Risk assessment of multi order dependencies applied on critical ICT infrastructures

Vasilis Stavrou

Information Security and Critical Infrastructure Protection Laboratory, Dept. of Informatics, Athens University of Economics & Business, Greece

January 2014

Presentation of: Kotzanikolaou P., Theoharidou M., Gritzalis D., “Risk assessment of multi-order interdependencies between critical ICT infrastructures”, Critical Information Infrastructure Protection and Resilience in the ICT Sector, pp. 151-170, Theron P., Bologna S. (Eds.), IGI Global.

Introduction

- *Criticality assessment in Critical Infrastructures (CIs)* has similarities with *risk assessment in traditional information systems*.
- Extended approach to capture CI complexities:
  - Risk assessment in CIs requires that societal impacts are taken into consideration.
  - CIs are connected with many others. The effects of a disruption or failure may spread both geographically and across multiple sectors.
- Identifying multi-order dependencies leads to more accurate criticality assessment.
- Goals of the chapter:
  - Assess the **risk that a CI is exposed to**.
  - Assess the **risk of n–order dependencies** between CIs.

Assessing Risk and Dependencies

- Traditional risk assessment methodologies do not assess:
  - Effect of failure/disruption to dependent infrastructures.
  - Impact to society.
- What makes an infrastructure **"critical":**
  - It affects many others connected with it - mostly outsiders for the organization operating the CI.

- Asset criticality depends on:
  - Potential impact of a security incident on the operator of a CI.
  - Outgoing societal risk caused to other dependent organizations.
- Risk assessment methods for CIs fail to model/assess risk caused by multi-order dependencies of CIs.

Dependencies and Failures

Dependencies	
Physical	State depends upon the material output(s) of the other CI.
Cyber/Informational	State depends on information transmitted through the other CI.
Geographic	State depends on environmental event on another CI.
Logical	State depends upon the state of another CI via a non-physical, cyber, or geographic connection
Social	State is affected by the spreading of disorder to another CI related to human activities.

Failures		
Cascading	**Escalating**	**Common-Cause**
A disruption in an infrastru-cture affects one or more components in another infrastructure.	An existing disruption in one infrastructure exacerbates an independent disruption of another one.	Two or more infrastructures networks are disrupted at the same time.

Risk vs. Criticality

- CIs Risk assessment focus on **impact** assessment of **incident** or **threat**.
- **Impact** is assessed under various terms (consequences, criticality, vitality) and expressed with various criteria or factors.
- The **effect** takes the form of Public Health & Safety, Economic Effect, Environment, Political Effect or Governance etc.

- Criticality assessment has more broad cope than risk assessment: It attempts to capture the **external**, societal **impacts**.

Risk Assessment Methodology for CI Dependencies

- Lack of risk assessment methodologies that focus on critical information and communication infrastructures.
  - The existing ones do not assess the risk that is based on the dependencies between them.
- In the approach adopted:
  - Each infrastructure is viewed as a single entity.
- The method assesses risk in two stages:

Detailed assessment of 1st order dependencies between CIs in three levels of abstraction.

Assessment of n-order dependencies, which allow the assessment of risk in chains of infra-structures.

Risk Assessment of 1st-order Dependencies

Risk assessment methodology in three layers			
	Infrastructure level	Sector level	National/intra-sector level
Step 1	Identify all the requisite CIs and the corresponding dependencies.	Identify the dependent CIs and the corresponding dependenci-es.	Calculate overall risk for each CI.
Step 2	Estimate the incoming risk.	Estimate the outgoing societal risk of an infrastructure.	Calculate overall risk for each sector.
Step 3	Create the incoming dependency risk matrix for each CI.	Estimate the inherent societal risk of each CI.	-
Step 4	-	Estimate overall incoming, outgoing societal risk.	-

- **Infrastructure level**: Dependencies are identified.
- **Sector level**: Expected incoming and outgoing societal risk associated with each CI belonging to the sector (estimated by sector coordinator).
- **Intra-sector/national level**: Dependency and societal risk of all sector members are considered, in order to compare the criticality between sectors.

