Cascading Effects of Common-Cause Failures in Critical Infrastructures

Panayiotis Kotzanikolaou, Marianthi Theoharidou, Dimitris Gritzalis

Chapter 12

CASCADING EFFECTS OF COMMON-CAUSE FAILURES IN CRITICAL INFRASTRUCTURES

Panayiotis Kotzanikolaou, Marianthi Theoharidou and Dimitris Gritzalis

Abstract One of the most challenging problems in critical infrastructure protection is the assessment and mitigation of cascading failures across infrastructures. In previous research, we have proposed a model for assessing the cumulative security risk of cascading threats due to high-order dependencies between infrastructures. However, recent empirical studies indicate that common-cause failures may result in extremely high impact situations, which may be comparable with or even more devastating than the cascading effects of high-order dependencies. This paper presents an extension to our model, which permits the assessment of the risk arising from complex situations involving multiple cascading failures triggered by major or concurrent common-cause events. The paper also discusses a realistic scenario that is used as a test case for the model extension.

Keywords: Infrastructure dependencies, common-cause failures, cascading effects

1. Introduction

The analysis of cascading failures is an important problem in critical infrastructure protection because, despite the low likelihood of such events, they can result in devastating consequences to multiple critical infrastructures. Examples of such "domino effects" are the electric power disruptions in California in 2001 [15] and the major blackouts in the United States, Canada and Europe in 2003 [1]. However, emphasis has been placed on common-cause failures, primarily because recent statistics [20] indicate that cascading effects are either very rare or are not well documented. Common-cause failures are events that may cause the concurrent disruption of multiple critical infrastructures, which may have no dependency of any type (e.g., cyber, physical, geographi-

cal, logical or social dependency). They can be caused by an adversary, such as the IP-hijacking of YouTube servers in Pakistan in 2008 and the London bombings of July 7, 2005; or they can be natural disasters, such as the 2005 Hurricane Katrina and the 2008 Mediterranean cable breaks [3]. In addition to their immediate effects, such disruptions also cause wider indirect institutional, political and economic effects. These effects include reduced public trust in government services and in democratic processes (e.g., e-voting [8, 10, 11]).

Although cascading and common-cause failures have been studied by many researchers, the relationships between them have been largely ignored. A common-cause failure can affect multiple infrastructures in different sectors such as government, health, information and communications technology and transportation [16, 17]. Each infrastructure that has failed concurrently due to a common-cause failure may lead – with some probability – to multiple cascading chains of failures in its dependent infrastructures.

This paper focuses on the combination of cascading and common-cause failures. In particular, it attempts to assess the overall risk of common-cause failures that may also result in multiple cascading failures. The combined approach is used to assess a scenario that results in concurrent cascading and common-cause failures. The analysis of such scenarios can assist decision-makers in identifying optimal approaches to mitigate risk.

2. Related Work

Dependency modeling has been studied extensively, including sector-specific methods (e.g., for gas lines, electric power grids and information and telecommunications systems) and more general methods that are applicable to multiple critical infrastructures. Dependency models can be divided into six broad categories [7, 14, 21]: (i) aggregate supply and demand models, which evaluate the total demand for infrastructure services in a region and the ability to supply services; (ii) dynamic simulation models, which examine infrastructure operations, effects of disruptions and the associated downstream consequences; (iii) agent-based models, which permit the analysis of the operational characteristics and physical states of infrastructures; (iv) physics-based models, which analyze the physical aspects of infrastructures using standard engineering techniques; (v) population mobility models, which examine the movement of entities through geographical regions; and (vi) Leontief input-output models, which, in the basic case, conduct linear, aggregated time-independent analyses of the generation, flow and consumption of commodities in the various infrastructure sectors.

Critical infrastructure disruptions or outages are usually categorized as cascading, escalating or common-cause [15]:

- A cascading failure occurs when a disruption in one infrastructure affects one or more components in another infrastructure, which, in turn, leads to the partial or complete unavailability of the second infrastructure.
- An escalating failure occurs when a disruption in one infrastructure exacerbates an independent disruption in another infrastructure, usually in

the form of increasing severity or increasing time for recovery and restoration in the second infrastructure.

