S.M. Elkabets, I.M. Shohet. ***Risk management model for critical infrastructures.*** *Gerontechnology 2012;11(2):164;* doi:10.4017/gt.2012.11.02.407.00 **Purpose** Modern societies are increasingly dependent on the successful provision of critical services delivered through critical infrastructures (CIs). CIs consists of systems that, if disrupted or destroyed, have a major impact on the health, safety, security, and wellbeing of society, or on the effective performance of governments[1]. Each infrastructure is in itself a complex system; when grouped together these systems become highly interconnected and mutually dependent, and because of that extreme events cause rippling and cascading effects of CIs. During the last few decades terrorism and physical attacks on CIs (particularly government, military, commercial and public buildings) have continued to increase. This is a concern for the safety of the CIs and the nations' stability and economic wellbeing. **Method** The paper proposes a quantitative ‘triple R analysis’ risk analysis model to determine the most effective protective strategy (resilience, robustness, or redundancy) to reduce risk to CIs under extreme events caused by terror threats. The triple-R risk model consists of four principal phases: (i) scenario analysis, (ii) threat assessment, (iii) security vulnerability assessment, and (iv) consequence analysis. The method includes implementation of quantitative methods such as stochastic simulation, game theory, fault-tree-analysis (FTA), and probabilistic-risk-analysis (PRA), and an analysis of the trade-offs between resilience, robustness, and redundancy. A function named ‘total cost of protective effectiveness’ (*Figure 1*) was developed and implemented in energy CIs. **Results & Discussion** A case study on electric power transmission station was carried out to demonstrate and examine the applicability of the proposed model[2]. The results of the methodology show that the risk in CIs may be reduced by as much as half of the risk without additional protective measures[3-4].

References

1. Haimes Y, Barker K. Assessing uncertainty in extreme event: Applications to risk-based decision making in interdependent infrastructure sectors. Reliability Engineering and System Safety 2009;94:819-829
2. Silvano C, Di Giandomenico F, Lollini P. Definition, implementation and application of a model-based framework for analyzing interdependencies in electric power systems. International Journal of Critical Infrastructure Protection 2010;3:1230-1269
3. Utne IB, Hokstad P, Vatn J. A method for risk modeling of interdependencies in critical infrastructures. Reliability Engineering and System Safety 2011;96:671–678
4. Yoshida M, Kobayashi K. Disclosure Strategies for critical Infrastructure against Terror Attacks. Risk Analysis 2010;97(7):3194-3199

Keywords: information technology, risk, resilience, redundancy, robustness

Affiliation: Ben-Gurion University of the Negev, Be’er Sheva, Israel; *E:* @bgumail.bgu.ac.il

Full paper: No

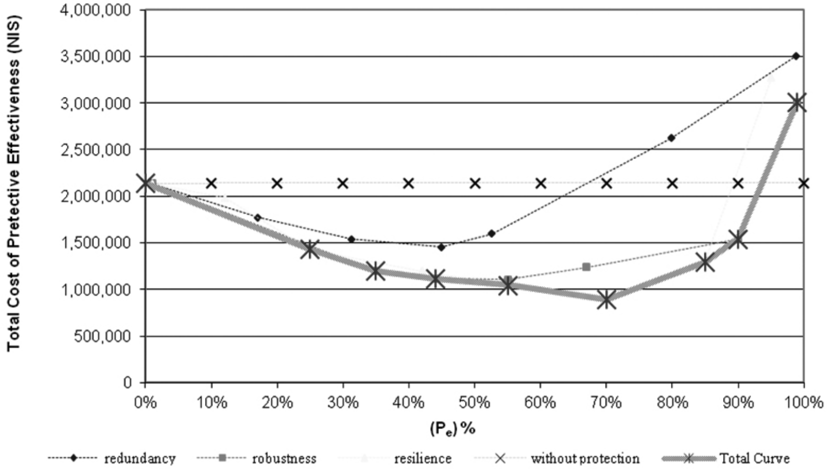

Figure 1. Total Cost of Protective Effectiveness for Energy Critical Infrastructures – Trade-offs between redundancy, Robustness and resilience