Risk Assessment of N-order Dependencies

- Goal: Assess the n-order dependencies of a CI.
- Extend 1st-order model to N-order dependencies:
  - In order to capture the likelihood of n-order cascading events and the relative risk factors.
  - The cumulative societal risk should consider the overall risk exhibited by all the CIs within the sub-chains of the n-order dependency.
- The proposed algorithm:
  - Examines each infrastructure as the root of dependency chain(s).
  - Constructs chain(s) of its n-order dependencies.
  - Assesses societal risk of each chain.

Proposed Algorithm

- The steps of the algorithm are summarized to the following:

1. Identification of the 1st-order dependencies of the root CI
2. Identification of the n-order dependencies of the root CI
3. Evaluation of the n-order Cumulative Dependency Risk
4. Examine Next Infrastructure
5. Rank Cascading Risk
6. Mitigate Cascading Risk

Conclusion and Future Work

- Focused on risk assessment of multi-order dependencies between CIs.
- The proposed methodology examines the risk of dependency in two stages:
  - **1st-order** dependencies: Infrastructures and sectors considered pairs.
  - **N-order** dependencies: Infrastructures viewed as chains.
- The dependencies are further examined to identify potential cascading effects.

- Future steps include:
  - Further analysis of the dependency graphs.
  - Adoption of graph analysis algorithms to identify the most critical paths of dependencies.
  - Provide ways to reduce risk by exploring alternative paths in dependency graph.

References

1. Crowther, K. (2008). Decentralized risk management for strategic preparedness of critical infrastructure through decomposition of the inoperability input-output model. In: International Journal of Critical Infrastructure Protection, 1, 53–67.
2. De Porcellinis, S., Oliva, G., Panzieri, S., & Setola, R. (2009). A holistic-reductionistic approach for modeling dependencies. In: Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection, 215-227, Springer.
3. Kotzanikolaou, P., Theoharidou, M., & Gritzalis, D. (2013). Accessing n-order dependencies between critical infrastructures. In: International Journal of Critical Infrastructures, 9(1-2), 93-110.
4. Kotzanikolaou, P., Theoharidou, M., & Gritzalis, D. (2011). Dependencies between critical infrastructures: Analyzing the risk of cascading effects. In: Proc. of the 6th International Conference on Critical Infrastructure Security, 107-118, Springer.
5. Kröger, W. (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. In: Reliability Engineering & System Safety, 93(12), 1781–1787.
6. Nieuwenhuijs, A., Luiijf, E., & Klaver, M. (2008). Modeling dependencies in critical infrastructures. In: Critical infrastructure Protection, 205-214, Springer.
7. Setola, R., De Porcellinis, S., & Sforna, M. (2009). Critical infrastructure dependency assessment using the input-output inoperability model. In: International Journal of Critical Infrastructure Protection, 2(4), 170–178.
8. Theoharidou, M., Kotzanikolaou, P., & Gritzalis, D. (2009). Risk-based criticality analysis. In: Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection, 35-49, Springer.
9. Theoharidou, M., Kotzanikolaou, P., & Gritzalis, D. (2010). A multi-layer criticality assessment methodology based on dependencies. In: Computers & Security, 29(6), 643–658.
10. Theoharidou, M., Kotzanikolaou, P., & Gritzalis, D. (2011). Risk assessment methodology for dependent critical infrastructures. In: International Journal of Risk Assessment and Management, 15(2/3), 128–148.
11. Utne, I. B., Hokstad, P., & Vatn J. (2011). A method for risk modeling of interdependencies in critical infrastructures. In: Reliability Engineering & System Safety, 96(6), 671-678.
12. Virvilis, N., Dritsas, S., & Gritzalis, D. (2011). Secure Cloud Storage: Available Infrastructure and Architecture Review and Evaluation. In: Proc. of the 8th International Conference on Trust, Privacy & Security in Digital Business, 74-85, Springer.
13. Zio, E., & Sansavini, G. (2011). Modeling interdependent network systems for identifying cascade-safe operating margins. In: Transactions on Reliability, 60(1), 94–101.