- A common-cause failure occurs when two or more (connected) infrastructures are disrupted at the same time and components within each infrastructure fail because of a common cause. This occurs when two infrastructures are co-located (geographic interdependency) or when the root cause of the failure is widespread (e.g., a natural or a man-made disaster).

Statistical data about the three failure types is limited. The principal reason is that infrastructure asset owners and operators are unwilling to report incidents and vulnerabilities. A recent empirical study [20] examined data reported to the media. While there is some skepticism regarding the completeness of the data about reported incidents, some interesting findings emerge. First, the study produced a different categorization of failures from the one presented by Rinaldi, *et al.* [15]. Events are classified as: (i) cascade initiating, an event that causes an event in another critical infrastructure; (ii) cascade resulting, an event that results from an event in another critical infrastructure; and (iii) independent, an event that is neither cascade initiating nor cascade resulting.

Other key findings are that cascading dependencies are restricted to a limited number of critical infrastructure sectors, they occur more frequently than expected and often do not cascade deeply. The most commonly reported initiators of cascading effects are the information and communications technology sector and the energy sector, which is expected because these sectors provide products and services to all the other infrastructure sectors. For example, a large number of infrastructures may rely on a common electricity provider because, in many countries, there are relatively few providers. Likewise, critical infrastructures often have few choices regarding Internet and telecommunications service providers [2, 9].

The limited depth observed with regard to cascading failures is likely due to the fact that infrastructure owners and operators make contingency plans and apply countermeasures to mitigate the risk of the obvious upstream dependencies. Examples include the use of emergency generators to cope with power disruptions, and redundant telecommunications links and service providers. Statistics show that cascading effects usually stop after a few nodes due to the presence of countermeasures and contingency plans. However, most of the time these do not take into account changes in the operational mode of critical infrastructures (e.g., stressed, crisis and recovery modes) [12]. Also, they do not consider the changes in the operational modes of upstream suppliers that may be critical to the infrastructures under consideration.

Two (from among several) documented examples of common-cause failures for the two cascading initiating sectors are the blackouts in the United States, Canada and Europe [1] and the cable break incidents in the Taiwan Strait and the Suez Canal [3]. Both types of failures share the common characteristic that a single event caused disruptions to multiple critical infrastructures (common-cause) that, in turn, caused cascading effects to multiple sectors in large geographical regions.

Table 1. Dependency risk table.

Init. CI	Casc. CI	Dependency Type	Impact Type	Impact Scale	Likelihood	Risk
CI_A	CI_E	Cyber: Provides payment services	Public trust	Low	Low	3
CI_B	CI_A	Physical: Provides power services	Economic	Very Low	Low	2
CI_B	CI_C	Physical: Provides power services	Public trust	High	Very Low	4
CI_B	CI_D	Physical: Provides power services	Economic	Very High	Very Low	5
CI_B	CI_E	Physical: Provides power services	Public trust	Low	Low	3
CI_C	CI_E	Cyber: Provides network services	Public trust	Low	Very Low	2
CI_D	CI_C	Physical: Provides connectivity	Public trust	High	Very Low	4

3. Proposed Method

This section presents our approach for assessing the risk arising from complex situations involving multiple cascading failures triggered by major or concurrent common-cause events.

3.1 Preliminaries

We have previously proposed a method for assessing the risk of n^{th}-order dependencies based on the combined results of organization-level risk assessments [4–6]. This method permits the use of existing risk assessment results (e.g., provided by infrastructure operators) that usually document the obvious, upstream dependencies [18].

