in between. Therefore, we can conclude that network-based risk is a more appropriate measure of risk than direct risk as it takes into account both endogenous subsectoral risk and the risks of all subsectors directly or indirectly dependent on it. However, it is also much more complex. This is evident from the way the risks and also the rankings of subsectors change as we change the level of the transfer of risk (α) through the network, especially when some changes cannot be explained by the risk of the subsector and the local network structure. From the perspective of a single subsector (or a local network perspective), this also means that the disruption of any subsector could be unpredictably transferred to all other subsectors and this could seriously affect their risks. Such unpredictable network transfers of risk should be given more attention in academia and practice in the future. Attention and resources should be prioritized to target those infrastructures with the biggest network-based risk and not only directly risky infrastructure. Improving their robustness would highly and effectively improve the robustness of the whole system of systems. Joint cross-sectoral exercises should be conducted to increase our infrastructural preparedness and defense in depth. The CTI assessment as a multi-actor joint activity should be repeated over time to reflect changes in the infrastructural base and related interdependencies.

These results simultaneously point to the high relevance, complexity and unpredictability of a network-based risk assessment. It is certain that the flow of risk through the network of critical infrastructures must be measured, assessed and predicted, yet what is not clear is with what level of network transfer (α). A high transfer level decreases the importance of direct consequences and time, which turned out to be very important in our calculations of direct risks.

Our results should also be judged with some limitations in mind. Expert-based assessments are only assessments – even experts can make subjective estimations. We tried to minimize this by leading our subsectoral workshops in the direction of a consensual and joint determination of the variable values. Superior results would be obtained if the Delphi method had been used where the experts would have reconvened and jointly reassessed all the variables based on the results of the first round from their and from other subsectors. This was impossible in our case due to the time and financial constraints brought about by the consensual and logistical difficulties of organizing so many multi-actor workshops. The second limitation refers to the variable of time, which should optimally be a numerical variable, especially due to its position in the denominator of the risk formula. The experts were, however, unable to assess it on a classic numerical scale. Further, several options for the inclusion of time in the network-based risk calculation were considered. Eventually, we decided to include time by dividing the consequences of each

subsector by the time needed till these consequences create a serious crisis. This option most appropriately reflects the network aspects of risk as it includes the time variable (in combination with consequences) of all other subsectors that are directly or indirectly dependent on the subsector being assessed. The next limitation of our approach refers to the scenario for assessing the CTI variables (complete malfunction – no countermeasures). While useful for obtaining pure risk values and their cross-sectoral comparison, the interpretation of its results is made more difficult than in the case of a scenario with a simpler threat (for example, one kind of terrorist attack in all subsectors). Finally, α centrality is an approximate measure that does not take account of all details of the transfer of malfunctions and their effects on risk transfer in the case of a total malfunction of a subsector, whereas it is a good measure of risk in the case of a partial malfunction. Better estimates of the 'true network-based risk' could be obtained through a simulation of the diffusion of malfunctions through the network of dependencies and subsequent network-based risk calculation. However, to obtain superior results through simulations, much more detailed data on the transfer of malfunctions would be needed, with an emphasis on the interaction of dependencies from different subsectors. In fact, we would need a function for each subsector that would give us the operational status of a subsector given the statuses of all other subsectors in the system (upon which this subsector depends). As such data are currently unavailable, we opted for the simpler, but more usable approach here.

In the future, we plan to repeat the CTI assessment and improve it by applying the Delphi method to obtain even better data. If sufficiently detailed data on the interactions of the dependencies can be gathered, we will use the simulations described above to obtain a more exact and realistic network-based risk estimate. We are also examining the potential to use our network approach to study and visualize cascading and network effects on real cases of complex crises (with real data and not only assessments).

Acknowledgements

The empirical part of this article was made possible by a grant from the Slovenian Research Agency and the Ministry of Defense (project title: Definition and Protection of Critical Infrastructures, CRP M5-0159). We are grateful for the comments on early drafts provided by Rae Zimmerman, Andrej Blejec, Alain de Beuckelaer and the two anonymous reviewers.

