

# Critical infrastructure interdependencies: The nervous system of a technologically developed country and how to protect it



George Stergiopoulos  
November 2015

# Critical infrastructure interdependencies: The nervous system of a technologically developed country and how to protect it

eLife-2015 Congress  
Athens, Greece  
November 2015



**ΟΠΑ**  
AUEB

**George Stergiopoulos**

Information Security & Critical Infrastructure Protection Laboratory  
Dept. of Informatics | Athens University of Economics & Business

# Critical Infrastructures:

The heart of a technologically developed country

**Critical Infrastructure (CI):** *“Asset or system essential for the maintenance of vital societal functions”.*

- **Damage** to a critical infrastructure, **destruction** or **disruption** by natural disasters, terrorism, criminal activity or malicious behavior, may have a **significant negative impact** for the **security** of the EU and the **well-being** of its citizens.  
*(Directorate-General of Migration and Home Affairs, the European Commission)*

**Backbone** of a nation's economy, security and health.

- Provide **Energy** and **Transport**
- Support **transportation** and **communication** systems
- Must be **protected** against all types of **hazards** along with their services and systems
- **Failures** can be **cross-border**. Particular valid in Europe since many Member States are affected (e.g. blackouts)



# Critical Infrastructures: The heart of a technologically developed country



Synopsis of NISAC Modeling Capabilities (<http://www.sandia.gov/nisac/capabilities/>)



## **Basis:** A multi-risk dependency analysis methodology

**Infrastructure Dependency:** *“One-directional reliance of an asset, system, network, or collection thereof – within or across sectors – on an input, interaction, or other requirement from other sources in order to function properly”*

**Modeled** as graphs:

- Nodes depict infrastructures or components
- Edges depict infrastructure dependencies

**Estimations** quantify the *Impact* and *Likelihood* of a disruption

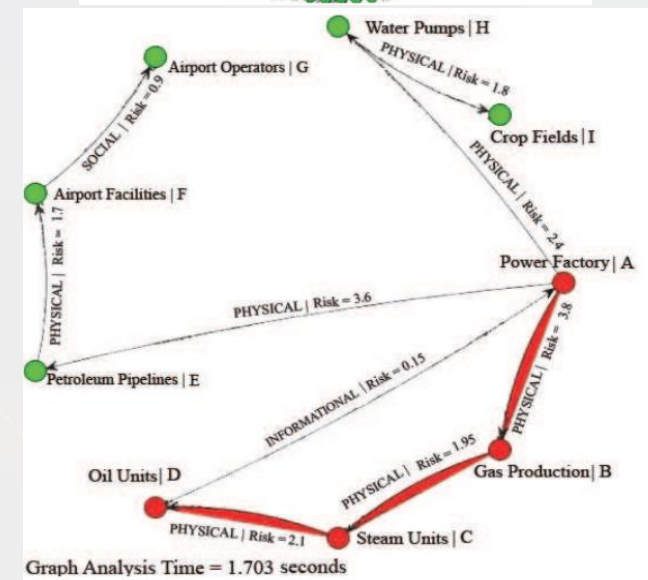
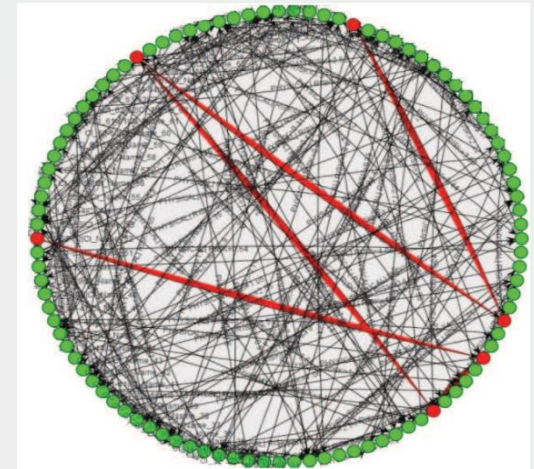
- Impact and Likelihood describe edges connecting CIs



# Current research: Time-based analysis of failures

## Critical Infrastructure Dependency Analysis (CIDA) tool

- Neo4J technology
- Developed using Java language
- Accepts risk assessment input
- Supports 17 different CI sectors, including communications, energy, transportation
- Computes risk for paths of connected CIS