Following the approach suggested in [19], a risk assessor can construct a dependency risk table as shown in Table 1. The dependency risk table lists the infrastructures that are dependent on each examined infrastructure, which means that it provides information on the cascading risks for each examined infrastructure. For each identified dependency, the table indicates the impact type, impact scale ($I_{i,j}$) and likelihood ($L_{i,j}$) of a disruption. The product of the impact scale and likelihood is defined as the dependency risk $R_{i,j}$ of infrastructure CI_j due to its dependency on infrastructure CI_i. For example, infrastructure CI_B, which belongs to the energy sector, can initiate cascading effects of various levels of risk to four other infrastructures: CI_A (finance sector), CI_C and CI_D (information and communications technology sector) and CI_E (government sector). It is important to note that high-level coordination is required in order to construct a dependency risk table. Risk assessment data

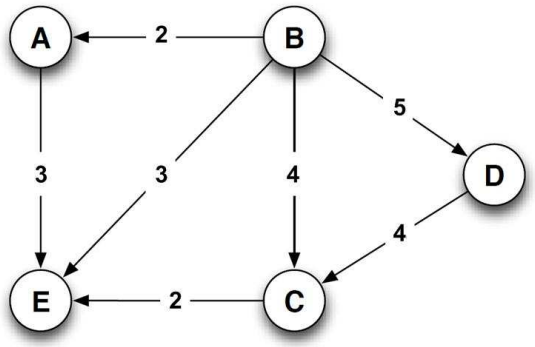

Figure 1. Dependency risk graph.

from all the examined infrastructures must be collected and homogenized (e.g., by government authorities such as sector coordinators).

Dependencies can also be visualized in the form of a graph as shown in Figure 1. An infrastructure is denoted as a circle. An arrow from $X \rightarrow Y$ denotes a risk dependency, i.e., an outgoing risk from infrastructure CI_X to infrastructure CI_Y. A bi-directional arrow $X \leftrightarrow Y$ denotes a cascading risk from CI_X to CI_Y and another cascading risk from CI_Y to CI_X. The number associated with each arrow refers to the level of the cascade resulting risk for the receiver due to the dependency, based on a risk scale from one through nine. For example, in Figure 1, CI_E has a dependency risk $R_{A,E} = 3$ from infrastructure CI_A. This risk value refers to the likelihood that a disruption from CI_A will cascade to CI_E ($L_{A,E}$) as well as the societal impact caused to CI_E if a failure is realized at the source of the dependency CI_A (i.e., $I_{A,E}$). All these parameters ($L_{i,j}, I_{i,j}$ and Ri, j) must be defined in order to assess the risk of the first-order dependencies.

A recursive algorithm is used to estimate the n^{th}-order cascading risks. Let $\mathbb{CI} = (CI_1, ...CI_m)$ be the set of examined infrastructures. Let $CI_{Y_0} \rightarrow CI_{Y_1} \rightarrow \ldots \rightarrow CI_{Y_n}$ denote a chain of connected infrastructures of length n. The algorithm examines each critical infrastructure as a potential cause of a cascading chain (denoted as CI_{Y_0}) and then computes the dependency risk DR exhibited by CI_{Y_n} due to its n^{th}-order dependency.

Risk of n^{th}-Order Cascading Events: Let $CI_{Y_0} \rightarrow CI_{Y_1} \rightarrow \ldots \rightarrow CI_{Y_n}$ be a chain of dependencies, $L_{Y_0,\ldots,Y_n}$ be the likelihood of an n^{th}-order cascading event and I_{Y_{n-1},Y_n} be the impact of the $CI_{Y_{n-1}} \rightarrow CI_{Y_n}$ dependency. Then, the cascading risk exhibited by CI_{Y_n} due to the n^{th}-order dependency is computed as:

$$R_{Y_0,\ldots,Y_n} = L_{Y_0,\ldots,Y_n} \cdot I_{Y_{n-1},Y_n} \equiv \prod_{i=0}^{n-1} L_{Y_i,Y_{i+1}} \cdot I_{Y_{n-1},Y_n}. \quad (1)$$

The cumulative dependency risk defined below considers the overall risk for all the infrastructures in the sub-chains of the n^{th}-order dependency.