Notes

1 In the case of Italy, the whole country was affected except for the islands. In the other case, Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, New Jersey and even Ontario were affected by the massive blackout.

2 A normalized dependency matrix is obtained by dividing all values by 4 to obtain a scale from 0 to 1.
3 α can at most be $1/\lambda$, where λ is the highest eigenvalue of the N matrix. Higher values could lead to negative risks.
4 The process of designing the questionnaire was based on preliminary theoretical studies of critical infrastructure, case studies of other countries, and EU policy in this field. The first version of the questionnaire was tested by our academic colleagues for its clarity and methodological consistency and also commented on by the (subsectoral) experts from practice. These comments confirmed the empirical usability of the questionnaire and led us to adapt some questions. The three questions on consequences, time effects and interdependency were closed and quantitative, whereas the remaining questions (not part of this article) were predominantly qualitative and open (see Prezelj *et al*, 2012).
5 Larger values would result in negative risk values.

References

Anderson, C.W., Santos, J.R. and Haimes, Y.Y. (2007) A risk-based input-output methodology for measuring the effects of the August 2003 Northeast blackout. *Economic Systems Research* 19(2): 183–204.

Ashmore, W.C. (2009) Impact of alleged Russian cyber attacks. *Baltic Security & Defence Review* 11: 4–40.

Aven, T. (2011a) *Quantitative Risk Assessment*. Cambridge, UK: Cambridge University Press.

Aven, T. (2011b) A risk concept applicable for both probabilistic and non-probabilistic perspectives. *Safety Science* 49(8–9): 1080–1086.

Barker, K. and Santos, J.R. (2010) A risk-based approach for identifying key economic and infrastructure systems. *Risk Analysis* 30(6): 962–974.

Batagelj, V. and Mrvar, A. (2011) Pajek 2.03, http://pajek.imfm.si/doku.php?id=download, accessed 11 April 2011.

Ben-Ari, A. and Or-Chen, K. (2009) Integrating competing conceptions of risk: A call for future direction of research. *Journal of Risk Research* 12(6): 865–877.

Biedleman, S.W. (2011) Defining and deterring cyber war. *Military Technology* 35(11): 57–62.

Bier, V.M., Haimes, Y.Y., Lambert, J.H., Matalas, N.C. and Zimmerman, R. (1999) A survey of approaches for assessing and managing the risk of extremes. *Risk Analysis* 19(1): 83–94.

Boin, A., Lagadec, P., Michel-Kerjan, E. and Overdijk, W. (2003) Critical infrastructures under threat: Learning from the anthrax scare. *Journal of Contingencies and Crisis Management* 11(3): 99–104.

Bonacich, P. (1972) Factoring and weighting approaches to status scores and clique identification. *Journal of Mathematical Sociology* 2(1): 113–120.

Bonacich, P. (1987) Power and centrality: A family of measures. *American Journal of Sociology* 92(5): 1170–1182.

Bonacich, P. and Lloyd, P. (2001) Eigenvector-like measures of centrality for asymmetric relations. *Social Networks* 23(3): 191–201.

Borgatti, S.P. (2005) Centrality and network flow. *Social Networks* 27(1): 55–71.

Borgatti, S.P. and Everett, M.G. (1999) Models of core/periphery structures. *Social Networks* 21(4): 375–395.

Borgatti, S.P. and Everett, M.G. (2006) A graph-theoretic perspective on centrality. *Social Networks* 28(4): 466–484.

Borgatti, S.P., Mehra, A., Brass, D.J. and Labianca, G. (2009) Network analysis in the social sciences. *Science* 323(5916): 892–895.

Bradley, J. (2007) Time period and risk measures in the general risk equation. *Journal of Risk Research* 10(3): 355–369.

Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E. and Havlin, S. (2010) Catastrophic cascade of failures in interdependent networks. *Nature* 464(7291): 1025–1028.

Bundesamt für Sicherheit in der Informationstechnik. (2008) *Analyse Kritischer Infrastrukturen: Die Methode AKIS*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/AKIS_2008_pdf.pdf?__blob=publicationFile, accessed 21 December 2011.

