VULNERABILITY ANALYSIS IN CRITICAL INFRASTRUCTURES: A METHODOLOGY

António Carlos dos Santos Ferreira
Major / Military Engineer
Portuguese Military University Institute
ferreira.acs@ium.pt

INTRODUCTION

Vulnerability analysis is a key aspect for the development of methodologies to define the levels of protection in critical infrastructures (CI). This article is the result of an investigation that seeks to discuss the concept of vulnerability the methodologies and processes for its assessment in CI facing terrorist threat, with particular focus on the development of an analysis model, exploring a multicriteria method in support to decision, in order to limit the risks in the maximum extent possible.

Through a qualitative research methodology, based on the analysis dimensions *Threat* and *Infrastructure* and their respective variables, we attempted to conceptualize the vulnerability, after which we proceeded to identify, characterize and analyze the variables in order to be able to categorize those dimensions, identifying posible factors of analysis. Based on the analyzed dimensions and variables, an algorithm was modeled and tools were created to transform qualitative judgments into quantitative assessments.

CONCEPTUAL FRAMEWORK

There are two interpretations of the vulnerability's concept. One is that vulnerability consists on combining the attractiveness of na infrastructure as a target and the level of deterrence or protection provided by existing countermeasures (Renfroeand Smith, 2016), in other words, represents the probability of success of an attack. Almeida, citing Apostolakis and Lemon (2003:362), defines vulnerability as the "expression of inherent states of the system (whether physical, technical, organizational, cultural) that can be exploited by adversaries to damage or cause damage to the system" (2011, p.15). In this second aspect, vulnerability emerges as a characteristic (physical, procedural, etc.) of the infrastructure that can be exploited by the threat, that is, a weakness. Although they are two distinct concepts, the first, a general concept and the second, a particular concept, they are mutually complementary.

Vulnerability analysis is the process that a commander or a person in charge of a critical infrastructure employs to determine the susceptibility of an infrastructure to a terrorist's attack or, by other words, the likelihood of success of an attack.

VULNERABILITY ANALYSIS MODEL

In order to determine the vulnerability of a CI, it is necessary to apply a methodology, based on a sequential, interactive, analytical and algebraic algorithm, to transform the qualitative judgments obtained from the threat and infrastructure assessment into quantitative values that can be used, analitically, to determine, in percentage, the probability of success of a terrorist attack using explosive devices against the CI.

