Quantitative and qualitative differences worth considering in approaching critical infrastructures resilience

Dorel Badea[1,*], *Ghiță* Bârsan[1], *Ioan* Virca[1], and *Dumitru* Iancu[2]

[1] "Nicolae Bălcescu" Land Forces Academy, Department of Technical Sciences, 550170 Revoluției 3-5, Sibiu, Romania
[2]"Nicolae Bălcescu" Land Forces Academy, Department of Management and Administrative Sciences, 550170 Revoluției 3-5, Sibiu, Romania

Abstract. Through the implicit connections between risk, safety, protection and, last but not least, resiliency, that need to be managed, critical infrastructures have become a subject of increasing interest both for specialists and for academics. Based on this premise, this article analyzes in terms of operational performance several internationally used solutions for assessing resilience, having in view the desire to choose the best in order to be presented in some specialized disciplines of the postgraduate curricula that are annually presented in the educational offer of the Land Forces Academy. The authors also present their own vision on approaching the resilience of critical infrastructures so that it can harmoniously be integrated into the security plans of the holders or operators of such special assets.

1 Theoretical considerations

For all humanity, especially after the 2000s, it has become clear that the sources of dysfunctionality, seriously affecting the development of society, are no longer of a strictly military nature, others manifesting themselves intensively and extensively, with at least disturbing effects in terms of ensuring continuity in the daily activities. Reconsidering the role and importance of critical infrastructures has thus become more than a necessity, the volume of the works elaborated in the field of applied scientific research being an indicator in this sense. However, one can state that there is a convergence trend for certain points of view concerning issues specific to critical infrastructures, but at the same time complex issues that will be clarified in years ahead. In this context, we bring into discussion concepts such as security, protection, resilience, and lay stress on their complementary character, our objective being to focus our attention on the last concept in the previous enumeration.

National Infrastructure Advisory Council [1] approaches resilience of critical infrastructures as being the capacity to reduce the amplitude and/or duration of certain disturbing events, offering details on the fact that the efficiency of an infrastructure or

* Corresponding author: dorel.badea@yahoo.com

organization resilience depends on its capacity of anticipating, absorbing, adapting to and/or quickly recovering after the emergence of a disturbing event. But the problem consists in approaching resilience on the basis of a SMART determination, the results of the research carried out especially at European level (CIPRNet - Critical Infrastructure Preparedness and Resilience Research Network; CRISADMIN - Critical Infrastructure Simulation of Advanced Models on Interconnected Networks Resilience) or in the United States, still not converging towards a certain standard methodology.

The difficulty lies in providing some series of input data that are simulated based on robust models and allow for *what if* type of analyses. For a national approach, in the work coordinated by G. Bârsan, A.Dinicu and D.Badea [2], an annual questionnaire-based research is proposed, applied to all critical infrastructure operators through which information is to be collected on:
- the number of events recorded in the reference period,
- the average time to restore the functionality of infrastructure, important factors influencing the performance (implementation of risk management standards, SCADA state of equipment readiness, staff participation in specialized training activities, etc.),
- the staffing (by management and execution category) in the reference period (existing/required), number of training exercises conducted to simulate scenarios.

Basically, qualitative information is translated into quantitative information, which, after being compared with some specific data characterizing the existence of that system, becomes subject to processing by software and specialized tools. Acknowledging the fact that through the first research model mentioned we just try to understand some patterns of behavior, motivations, opinions and attitudes - and, subsequently, the results can be interpreted only in a certain context. The component of numerical data is the defining element of the quantitative research, and these data are obtained both in real environments and in laboratory conditions, the quantitative analysis methodology being used very often.

