Advances in Critical Information Infrastructure Protection

George Stergiopoulos, Vasilis Stavrou

{geostergiop, stavrouv}@aueb.gr

Information Security and Critical Infrastructure Protection Research Laboratory

Dept. of Informatics, Athens University of Economics & Business (AUEB)

Critical Infrastructures (CI)

- Incapacity or destruction of systems and assets that would have a debilitating impact on [1]:
  - Security
  - National economic security
  - National public health or safety

  or any combination of those matters.

Risk analysis and Criticality analysis

- Impact is assessed under various terms, such as consequences, criticality, or vitality, and expressed with various criteria or factors [2].

- Criticality assessment has a more broad scope than risk assessment.
  - Captures the external, societal impacts.

Risk analysis vs. criticality analysis

	Risk Analysis	Criticality Analysis
Aim	Organization	Society
Scope	Internal assets	Internal assets and interdependencies
Impact Type	Organization-centric	Society-centric
Threats	System	CI and interdependencies
Vulnerabilities	System	CI and interdependencies
Impact Scale	Variable	Higher

Criticality assessment in large-scale environments

- Structured, multi-layer Criticality Assessment methodology [3] that takes into consideration the operator, the sector and the intra-sector layer.
- **Layer 1**: Operator risk assessment:
  - Evaluate possible impacts within the scope of the examined organization.
  - A CIO may consider both inside and outside threats.
- **Layer 2**: Sector risk assessment:
  - Cumulative impacts from the realization of various threats.
  - Dependencies with other sectors are examined.
- **Layer 3**: Intra-sector/National criticality assessment:
  - New form of risk assessment is required: criticality assessment.
  - Impacts external to a specific CIO, i.e. social/societal impacts, sector-wide impacts or impacts to people/citizens.

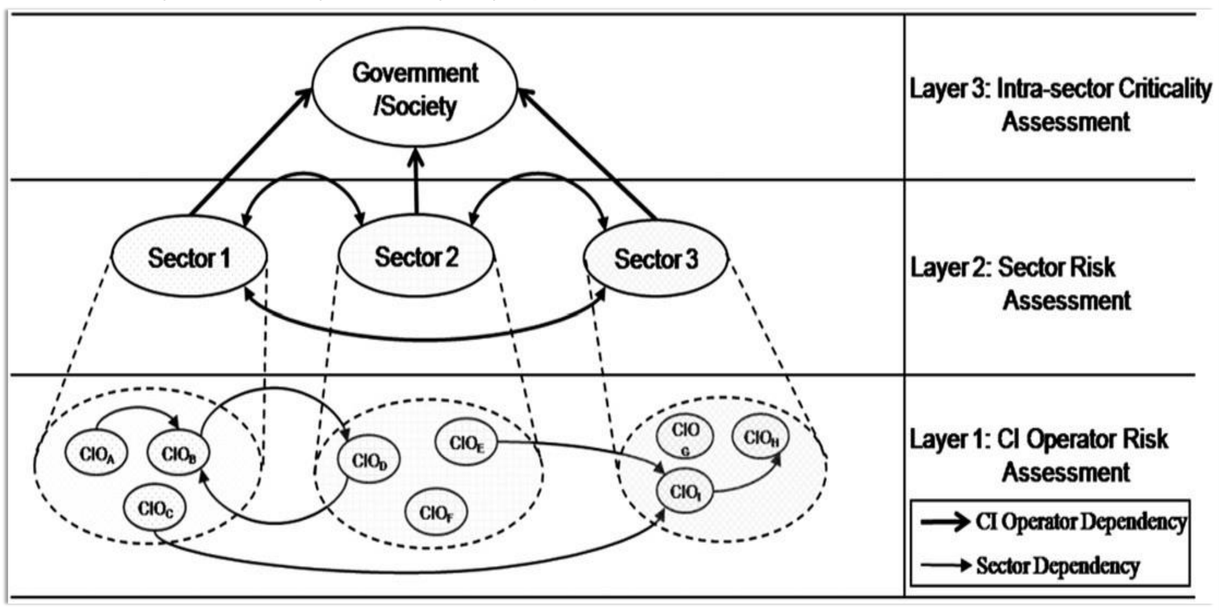

Fig 2. Three-layer criticality analysis

Criticality

- Total Impact for every applicable combination of a component, an incident-threat and a resulting effect to an infrastructure [4].

