Critical Infrastructure Protection Tools: A survey

Efstratios Vasilellis, George Stergiopoulos

p3110024, svasilellis@hotmail.com , geostergiop@aueb.gr

Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory

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

Critical Infrastructure Protection (CIP) is a very important process not only from an economic perspective but also from a societal one as well. This is due to the significant impact caused by disruption or malfunction of services in Critical Infrastructures (Cis). Experience and research has proved that failures in CIs cascade from one to another, whether they stem from natural disasters or terrorist attacks. This can greatly increase the magnitude of impact of each failure. Cascading effects are driven by interdependencies among infrastructure sectors. In this thesis, we are going to compare software according to their functionality and purpose at the different stages of risk management framework as well as according to the technical approach that was used during their development

Definitions

In order to comprehend the main section of our results it is vital to explain the next definitions of the functionality classification [2]:

- **Risk Identification (RI)**: Tools can provide identification of not only non-technical but also technical threats to infrastructure system in both local and regional geographic scope.

- **Risk Impact Assessment (RIA)**: Tools can provide risk measurement against its likelihood of occurrence as well as the severity of its impacts according to some predefined scales for each asset. As a result, decisions based on risk assessments may end in either ignoring or managing the threats.

- **Risk Prioritization (RP)**: Tools can provide identification where risk reduction is more compelling in order to determine the appropriate proactive measures needed to be taken. In order to achieve this, a comparison of relative risk levels and resource sectors, together with options for achieving security goals are required. As a result, the proactive measures are applied where there is possibility of reducing security risk, and thus have a more cost-effective decision.

- **Risk Mitigation Planning (RMP)**: Tools can provide implementation of protection programs and measures which aim at risk reduction.

- **Effectiveness Evaluation (EE)**: Tools can provide measures of how effective the implemented strategies where, according to a system of indicators that provide information whether the specific security goal was achieved. These indicators are both descriptive as well as process-based.

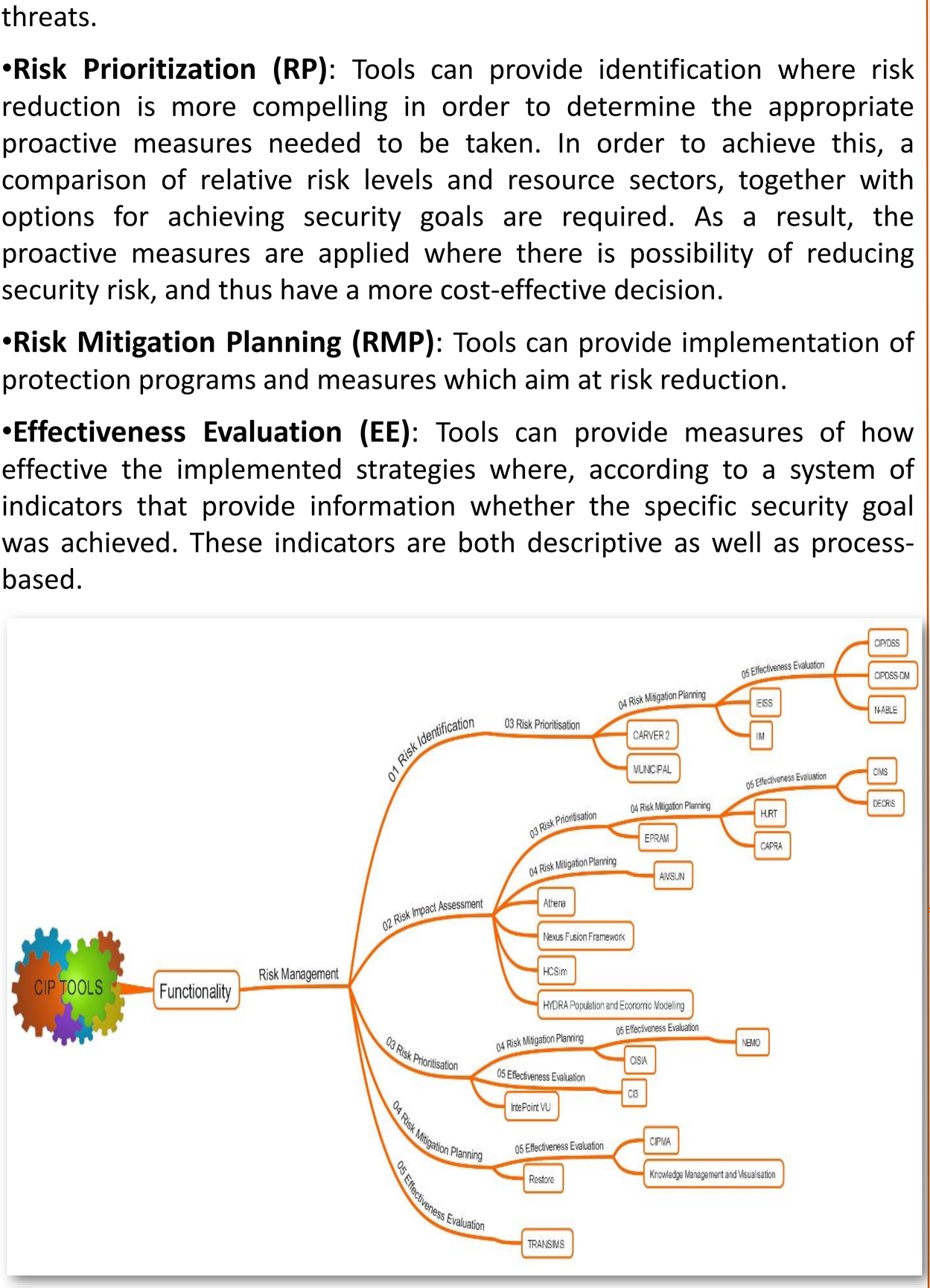

***Figure 1**: Classification of tools according to their functionality*

There are different kinds of modelling techniques which are used by different methodologies and are applied to CIP which include multi-agent systems, system dynamics, rating matrices, relational databases and network theory. Those modeling techniques are also combined with supplementary computational techniques like continuous time-step simulation, discrete time-step simulation, Monte Carlo simulation, decision trees, geographic information techniques, risk management techniques as well as event or real time record. [2]