Copas, J. (1999) Statistical modelling for risk assessment. *Risk Management* 1(1): 35–49.

CSIS Conference. (1998) The Y2K crisis: A global ticking time bomb? *The Washington Quarterly* 21(4): 147–166.

Di Mauro, C., Bouchon, S., Logtmeijer, C., Pride, R.D., Hartung, T. and Nordvik, J.P. (2010) A structured approach to identifying European critical infrastructures. *International Journal of Critical Infrastructures* 6(3): 277–292.

Dunn, M. (2004) Analysis of methods and models for CII assessment. In: M. Dunn and I. Wiegert (eds.) *International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries*. Zurich, Switzerland: ETH – Swiss Federal Institute of Technology, pp. 219–297.

Dunn, M. (2005) The socio-political dimensions of critical information infrastructure protection. *International Journal of Critical Infrastructures* 1(2/3): 258–268.

Dunn, M. and Mauer, V. (eds.) (2006) Introduction. In: *International CIIP Handbook 2006 – Vol II: Analyzing Issues, Challenges and Prospects*. Zurich, Switzerland: Center for Security Studies.

Dunjo, J., Fthenakis, V., Vilchez, J. and Arnaldos, J. (2010) Hazard and operability (HAZOP) analysis: A literature review. *Journal of Hazardous Materials* 173(1–3): 19–32.

European Commission. (2006) *Proposal for a Directive of the Council on the Identification and Designation of European Critical Infrastructures*, 16933/06, 2006/0276(CNS), 18 December, Brussels.

Freeman, L.C. (1979) Centrality in social networks conceptual clarification. *Social Networks* 1(3): 215–239.

Fischer, F. (2010) *Kritische Infrastrukturen Denkweisen, Zusammenhänge, Visualisierungen*, Karlsruher Institut für Technologie (K.I.T.), Institut für Kern- und Energietechnik (IKET), Karlsruhe.

Gorman, S.P. (2005) *Networks, Security and Complexity: The Role of Public Policy in Critical Infrastructure Protection*. Cheltenham, UK: Edward Elgar.

Haimes, Y.Y. (2004) *Risk Modeling, Assessment, and Management*. Hoboken, NJ: John Wiley & Sons.

Haimes, Y.Y. (2009) On the complex definition of risk: A systems-based approach. *Risk Analysis* 29(11): 1647–1654.

Hansen, M. (1999) Y2K the year 2000: Apocalypse soon. *Professional Safety* 44(2): 37–42.

Hansson, S.O. (2010) Risk: Objective or subjective, facts or values. *Journal of Risk Research* 13(2): 231–238.

International Risk Governance Council. (2006) *White Paper on Risk Governance: Towards an Integrative Approach*, Geneva, http://www.irgc.org/IMG/pdf/IRGC_WP_No_1_Risk_Governance__reprinted_version_.pdf, accessed 20 December 2011.

Kaplan, S. (1997) The words of risk analysis. *Risk Analysis* 17(4): 407–417.

Kletz, A.T. (1997) Hazop – Past and future. *Reliability Engineering and System Safety* 55(3): 263–266.

Koubatis, A. and Schonberger, J.Y. (2005) Risk management of complex critical systems. *International Journal of Critical Infrastructures* 1(2/3): 195–215.

Le Grand, G., Springinsfeld, F. and Riguidel, M. (2003) *Policy Based Management for Critical Infrastructure Protection: ACIP Project*. Paper presented at the Annual Meeting 'Informatik 2003' of the German Informatics Society, Johann Wolfgang Goethe-Universität, Frankfurt am Main.

Leontief, W.W. (1951) Input–output economics. *Scientific American* 185(4): 15–21.

Lewis, T. (2006) *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. New Jersey: Wiley Interscience.

Lian, C. and Haimes, Y.Y. (2006) Managing the risk of terrorism to interdependent infrastructure systems through the dynamic inoperability input–output model. *Systems Engineering* 9(3): 241–258.