Cumulative Dependency Risk: Let $CI_{Y_0} \rightarrow CI_{Y_1} \rightarrow \ldots \rightarrow CI_{Y_n}$ be a chain of dependencies of length n. The cumulative dependency risk, denoted as $DR_{Y_0,Y_1,\ldots,Y_n}$ is defined as the overall risk produced by an n^{th}-order dependency and is computed as:

$$DR_{Y_0,\ldots,Y_n} = \sum_{i=1}^{n} R_{Y_0,\ldots,Y_i} \equiv \sum_{i=1}^{n} (\prod_{j=1}^{i} L_{Y_{j-1},Y_j}) \cdot I_{Y_{i-1},Y_i}. \quad (2)$$

Informally, Equation (2) computes the cumulative dependency risk exhibited by every node in the chain due to a failure realized in the source of the dependency chain. The computation of the risk is based on a risk matrix that combines the likelihood and the incoming impact values of each vertex in the chain. Interested readers are referred to [5] for a detailed analysis of dependency risk estimation.

3.2 Combining Failure Risks

The assessment of cascading failures may reveal hidden, neglected or non-obvious dependencies between critical infrastructures. However, the dependency risk assessed using Equations (1) and (2) only assumes an initiating event (failure) in a single critical infrastructure that causes cascading failures. Thus, it does not capture the overall risk due to large-scale common-cause failures that affect multiple critical infrastructures and potentially initiate multiple cascading chains.

The following method combines common-cause and cascading events in order to assess the potential risk caused by complex situations:

1. **Identify Common-Cause Threats:** Identify every potential threat T_x that may result in a common-cause failure in a critical infrastructure. The potential threats can be accidents, natural disasters or human-initiated attacks.

2. **Assess Likelihood of Threats:** When a potential threat T_x that may cause a common-cause failure is identified, the probability of occurrence L_{T_x} of the threat is assessed. The likelihood of natural disasters can be assessed based on statistics of previous incidents, prognostications and the presence of vulnerabilities. The assessment of the likelihood of adversarial attacks is more complex. These are affected by the motivation and skills of adversaries, as well as the perceived impact of the attacks. Thus, expert opinions coupled with a worst-case approach are commonly used, which results in the maximum valuation of risk.

3. **Assess Cumulative Dependency Risk of Cascading Chains:** For each initiating event (i.e., threat identified in Step 1), Equation (2) is used

to evaluate the n^{th}-order dependency risk for every critical infrastructure that is initially affected by the common-cause threat.

4. **Assess Combined Common-Cause and Cascading Failure Risk:** Let $\mathbb{CI}$ be the set of all examined critical infrastructures. The combined risk of all possible chains of cascading events $CI_{Y_0} \rightarrow CI_{Y_1} \rightarrow CI_{Y_n}$ for each possible source infrastructure $CI_{Y_0} \in \mathbb{CI}$ is computed as the sum of all possible risk chains $DR_{Y_0,\ldots,Y_n}$ for all $Y_0 \in \mathbb{CI}$ multiplied by the likelihood L_{T_x} of each examined threat T_x estimated in Step 2:

$$\sum DR_{Y_0,\ldots,Y_n}(T_x) = L_{T_x} \cdot \sum_{\forall Y_0 \in \mathbb{CI}} DR_{Y_0,\ldots,Y_n} \tag{3}$$

Informally, Equation (3) combines the likelihood L_{T_x} of each examined threat T_x with all the possible dependency chains that may be triggered by the threat being realized. Every critical infrastructure that is affected by T_x is examined as a possible root of a dependency chain (as CI_{Y_0}) based on the risk dependency table and dependency graph. For each CI_{Y_0}, the cumulative dependency risk is computed by applying Equation (2). The next section uses an example scenario to demonstrate the use of the method.