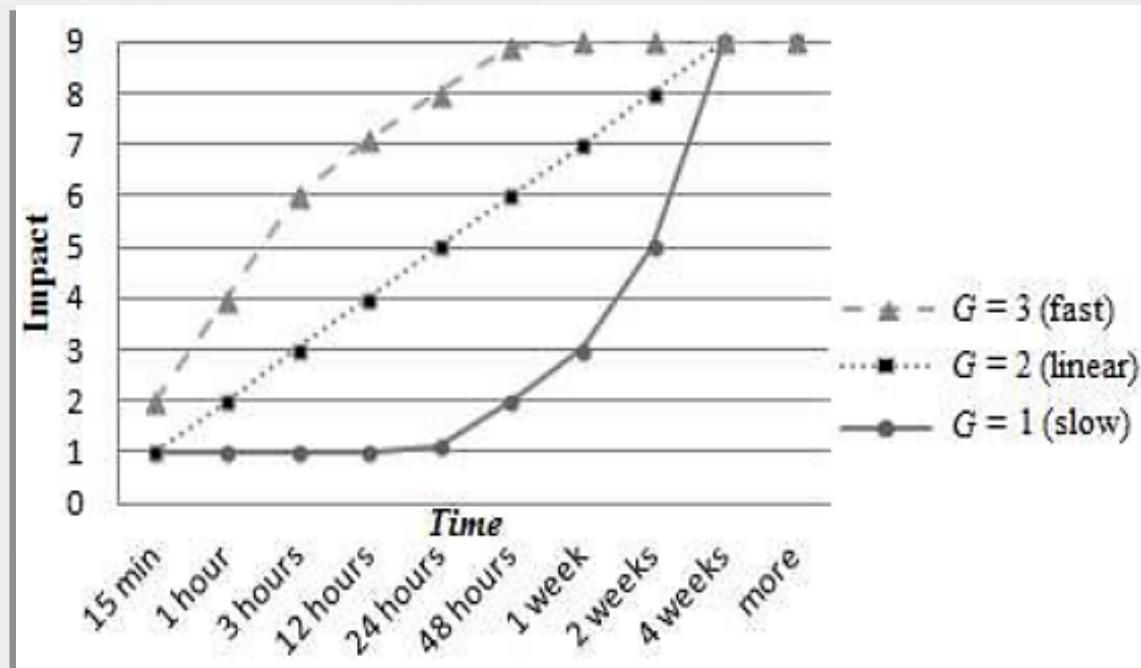


# Current research: Time-based analysis of failures

Gives estimate of **impact progression** from failures

- Impact worst-case scenario and Growth rate by risk assessment

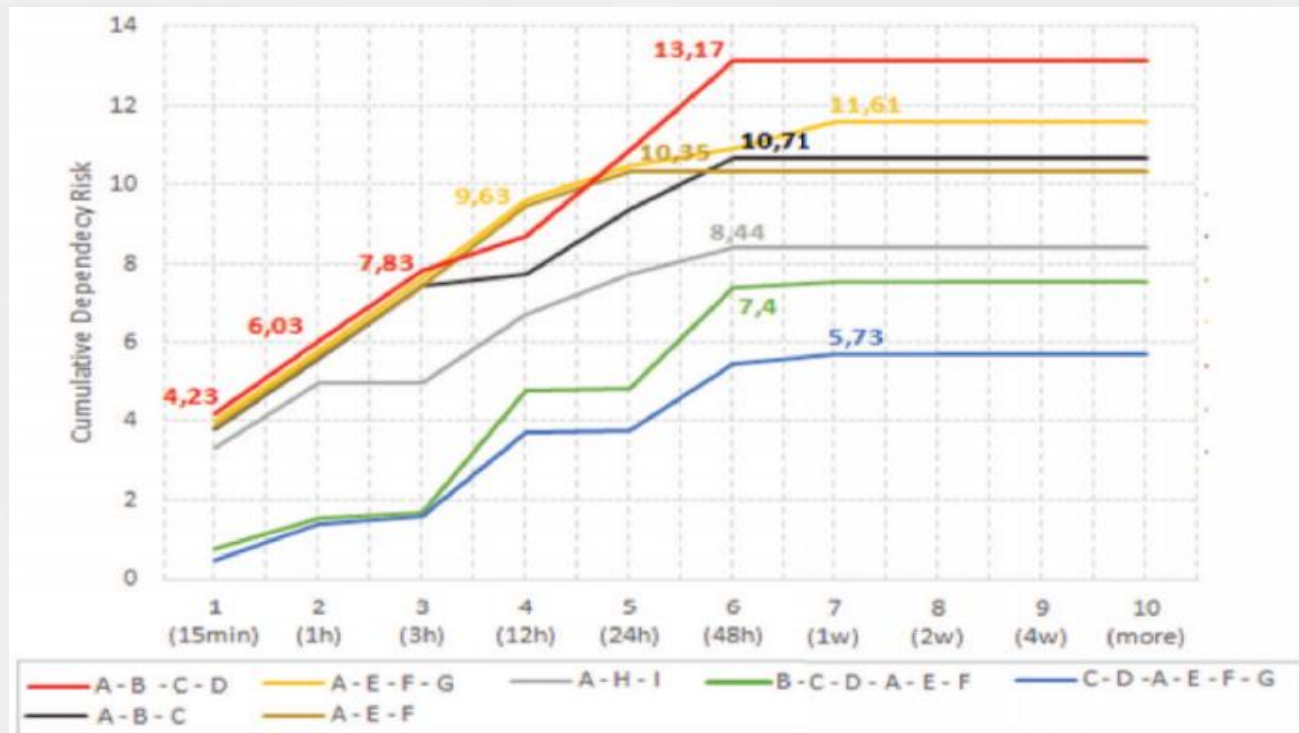
**Supports** slow, linear or fast evolution of impacts after failure



# Current research: Time-based analysis of failures

**Analysis** detects dangerous CI paths for each time slot

- Helps implement security controls – Decide where to focus
  - E.g. At 48h after initial failure, we must try saving CIs A-B-C
  - E.g. At 12h after initial failure, we must try saving CIs A-E-F-G



# Current research: Risk mitigation using graph theory

Use of **Graph Theory** to describe dangerous CI nodes

- Detects correlations between metrics with high values and nodes