Lowrance, W. (1976) *Of acceptable Risk: Science and the Determination of Safety*. Los Altos, CA: William Kaufmann.

Luiijf, E., Burger, H. and Klaver, M. (2003) Critical infrastructure protection in the Netherlands: A quick scan. Paper presented at the ECAIR Conference on Best Paper Proceedings in Copenhagen, http://www.crypto.rub.de/imperia/md/content/lectures/kritis/bpp_13_cip_luiijf_burger_klaver.pdf.

Lyall, C. and Tait, J. (eds.) (2005) Shifting policy debates and the implications for governance. In: *New Modes of Governance: Developing an Integrated Policy Approach to Science, Technology, Risk and the Environment*. Aldershot, UK: Ashgate, pp. 1–17.

North American Electric Reliability Council. (2004) Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn? (2004), Report to the NERC Board of Trustees by the NERC Steering Group, July 13, http://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf, accessed 9 May 2012.

Mandel, R. (1999) *Deadly Transfers and the Global Playground: Transnational Security Threats in a Disorderly World*. Westport, CT: Praeger.

Perrow, C. (1999) *Normal Accidents: Living with the High-Risk Technologies*. Princeton, NJ: Princeton University Press.

Prezelj, I., Kopač, E., Svete, U. and Žiberna, A. (2012) Cross-sectoral scanning of critical infrastructures: From functional differences to policy-relevant similarities. *Journal of Homeland Security and Emergency Management* 9(1): 1–29.

Quiggin, J. (2005) The Y2K scare: Causes, costs and cures. *Australian Journal of Public Administration* 64(3): 46–55.

Quirk, M.D. and Fernandez, S.J. (2005) Infrastructure robustness for multiscale critical missions. *Journal of Homeland Security and Emergency Management* 2(2), Article 2. doi: 10.2202/1547-7355.1092.

Reeve, S. and McGhee, C. (1996) *The Millennium Bomb: Countdown to a £400 Billion Catastrophe*. London: Vision Paperbacks.

Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K. (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine* 21(6): 11–25.

Rosenthal, U., Charles, M. and T'hart, P. (1989) The world of crisis and crisis management. In: U. Rosenthal and P. T'hart (eds.) *Coping with Crises: The Management of Disaster, Riots and Terrorism*. Springfield, MA: Charles Thomas.

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

Shackelford, S.J. (2009) From nuclear war to net war: Analogizing cyber attacks in international law. *Berkeley Journal of International Law* 27(1): 192–251.

Smith, D. and Fischbacher, M. (2009) The changing nature of risk and risk management: The challenge of borders, uncertainty and resilience. *Risk Management* 11(1): 1–12.

Sophie, A. (2003) Blackout in Italy underlines need for new power plants. *Christian Science Monitor* 95(213): 7.

Standards Australia & New Zealand. (2009) *Risk Management – Principles and Guidelines*, AS/NZS ISO 31000:2009, Council of Standards Australia and Council of Standards New Zealand: Sydney and Wellington.

The Council of The European Union. (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. 2008/114/EC.Sect. L 345: 75–82.

U.S.–Canada Power System Outage Task Force. (2004) Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. April, https://reports.energy.gov/BlackoutFinal-Web.pdf, accessed 9 May 2012.

Van Asselt, M.B.A. and Renn, O. (2011) Risk governance. *Journal of Risk Research* 14(4): 431–449.

Willis, H.H. (2007) Guiding resource allocations based on terrorism risk. *Risk Analysis* 27(3): 597–606.

Willis, H.H., Morral, A.R., Kelly, T.K. and Medby, J. (2005) *Estimating Terrorism Risk*. Santa Monica, CA: RAND Corporation.

Zimmerman, R. (2004) Decision-making and the vulnerability of interdependent critical infrastructure. *Systems, Man and Cybernetics, 2004 IEEE International Conference* 5(213): 4059–4063.