4. Example Scenario

The example scenario focuses on the information and communications technology sector because, along with the energy sector, it is likely to cause cascading chains. The four-step methodology described in the previous section is applied to the scenario.

1. **Identify Common-Cause Threat:** A communication link failure T_{CLF} can cause multiple (common-cause) failures. Such a failure, e.g., a cable break, can be accidental. Underwater cable breaks are common on intercontinental links. They have been caused by direct physical damage from ship anchors, fishing and dredging, and natural disasters such as earthquakes and currents created by extreme weather [3]. A link failure can also be caused by a power outage and, of course, sabotage.

2. **Assess Likelihood of Threat:** Next, it is necessary to assess the likelihood of a cable break $L_{T_{CLF}}$. Previous accident data provides useful information to estimate the likelihood. In 2007, there were more than 50 undersea failures in the Atlantic alone [3]. If we consider the same threat, but as a human-initiated attack, then additional information would have to be incorporated to assess the likelihood. In particular, it would be necessary to identify a potential adversary and proceed to assess factors such as motivation, available resources to perform the attack and the perceived outcome of the attack. Let us assume that the likelihood that a cable break would occur in a particular region is Medium (M) because there were several incidents in the region during the past year,

i.e., $L_{T_{CLF}} = M$. Also, a resonable assumption based on past incidents is that a cable break in this region affects a maximum of four Internet providers that supply services to two countries.

3. **Assess Cumulative Dependency Risk of Cascading Chains:** In this step, Equation (2) is applied to to evaluate the n^{th}-order dependency risks for each possible cascading chain initiated by each of the four service providers belonging to $\mathbb{CI}$, i.e., $\mathbb{CI} = \{CI_{A_0}, CI_{B_0}, CI_{C_0}, CI_{D_0}\}$. Thus, for each identified critical infrastructure, it is necessary to retrieve existing dependency tables and graphs. The cumulative dependency risk for provider CI_{A_0} is the overall risk caused by a failure chain initiated by CI_{A_0}, e.g., $CI_{A_0} \rightarrow CI_{A_1} \rightarrow \ldots \rightarrow CI_{A_n}$ based on Equation (2). The same procedure is followed for the other three providers. If we assume that, for every critical infrastructure, only one chain of failures is identified, then the result of this step is four different, but comparable, values of dependency risk $DR_{CI_{i_0},\ldots,CI_{i_n}}$; $i = A, B, C, D$.

   The dependency risks of these chains may vary based on geography and the presence of redundancies. For example, cable breaks in the Atlantic may occur relatively frequently, but they do not have serious impact because of redundant links. In contrast, cable breaks in the Taiwan Strait or Suez Canal can cause entire geographic regions to lose connectivity [13], resulting in a significantly higher societal impact.

   Even within the same region, the cumulative dependency risks of critical infrastructures may differ because they do not share the same mitigation plans. For example, CI_{A_0} may not cause cascading events with a high likelihood and CI_{A_1} may have countermeasures that reduce the impact caused by the disruption of CI_{A_0}. In contrast, CI_{B_0} may be very likely to cause cascading failures to CI_{B_1} and CI_{B_2}, which may consequently cause a high societal impact if CI_{B_2} is affected (e.g., if a large proportion of a nation's population loses Internet connectivity). The cumulative dependency risk for the chain caused by CI_{B_0} is expected to be higher than the chain caused by CI_{A_0}, i.e., $DR_{CI_{B_0},CI_{B_1},CI_{B_2}} > DR_{CI_{A_0},CI_{A_1}}$.

4. **Assess Combined Common-Cause and Cascading Failure Risk:** The final step is to assess the overall risk caused by the initial (common-cause) failure, i.e., the cable break, to the four affected infrastructures. The risk of the communications link failure threat is assessed using Equation (3) and is given by:

$$R_{T_{CLF}} = L_{T_{CLF}} \cdot \sum_{\forall X_0 \in \mathbb{CI}} DR_{CI_{X_0},\ldots,CI_{X_n}}. \tag{4}$$

   This measure takes into account the likelihood of the common-cause (i.e., cable break) as well as the cascading risk of this event. In the scenario, four infrastructures are affected initially. According to the conditions that affect the likelihood of a cascading failure and the resulting impact if such

a failure spreads, different cumulative dependency risks would be assessed for each chain caused by a failure in the four critical infrastructures.