**Tests** on 32,950 examples to find out which metrics to use

- 700 graphs with 774,015,270 paths

INFORMATION GAIN	Inbound Test	Outbound Test
Betweenness	0.259	0.277
Eccentricity	0.238	0.285
Closeness	0.387	0.345
Eigenvector	0.151	0.260
Intersection of all Centralities	0.176	0.248
Inbound degree (sinkholes)	-	0.302
Outbound degree	0.281	-

Table 1: Weka's output ranking using the Information Gain algorithm

GAIN RATIO	Inbound Test	Outbound Test
Betweenness	0.08	0.101
Eccentricity	0.08	0.101
Closeness	0.14	0.120
Eigenvector	0.06	0.09
Intersection of all Centralities	0.458	0.550
Inbound degree (sinkholes)	-	0.103
Outbound degree	0.101	-

Table 2: Weka's output ranking using the Gain Ratio algorithm



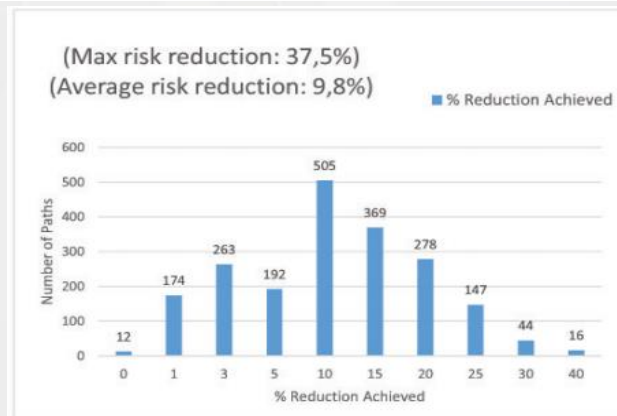
# Current research: Risk mitigation using graph theory