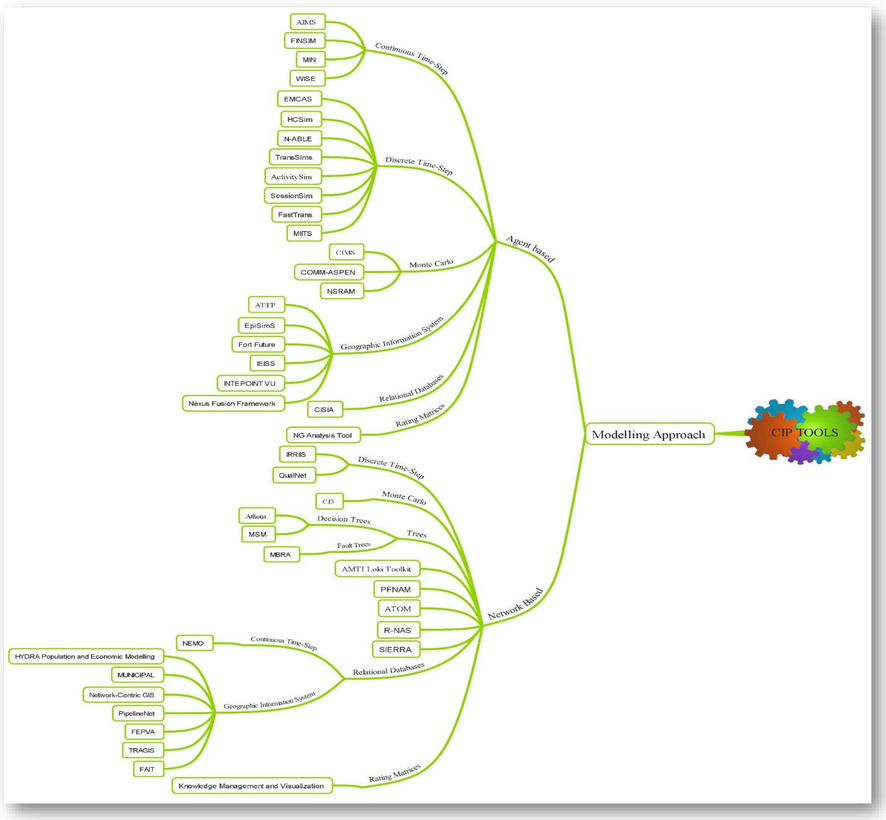

***Figure 2**: Classification of tools according to their modelling approach*

CIP tools categorization

Our results are mainly presented on a table. ***Table 1*** shows an example of this presentation. Each tool's functionality, modelling approach and sectors that affiliates with, are presented.

Application/ Methodology	Modelling approach	Functionality	Infrastructure Sector
CIMS	Agent Based, MC	RIA, RP, RMP,EE	CF, C, E, HPH, TS

***Table 1**: CIP Applications and Methodologies*

Conclusions and Results

This poster is a contribution review of the capabilities of various not only strategies and applications, but also methodologies which are used for both identification and evaluation or risks that occur in critical infrastructure. Emphasis has been put on the comparison of similar tools from the perspective of their functionality and modelling approach. Our research showed that there is not a unique approach to protect critical infrastructures, but there is always great necessity of interdependencies analysis in order to understand the interconnections which exist between multiple critical infrastructures, and by ignoring this we might have a debilitating effect upon our results.

References

1. Pederson P., Dudenhoeffer D., Permann M., Hartley S., "Critical Infrastructure Interdependency Modeling: A Survey of US and International Research", Idaho National Laboratory, August 2006.
2. Yusta J., Correa G., Lacal-Arántegui R., "Methodologies and applications for critical infrastructure protection: State-of-the-art", *Energy Policy*, 39(10), pp. 6100-6119, 2011.
3. Dudenhoeffer D., Permann M., Manic M., "CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis".
4. Kandias M., Mylonas A., Theocharidou M., Gritzalis D., "Exploitation of auctions for outsourcing security-critical projects", in *Proc. of the 16th IEEE Symposium on Computers and Communications*, pp. 646-651, Greece, 2011.
5. Kotzanikolaou P., Theocharidou 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.
6. Kotzanikolaou P., Theocharidou M., Gritzalis D., "Accessing n-order dependencies between critical infrastructures", *International Journal of Critical Infrastructure Protection*, Vol. 9, No. 1-2, pp. 93-110, 2013.
7. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk assessment methodology for interdependent critical infrastructures", *International Journal of Risk Assessment and Management*, 2011.
8. Theocharidou M., Kandias M., Gritzalis D., "Securing Transportation-Critical Infrastructures: Trends and Perspectives", in *Proc. of the 7th IEEE International Conference in Global Security, Safety and Sustainability*, pp. 171-178, Springer, 2012.
9. Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Lykou G., Gritzalis D., "Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures", *International Journal of Critical Infrastructure Protection*, March 2016.