The approach presented above offers two principal benefits. First, assessing the cascading risk due to n^{th}-order dependencies permits the detection of high societal impacts that would otherwise not appear if only the immediate risks caused by a threat were to be considered. In the cable break scenario, the high societal impact due to the second-order dependency of CI_{B_2} to CI_{B_0} would have been ignored. Second, combining the risks of cascading effects with the common-cause likelihood provides decision makers with a more accurate view of how such threats can affect populations, even at the international level.

In the scenario described above, the assessments would have taken place individually by each of the infrastructure operators and the overall risk of the threat would not have been assessed accurately. Likewise, if the cable break is not considered to be an accident, then the likelihood of occurrence would have been assessed differently, resulting in a different overall risk.

5. Conclusions

Although cascading failures and common-cause failures have been studied by many researchers, the risk deriving from combined failures has not been thoroughly investigated. The method proposed in this paper is a simple and efficient approach for studying the cascading effects caused by large-scale, common-cause events. The combined method can be applied to real-world scenarios to evaluate whether or not common-cause failures can propagate to infrastructures that are not directly affected by the common-cause threat under consideration. This analysis can assist decision-makers in identifying optimal approaches to mitigate risk.

One limitation underlying the proposed method is the combination of risk assessment results at the organizational level. In order to construct a valid dependency risk table, risk assessment data from all the examined critical infrastructures must be collected and homogenized. Thus, the implementation of the methodology requires high-level coordination and management at the national, if not international, level. Another limitation is the identification and evaluation of common-cause threats. This occurs because of the lack of historical data about incidents, largely due to their rarity and the unwillingness of infrastructure owners and operators to provide detailed data. One way to address this problem is to project the consequences of common-cause and cascading effect scenarios by simulating various attack scenarios; this makes it possible to identify the hidden risks and underestimated threats.

Our future work involves the development of an automated tool for implementing and validating the proposed method. The tool will assist risk assessors and decision-makers in gathering information and evaluating the risk of common-cause and cascading events. In addition, the automated tool will help analyze scenarios involving common-cause events (especially, scenarios triggered by low-likelihood events) and identify the underestimated common-cause

threats that could result in very high risks. The analysis of these scenarios could also reveal conflicting data obtained during the information gathering phase and help validate input data for future assessments.

Acknowledgement

This research was supported in part by the S-Port (09SYN-72-650) Project funded by the Hellenic General Secretariat for Research and Technology under the Synergasia Programme, and by the Research Funding Program for Excellence and Extroversion (Action 2) of the Athens University of Economics and Business.

References

[1] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor and V. Vittal, 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*, vol. 20(4), pp. 1922–1928, 2005.

[2] J. Iliadis, D. Spinellis, D. Gritzalis, B. Preneel and S. Katsikas, Evaluating certificate status information mechanisms, *Proceedings of the Seventh ACM Conference on Computer and Communications Security*, pp. 1–8, 2000.

[3] C. Johnson, The telecoms inclusion principle: The missing link between critical infrastructure protection and critical information infrastructure protection, in *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, P. Theron and S. Bologna (Eds.), IGI Global, Hershey, Pennslyvania, pp. 277–303, 2013.

[4] P. Kotzanikolaou, M. Theoharidou and D. Gritzalis, Interdependencies between critical infrastructures: Analyzing the risk of cascading effects, *Proceedings of the Sixth International Conference on Critical Information Infrastructure Security*, pp. 107–118, 2011.

[5] P. Kotzanikolaou, M. Theoharidou and D. Gritzalis, Assessing n-order dependencies between critical infrastructures, *International Journal of Critical Infrastructures*, vol. 9(1/2), pp. 93–110, 2013.