**Proposed algorithm** as a risk mitigation strategy that selects most dangerous CI nodes for risk mitigation

➤ **Evaluated** on 2000 random specialized experiments

<i>Risk Metrics</i>	<i>Strategies</i>	Information Gain	Top Initiators	Top Sinkholes
Most critical path		43.7% (max)	38.4% (max)	34.5% (max)
		12.1% (avg)	11.8% (avg)	10.3% (avg)
Top 20 critical paths		37.5% (max)	28.7% (max)	29.8% (max)
		9.8% (avg)	10.0% (avg)	7.3% (avg)
Entire graph		12.2% (max)	10.1% (max)	10.8% (max)
		7.5% (avg)	5.3% (avg)	6.7% (avg)

Table 3: Comparison of results from all mitigation strategies





# Research collaboration opportunities

- ✓ Nation-wide network of infrastructures can be studied via the **CIDA** tool and the **Risk mitigation mechanisms** presented.
- ✓ Contribution from risk assessment auditors and Public Infrastructures could **facilitate** further analysis of **national critical infrastructure dependencies**.
- ✓ New opportunities for practical **analysis** of **results** and **findings**.
- ✓ **Governments** could benefit from massive, automated **dependency analysis** offered by tools to help **predict nation-wide catastrophes**.



# General conclusions

- ✓ Major research opportunities do exist in the Critical Infrastructure research area between **interdependencies**, **risk assessment** and **failure detection**.
- ✓ All **initiatives** from the INFOSEC group **complement** each other.
- ✓ Each group publication helps **solve** a different **problem**:
  - ✓ Need for **time-based analysis** of **impact** evolution in failures
  - ✓ Need to **detect dangerous CI nodes** that greatly affect the **dependencies** of interconnected infrastructures
- ✓ **Test results** from both initiatives look promising when evaluated on **real-world** scenarios



## References

1. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Interdependencies between Critical Infrastructures: Analyzing the risk of cascading effects", in *Proc. of the 6<sup>th</sup> International Workshop on Critical Infrastructure Security*, pp. 107-118, Springer (LNCS 6983), Switzerland, 2011.
2. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Risk assessment of multi-order interdependencies between critical information and communication infrastructures", *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, pp. 151-170, IGI Global, 2013.
3. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Accessing n-order dependencies between critical infrastructures", *International Journal of Critical Infrastructure Protection*, Vol. 9, Nos. 1-2, pp. 93-110, 2013.
4. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Cascading effects of common-cause failures on Critical Infrastructures, in *Proc. of the 7<sup>th</sup> IFIP International Conference on Critical Infrastructure Protection*, pp. 171-182, Springer (AICT 417), USA, March 2013.
5. Stergiopoulos G., Kotzanikolaou P., Theoharidou M., Gritzalis D., *CIDA: Critical Infrastructure Dependency Analysis Tool*, <https://github.com/geostergiop/CIDA>, September 2014.
6. Stergiopoulos G., Theoharidou M., Kotzanikolaou P., Gritzalis D., "Using centrality measures in dependency risk graphs for efficient risk mitigation", in *Critical Infrastructure Protection IX*, pp. 25-40, Springer, 2015.
7. Stergiopoulos G., Kotzanikolaou P., Theoharidou M., Gritzalis D., "Risk mitigation strategies for Critical Infrastructures based on graph centrality analysis", *International Journal of Critical Infrastructure Protection*, September 2015.
8. Stergiopoulos G., Theoharidou M., Gritzalis D., "Using logical error detection in remote-terminal units to predict initiating events of Critical Infrastructures failures", in *Proc. of the 3<sup>rd</sup> International Conference on Human Aspects of Information Security, Privacy and Trust*, Springer (LNCS 9190), USA, August 2015.
9. Theoharidou M., Kandias M., Gritzalis D., "Securing Transportation-Critical Infrastructures: Trends and Perspectives", in *Proc. of the 7<sup>th</sup> IEEE International Conference in Global Security, Safety and Sustainability*, pp. 171-178, Springer (LNICST 99), Greece, 2012.
10. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk-based Criticality Analysis", in *Proc. of the 3<sup>rd</sup> IFIP International Conference on Critical Infrastructure Protection*, Springer, USA, March 2009.
11. Theoharidou M., Kotzanikolaou P., Gritzalis D., "A multi-layer criticality assessment methodology based on interdependencies", *Computers & Security*, Vol. 29, No. 6, pp. 643-658, 2010.
12. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk assessment methodology for interdependent Critical Infrastructures", *International Journal of Risk Assessment and Management*, Vol. 15, Nos. 2/3, pp. 128-148, 2011.