Appendix A

Table A1: Categories and scales for assessing the direct consequences of a subsectoral malfunction (European Commission, 2006; The Council Of The European Union, 2008, p. 78)

Scale	*Categories*								
	(c1) Population (dead and badly wounded people)	*(c2) Economic damage (million €)*	*(c3) Public effects*					*(c4) Environmental effects*	
			(C3.1) Public services	*(C3.2) Public trust*	*(C3.3) Public/ social order*	*(C3.4) End-users (percentage of affected population)*	*(C3.5) Geopolitical effects*	*(C4.1) Useless territorial area (percentage of national territory)*	*(C4.2) Share of homeless population (in percentage)*
0 – None or very small	0–1	0–15	No significant effect, normal services are provided	No significant effect	No significant effect	0–20	No significant effect	<1	<1
1 – *Small*	2–5	Above 15–50	State cannot provide services for more than 1 day	Local media coverage, low level of public criticism	Public demonstration on local level	20–40	Geopolitical discussion in media	1–3	1–3
2 – *Medium*	6–15	Above 50–150	State cannot provide services for more than 3 days	Regional media coverage, medium level of public criticism	Public demonstration on regional level	40–60	Geopolitical discussions at ordinary interstate meeting	3–10	3–10
3 – *High*	16–50	Above 150–500	State cannot provide services for more than 1 week	National media coverage, high level of public criticism	Public demonstration on national level	60–80	Extraordinary geopolitical discussion among the affected states	10–30	10–30
4 – *Very high*	Above 50	Above 500	State cannot provide services for more than 2 weeks	International media coverage, very high level of public criticism	Panic, social disorders, plunderage	80–100	Interruption of political contacts, recall of ambassador	>30	>30

Appendix B

Table B1: Workshops and participating experts

Sector	*Subsector*	*Number of participation (experts)*	*Institutions*
Energy	Electricity	11	Ministry of Economic Development and Technology, Elektro Slovenia, GEN Energy, Holding of Slovenian Power Plants, Nuclear Power Plant Krško, Šoštanj Thermal Power Plant, Thermal Power Plant Ljubljana
	Oil	13	Ministry of Economic Development and Technology, The Agency of RS for Oil Reserves, the companies PETROL (energy, storage, safety), NAFTA Lendava, ISTRABENZ
	Gas	13	Ministry of Economic Development and Technology, The Agency of RS for Commodity Reserves, the companies PETROL, NAFTA Lendava, ISTRABENZ, GEOPLIN Slovenia, Plinarna Maribor, INTERINA Plin
Nuclear industry	Nuclear substances	3	The Slovenian Nuclear Safety Administration, GEN Energy/Nuclear Power Plant Krško, Institute Jozef Stefan – Reactor Centre
ICT	ICT	8	Post and Electronic Communication Agency of the RS, TELEKOM Slovenia, TUŠ Telekom, Radio and Television Slovenia, Slovenian Railways, DARS – The Motorway Company of the RS
Water	Drinking water	6	Ministry of the Environment and Spatial Planning, IVZ – Institute for Health Protection, the water supply companies Vodovod – kanalizacija Ljubljana, Mariborski vodovod and Vodovod – kanalizacija Celje
	Water quality	6	Ministry of the Environment and Spatial Planning, IVZ – Institute for Health Protection, Inspectorate of the RS for the Environment
	Water quantity	8	Ministry of the Environment and Spatial Planning, Ministry of Economic Development and Technology, Slovenian Environment Agency, Institute for the Water of the RS, and two holdings of hydro power plants: SAVA Power Plants and DRAVA Power Plants
Food	Food	5	Ministry of Agriculture, Forestry and Food, Food Safety Directorate, Slovenian Forest Service, Chamber of Commerce and Industry of Slovenia, Inspectorate for Agriculture, Forestry and Food
Health	Health care	11	Ministry of Health, representatives of major hospitals in Slovenia, University Medical Centre Ljubljana, Association of Private Doctors and Dentists
	Medicaments and laboratories	8	Ministry of Health, Public Agency of Slovenia for Medicaments, Institute for Health Protection, Slovenian Chamber of Pharmacy, Institute for Transfusion Medicine, University Medical Centre Ljubljana
Finances	Financial instruments	7	Bank of Slovenia, Ministry of Finance, Tax Administration of the RS, The Association of Slovenian Banks, NLB bank
Transport	Road transport	3	Ministry of Transport, Slovenian Roads Agency, DARS – The Motorway Company of RS
	Rail transport	3	Ministry of Transport, Directorate for Railways, Slovenian Railways
	Air transport	7	Ministry of Transport, main airports (Ljubljana, Maribor and Portorož), National Flight Control
	Sea transport	3	Ministry of Transport, Slovenian Maritime Administration, major port of Koper
Chemical industry	Chemical industry	5	Ministry of Economic Development and Technology, representatives of the large companies Krka, Belinka Petrokemija, NAFTA Lendava, KIK Kamnik, Steklarna Rogaška