[6] P. Kotzanikolaou, M. Theoharidou and D. Gritzalis, Risk assessment of multi-order dependencies between critical information and communication infrastructures, in *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, P. Theron and S. Bologna (Eds.), IGI Global, Hershey, Pennslyvania, pp. 153–172, 2013.

[7] W. Kroger and E. Zio, *Vulnerable Systems*, Springer-Verlag, London, United Kingdom, 2011.

[8] C. Lambrinoudakis, D. Gritzalis, V. Tsoumas, M. Karyda and S. Ikonomopoulos, Secure electronic voting: The current landscape, in *Secure Electronic Voting*, D. Gritzalis (Ed.), Kluwer Academic Publishers, Boston, Massachusetts, pp. 101–122, 2003.

[9] D. Lekkas and D. Gritzalis, Long-term verifiability of electronic healthcare record authenticity, *International Journal of Medical Informatics*, vol. 76(5-6), pp. 442–448, 2007.

[10] L. Mitrou, D. Gritzalis and S. Katsikas, Revisiting legal and regulatory requirements for secure e-voting, *Proceedings of the Seventeenth IFIP International Conference on Information Security: Visions and Perspectives*, pp. 469–480, 2002.

[11] L. Mitrou, D. Gritzalis, S. Katsikas and G. Quirchmayr, Electronic voting: Constitutional and legal requirements and their technical implications, in *Secure Electronic Voting*, D. Gritzalis (Ed.), Kluwer Academic Publishers, Boston, Massachusetts, pp. 43–60, 2003.

[12] A. Nieuwenhuijs, E. Luiijf and M. Klaver, Modeling dependencies in critical infrastructures, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Boston, Massachusetts, pp. 205–213, 2008.

[13] A. Popescu, B. Premore and E. Zmijewski, Impact of the Middle East cable breaks: A global BGP perspective, presented at the *Forty-Second North American Network Operators Group Meeting*, 2008.

[14] S. Rinaldi, Modeling and simulating critical infrastructures and their interdependencies, *Proceedings of the Thirty-Seventh Hawaii International Conference on System Sciences*, 2004.

[15] S. Rinaldi, J. Peerenboom and T. Kelly, Identifying, understanding and analyzing critical infrastructure interdependencies, *IEEE Control Systems*, vol. 21(6), pp. 11–25, 2001.

[16] M. Theoharidou, M. Kandias and D. Gritzalis, Securing transportation-critical infrastructures: Trends and perspectives, in *Global Security, Safety and Sustainability and e-Democracy*, C. Georgiadis, H. Jahankhani, E. Pimenidis, R. Bashroush and A. Al-Nemrat (Eds.), Springer, Heidelberg, Germany, pp. 171–178, 2012.

[17] M. Theoharidou, P. Kotzanikolaou and D. Gritzalis, Risk-based criticality analysis, in *Critical Infrastructure Protection III*, C. Palmer and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 35–49, 2009.

[18] M. Theoharidou, P. Kotzanikolaou and D. Gritzalis, A multi-layer criticality assessment methodology based on interdependencies, *Computers and Security*, vol. 29(6), pp. 643–658, 2010.

[19] M. Theoharidou, P. Kotzanikolaou and D. Gritzalis, Risk assessment methodology for interdependent critical infrastructures, *International Journal of Risk Assessment and Management*, vol. 15(2/3), pp. 128–148, 2011.

[20] M. van Eeten, A. Nieuwenhuijs, E. Luiijf, M. Klaver and E. Cruz, The state and the threat of cascading failures across critical infrastructures: The implications of empirical evidence from media incident reports, *Public Administration*, vol. 89(2), pp. 381–400, 2011.

[21] E. Zio and G. Sansavini, Modeling interdependent network systems for identifying cascade-safe operating margins, *IEEE Transactions on Reliability*, vol. 60(1), pp. 94–101, 2011.