2 Combining qualitative and quantitative components in approaching resilience of critical infrastructures

In this section of the paper we started from the hypothesis absolutely accepted in the literature in the field, according to which the protection of critical infrastructures cannot be ensured 100%. Subsequently, we consider that the solutions that address resilience do not yet have a high level of robustness, regardless of the methods applied and the computer instruments used, simplifying working models being necessary. In this framework, as an applied study, we chose to investigate the possibilities offered by the Analytic hierarchy process (AHP) method. The principle of AHP method consists in converting some subjective assessments made on the relative importance of some criteria into scores and weights. The method, developed by Saaty in 1980 [3], proved to be the most popular form of multi-criteria analysis, being used in many types of applications in different fields. The input data for the specific AHP algorithm are answers to interrogations such as "How important is criterion A relative to criterion B?" So comparisons in pairs are obtained, giving scores or weights, which will determine the final decision. According to the desideratum assumed by the title of the article, one should emphasize that this method does not take into account the alternatives upon which the criteria are applied in order to calculate the importance coefficients (weights) of the criteria. In most of the situations encountered in reality, both qualitative and quantitative criteria appear, the latter being normally expressed in different units of measure, so the question of the non-homogeneity of criteria is being raised. [4]

The created scenario brings into attention an institution holding regionally valuable critical infrastructures, which, given the legislative imperatives at EU and national level, as

well as the history of security incidents that took place in the past, sets as its primary goal the carrying out of a reengineering stage based on the implementation of an appropriate strategy.

Table 1. Presentation of taken into account strategies and criteria

Criteria	**Types of strategies**		
	Technology-based	Human resource-based	Procedure-based
Robustness	The extensive use of SCADA systems is considered, with state-of-the-art automatic and sensorization elements, that ensure good interoperability with other systems up and down the interdependency chain and, at the same time, a reduced time for detecting deficiencies. Integration within expert decisional systems is also considered.	It will focus on an intensive training system of employees within a basic component providing general competences for a systemic, technical and operational understanding of the issues related to critical infrastructures, and a specialty component stressing the operational particularities of the system itself. It insists on the employees' becoming aware of their roles within the system.	The focus is on the standard operating procedures for a various range of dysfunctions, approached in an integrative manner within the specific plan of risk management system. The need of being clearly defined in the form of a viable algorithm is made aware of, no major changes being necessary when social-technical modifications take place.
Necessary initial investments			
Operational compatibility with other interdependent critical systems			
Reaction capacity			

After carrying out an audit, a firm specializing in consultancy on industrial security concludes that the strategic objective must be to ensure resilience and proposes three technology-based strategies, people and procedures, with common and differentiation elements, as shown in table 1, being the general manager's responsibility to decide (Figure 1) which of the options presented should be implemented.

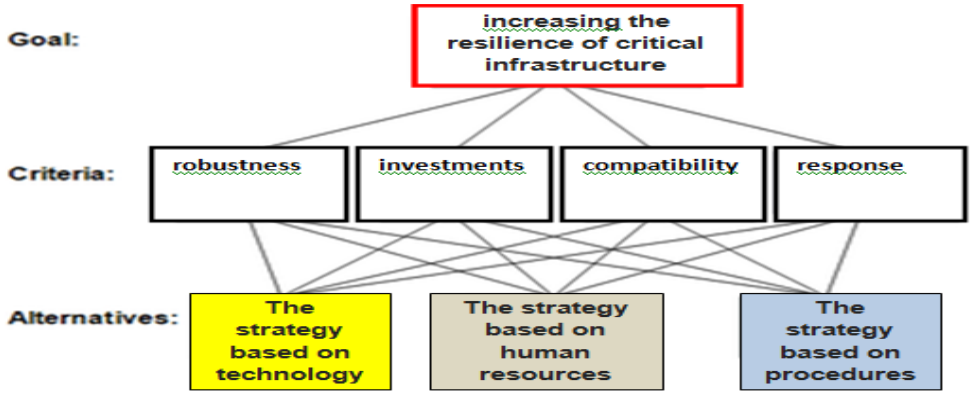

Fig. 1. The created decisional method

According to the AHP methodology and to an often cited and used practical example [5], the three strategies will be compared, each with each, relative to the four criteria considered, and based on the method of assigning weights shown in Table 2.