© 2013 Macmillan Publishers Ltd. 1460-3799 **Risk Management** Vol. 15, 2, 100–131

Appendix C

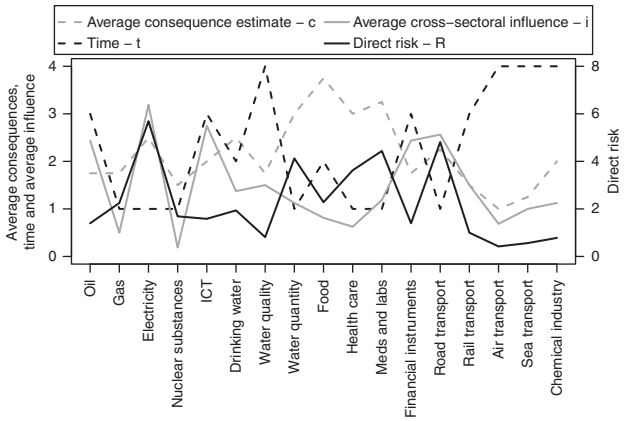

Figure C1: Direct risk in relation to estimated consequences, time and cross-sectoral influences.

Appendix D

Table D1: Network-based risks at different α's (with ranks in brackets)

Subsector \ α	*0.187*	*0.15*	*0.10*	*0.05*	*0 (Base)*
Electricity	19499 (1)	19.0 (1)	6.80 (1)	3.75 (2)	2.50 (4)
Road transport	15299 (4)	15.5 (2)	5.81 (2)	3.32 (4)	2.25 (5)
Medicaments and laboratories	5744 (12)	8.7 (8)	4.86 (3)	3.77 (1)	3.25 (1)
Water quantity	7750 (9)	9.7 (7)	4.78 (4)	3.53 (3)	3.00 (2.5)
Health care	3791 (14)	6.4 (13)	3.98 (8)	3.32 (5)	3.00 (2.5)
Food	4705 (13)	6.3 (14)	3.18 (10)	2.31 (6)	1.88 (6)
Gas	2999 (16)	4.5 (15)	2.53 (13)	1.99 (7)	1.75 (7)
Drinking water	6551 (11)	7.6 (10)	3.20 (9)	1.90 (8)	1.25 (9)
Nuclear substances	1359 (17)	2.8 (17)	1.89 (15)	1.64 (11)	1.50 (8)
ICT	17235 (2)	15.4 (3)	4.62 (5)	1.87 (9)	0.67 (10)
Oil	15386 (3)	13.7 (4)	4.09 (7)	1.63 (12)	0.58 (11.5)
Financial instruments	14780 (5)	13.5 (5)	4.11 (6)	1.66 (10)	0.58 (11.5)
Rail transport	11470 (6)	10.1 (6)	3.00 (11)	1.24 (14)	0.50 (13.5)
Water quality	8158 (7)	8.3 (9)	2.88 (12)	1.28 (13)	0.44 (15)
Chemical industry	6844 (10)	6.9 (11)	2.41 (14)	1.13 (15)	0.50 (13.5)
Sea transport	7839 (8)	6.6 (12)	1.86 (16)	0.74 (16)	0.31 (16)
Air transport	3773 (15)	4.1 (16)	1.49 (17)	0.69 (17)	0.25 (17)