$$Criticality_I = Impact_I = \sum_{\forall c,th,e} Impact_I(c, th, e)$$

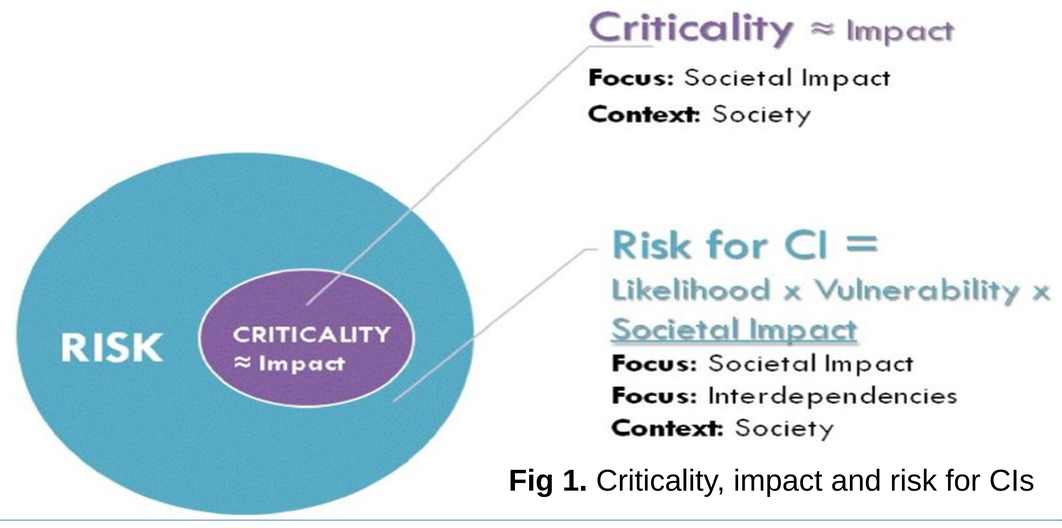

Fig 1. Criticality, impact and risk for CIs

Risk Assessment for interdependent CIs

- Improved methodology based on [3] for developing [4]:
  - Assesses Societal impact of an infrastructure or a sector.
  - Assesses Overall infrastructure risk, taking into account interdependencies.
  - Assesses Risk in three layers: the infrastructure level, the sector level and, finally, the national/intra-sector level.
  - Considers 1st-order dependencies and cannot assess complex chain effects.

Risk assessment of multi-order dependencies

- Proposed methodology [5] for multi-order dependencies:
  1. identify the initiating event.
  2. identify interdependencies and perform qualitative analysis.
  3. perform semi-quantitative assessment of the scenario.
  4. perform detailed quantitative analysis of interdependencies (optional).
  5. evaluate risk and measures to reduce interdependencies.
  6. perform cost/benefit analysis (optional).

Cascading Effects

- First-order outgoing risks in Operator level and societal risk.
- Dependency Risk Table summarizes dependencies [6] of each CI to others.
- Dependencies visualized through graphs.

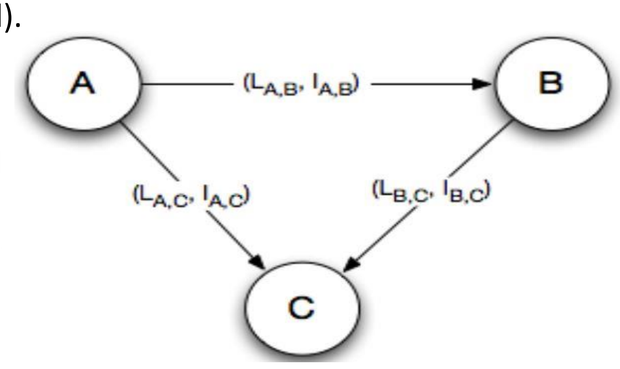

Fig 3. Three dependent infrastructures

Physical	• State of a CI depends upon the material output
Cyber/Informational	• State of a CI depends on information transmitted
Geographic	• State of a CI depends on an environmental event on another CI.
Logical	• State of a CI depends upon another CI via a nonphysical, cyber, or geographic connection.
Social	• State of a CI is affected by the spreading of disorder

Table 1. CI interdependencies

Conclusions

- The method of analyzing cascading effects [7] provides an efficient way to evaluate whether common-cause failures can propagate to infrastructures that are not directly affected by an examined common-cause threat.
- Assessment of likelihood, impact and risk is using five-item Likert scales [5].
  - Results from relevant approaches are incorporated in the assessment.
  - Risk assessment of n-order dependency requires computational resources if nodes of the dependency graph increase significantly.
- Dependencies examined on a normal mode of operation. Different analysis is required when examining stress, crisis or restoration modes of operation.
- Critical infrastructure protection methods have a severe positive impact on the protection of several security-critical applications. [9-12].
- Critical infrastructure protection fits well and builds upon our Laboratory record on information security.

References

1. Rinaldi, S., "Modeling and simulating critical infrastructures and their interdependencies", Proc. of the 37th Annual Hawaii International Conference on System Sciences, IEEE, USA, 2004.
2. Theoharidou, M., Kotzanikolaou, P., Gritzalis, D., "Risk-based Criticality Analysis", Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection, Springer, USA, 2009.
3. 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.
4. 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.
5. 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.
6. Kotzanikolaou, P., Theoharidou, M., Gritzalis, D., "Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects", Proc. of the 6th International Workshop on Critical Infrastructure Security, pp. 107-118, Springer (LNCS 6983), Swiss, 2011.
7. Kotzanikolaou, P., Theoharidou, M., Gritzalis, D., "Cascading effects of common-cause failures on Critical Infrastructures, Proc. of the 7th IFIP International Conference on Critical Infrastructure Protection, Springer, USA, 2013.
8. 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, 2013.
9. Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., Gritzalis, D., "An Insider Threat Prediction Model", Proc. of the 7th International Conference on Trust, Privacy, and Security in Digital Business, pp. 26-37, Springer (LNCS 6264), Spain, 2010.
10. Soupionis, Y., Gritzalis, D., "Audio CAPTCHA: Existing solutions assessment and a new implementation for VoIP telephony", Computers & Security, vol. 29, no. 5, pp. 603-618, 2010.
11. Mylonas, A., Dritsas, S., Tsoumas, B., Gritzalis, D., "On the feasibility of malware attacks in smartphone platforms", Proc. of the 9th International Conference on Security and Cryptography, 217-232, Lecture Notes (CCIS 314), Springer, Spain, 2012.
12. Theoharidou, M., Kandias, M., Gritzalis, D., "Securing Transportation-Critical Infrastructures: Trends and Perspectives", Proc. of the 7th IEEE International Conference in Global Security, Safety and Sustainability, pp. 171-178, Springer (LNICST 0099), Greece, 2012.