Table 2. Methodology of assigning [6]

The Fundamental Scale for Pairwise Comparisons		
Intensity of Importance	**Definition**	**Explanation**
1	**Equal importance**	Two elements contribute equally to the objective
3	**Moderate importance**	Experience and judgment moderately favor one element over another
5	**Strong importance**	Experience and judgment strongly favor one element over another
7	**Very strong importance**	One element is favored very strongly over another; its dominance is demonstrated in practice
9	**Extreme importance**	The evidence favoring one element over another is the highest possible order of affirmation
Intensities of 2, 4, 6 and 8 can be used to express intermediate values. Intensities of 1.1, 1.2, 1.3, etc. can be used for elements that are very close in importance.		

The final results obtained after going through the steps of the AHP method are shown in Table 3. According to the scores and given the scenario created, the best decision is to apply the human resource-based strategy in order to achieve the objective of increasing the resilience of a critical infrastructure.

Table 3. Centralizing the scores obtained for each strategy

Strategies	Criterion	Criterion Weight	S's weight	Weighted Score
S/Technol.	*Robustness*	0.550	0.163	0.089
	Investments	0.034	0.308	0.010
	Compatibility	0.177	0.151	0.026
	Response	0.236	0.100	0.023
				SECOND BEST - SUM 0.151
S/Hum.Res.	*Robustness*	0.550	0.539	0.297
	Investments	0.034	0.109	0.003
	Compatibility	0.177	0.630	0.112
	Response	0.236	0.673	0.159
				BEST - SUM 0.572
S/Proced.	*Robustness*	0.550	0.296	0.163
	Investments	0.034	0.581	0.020
	Compatibility	0.177	0.218	0.038
	Response	0.236	0.225	0.053
				LAST - SUM 0.275

3 Conclusions

Although useful especially in a situation with a large number of alternatives and criteria, the method involves a level of substantial subjectivity, starting with the first stage when the alternative strategies were compared based on each separate criterion (e.g. comparison relative to robustness, understood as viability over time, the technology-based strategy was assessed with a weight of 6-1 compared with the human resource-based strategy).

Further sensitivity analyses may contribute to increasing the relevance of the analysis. Specifically, the approach of resilience can only be made by using simplifying representations, being the only option to reduce complexity for research purposes, which was comprehensively highlighted by Roland Pulfer and Olga Bucovetchi [7]: "Making complexity transparent and manageable is the key factor to support innovation, to guarantee that innovation can be implemented into practice, to apply the highest professionalism and

to recognize and apply possibilities for improvement." As a didactic value, this scientific approach can form the basis for laboratory work at the discipline Protection of critical Infrastructures.

Case studies within the postgraduate program organized in the institution, in which individual analyses can be conducted on the excel format that has been used for this study in order to investigate the range of values within which the optimal solution can vary and, at the same time, some principles of analysis can be established for reducing the bias in comparing in pairs.

References

1. ***, NIAC: *A Framework for Establishing Critical Infrastructure Resilience Goals,* National Infrastructure Advisory Council (2010)
2. G.Bârsan, A. Dinicu, D. Badea, (coordinators), *Analiza şi modelarea conceptuală a situaţiilor complexe – studii interdisciplinare,* ("Nicolae Bălcescu" Land Forces Academy Publishing House, Sibiu, 2016)
3. T.L.Saaty, *The Analytic Hierarchy Process*, (McGraw-Hill, New York, 1980)
4. S.L. Constantin, B.V. Constantin, *Methodology based on AHP for choosing between GPRS, UMTS and WLAN* article available at: http://www.agir.ro/buletine/859.pdf, retrieved on 22.02.2017
5. www.ccunix.ccu.edu.tw/.../AHP/AHP1%20Example%201%, retrieved on 22.02.2017
6. https://en.wikipedia.org/wiki/Analytic_hierarchy_process_%, retrieved on 22.02.2017
7. R. Pulfer, O. Bucovetchi, Sci. Bull., Series B, Vol. 78, Iss. **4**, 140 (2016)