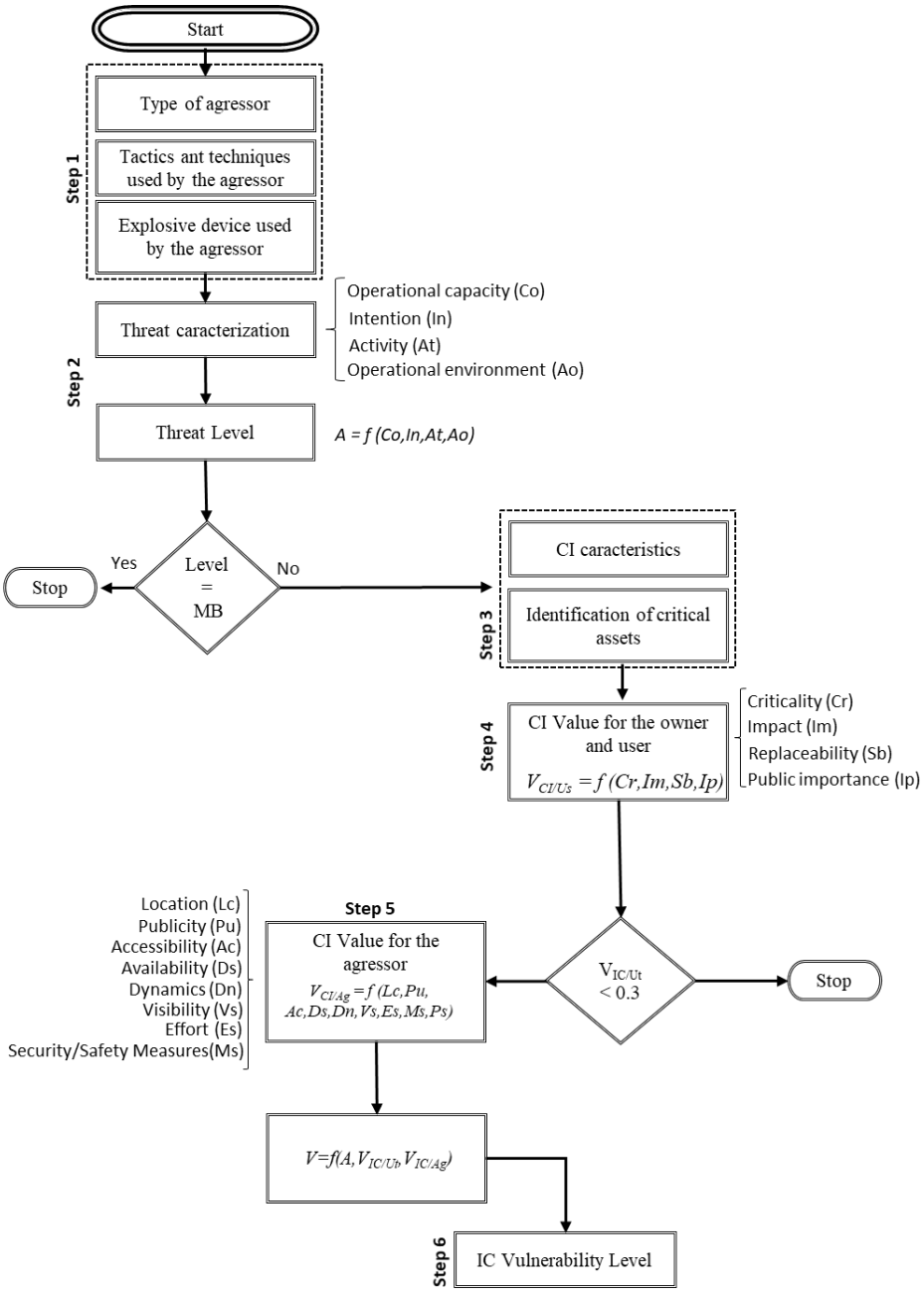

Figure 1 – Algorithmic model for vulnerability analysis

Source: (Author, 2018)

Thus, vulnerability is a value dependent on the probability of success of an attack (Morgesonet al, 2011, p. 24):

$$Vulnerability\ (V) = Probability\ (Success|Attack)$$

$$\boldsymbol{V = P(S|A)} \qquad (1)$$

The calculation of its value is directly related to the level of threat (A), to the value of the CI for the user ($\boldsymbol{V_{CI/Us}}$) and to the value of the CI for the agressor ($\boldsymbol{V_{CI/Ag}}$).

In an algebraic form:

$$V=P(S|A) \rightarrow \boldsymbol{V=f(A,V_{CI/Us},V_{CI/Ag})} \rightarrow V=\sum (A,V_{CI/Us},V_{CI/Ag}), \qquad (2)$$

Wherein:

(1) The threat level (A) is obtained in function of four factors: Operational capability (Co), Intention (In), Activity (At) and Operational environment (Ao):

$$\boldsymbol{A = f\ (Co,In,At,Ao)} \rightarrow A = \sum (Co,In,At,Ao) \qquad (3)$$

(2) The value that the CI has for the user is determined by four factors: criticality (Cr), impact (Im), replaceability (Sb)and public importance (Ip):

$$\boldsymbol{V_{IC/Ut} = f\ (Cr,Im,Sb,Ip)} \rightarrow V_{IC/Ut}=\frac{\sum(Cr,Im,Sb,Ip)}{\sum Max(Cr,Im,Sb,Ip)} \qquad (4)$$

(3) The value that the IC has for the terroristis a function of eight factors: location (Lc), publicity (Pu), accessibility (Ac), availability (Ds), dynamics (Dn), visibility (Vs), effort (Es)and security and safety measures (Ms):

$$\boldsymbol{V_{IC/Ag} = f\ (Lc,Pu,Ac,Ds,Dn,Vs,Es,Ms)} \rightarrow V_{IC/Ag}= \frac{\sum(Lc,Pu,Ac,Ds,Dn,Vs,Es,Ms)}{\sum Max\ (Lc,Pu,Ac,Ds,Dn,Vs,Es,Ms)} \qquad (5)$$

The value **V** represents, in addition to the probability of success of a terrorist attack, the CI vulnerability in percentage.

Associated with a certain range of probability of success of an attack, or percentage of vulnerability, is a certain level of vulnerability, which is determined by applying the following table.

Table 1 – Determination of Vulnerability level

Vulnerability Level	Probability				
	<= 0,3	0,31 - 0,50	0,51 - 0,74	0,75 - 0,89	0,90 - 1
Very High					X
High				X	
Medium			X		
Low		X			
Very Low	X				

Source: Adapted from (US DoD, 2008, p. 3-34)

As any analysis and decision-making process the human factor is paramount for the application of any algorithmic model, especially when subjective judgments arise in this process and depend on the analyst's and the decision maker's intellectual and emotional skills.

The integration of the MACBETH (Measuring Attractiveness by a Categorical Based EvaluationTechnique) - a multicriteria model to support decision – allows the analyst, based on the perceptions and preferences of the decision-maker, to define his own criteria weights in order to approach his qualitative observation of the problem to a quantitative solution, without doubt, an added value for this process.

The vulnerability analysis is one of the initial steps in the process of protection of CI, so the results of this research contribute to increase conceptual knowledge and constitute a tool to support the decision-making.

BIBLIOGRAPHY

Bana e Costa, C., Angulo-Meza, L., Oliveira, M., 2013. *O método MACBETH e aplicação no Brasil*. Engevista, 15(1), April, pp.3–27.

FEMA, 2005. *FEMA 452 - Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings. Risk Management Series*. USA: FEMA.

FEMA, 2012. *FEMA 428 Primer to Design Safe School Projects in Case of Terrorist Attacks and School Shootings. Buildings and Infrastructure Protection Series*. USA: FEMA.

Morgeson, J. et al, 2011. *Doctrinal Guidelines for Quantitative Vulnerability Assessments of Infrastructure – Related Risks*. Vol.1. Virginia: Institute for Defense Analyses.

Renfroe, N.A. e Smith, J.L., 2016. *Threat / Vulnerability Assessments and Risk Analysis*. [online] WBDG Whole Building Design Guide. Available at: https://www.wbdg.org/resources/threat-vulnerability-assessments-and-risk-analysis?r=riskmanage [accessed at 9 Dec. 2016].

US DoD, 2004. *DoD Antiterrorism Handbook*. USA: DoD

US DoD, 2008. *UFC 4-020-01 DoD Security Engineering Facilities Planning Manual*. USA: DoD.