VULNERABILITY ANALYSIS IN CRITICAL INFRASTRUCTURES: A METHODOLOGY

António FERREIRA, MSc
Major (OF-3)
ferreira.acs@ium.pt
Member of Research & Development Centre of Portuguese Military University
Portuguese Military University Institute

Abstract

Vulnerability assessment is a crucial aspect for the development of methodologies to define the levels of protection in critical infrastructures.

Throughout this research, we discussed the concept of vulnerability and methodologies and processes for its assessment in critical infrastructures due to a terrorist threat. The research focused on the development of an analysis model, exploring a multi-criteria decision method, in order to limit the risks to the maximum extent possible.

Through a qualitative research methodology, in which we applied an analysis model based on the Threat and Infrastructure dimensions and their respective factors, we verified that the vulnerability of a critical infrastructure consists in the probability of the success of an attack, conducted by a threat - properly identified, characterised, analysed and categorised - against an infrastructure with certain characteristics, which value is defined by the user and aggressor's point of view.

The construction of an algorithmic model for vulnerability assessment, complemented by tools to support the calculations and records, allows, through a rational, scientific and algebraic process, a qualitative analysis of factors to be transformed into measurable and quantifiable values, whose algebraic operation integrates them into a final result that expresses, as a percentage, the degree of vulnerability of a critical infrastructure facing a terrorist threat.

Keywords: Vulnerability, critical infrastructure, terrorist threat, assessment model, Macbeth

Introduction

The operation of critical infrastructures (CI) can be affected in several ways, either natural (e.g. flooding) or anthropogenic (e.g. accident, robbery, terrorist attack). Their effects can vary from simple disturbance to total destruction, either from an infrastructure or, by domino effect, with implications in several other vital sectors (Security and Forensic Sciences, 2016).

The threat of terrorist attacks with the use of explosive devices deserves special attention because it assumes several possible ways, and although in the future another kind of threat could turn out to be dominant, historically, it has been one of the most commonly used tactics by terrorists.

The protection of CI is a subject that gained enormous preponderance from the terrorist attacks of September 11, 2011 in the United States of America (USA), and that forced a rethink about its position on the physical component of CI protection (Natario 2014cited in Ferreira 2016, p. 1), including the risk management analysis that this type of infrastructure is subject to.

Vulnerability analysis is a key aspect for the development of methodologies that allow the definition of levels of protection in CI. It is essential to understand the concept of vulnerability and develop methodologies and processes for its evaluation in CI in the face of a terrorist threat, with a particular focus on the development of a model of analysis, exploring a method of support for multicriteria decision making, in order to be able to limit the maximum extent possible.

In spite of this more focused contribution to internal security issues, and in a dual-use perspective, there is also a need to look at CI in theatres of operations where military forces are deployed and whose protection is essential for the fulfilment of the mission and for their own force protection. Thus, the purpose of this research is to provide a planning tool that allows a commander or person responsible for a CI to determine their susceptibility to an attack caused by an aggressor and the identification of physical characteristics or procedures that make a particular infrastructure (e.g. military barracks), area, system or event, particularly vulnerable to a spectrum of plausible possibilities of threat.

This research is part of the field of Military Sciences in the research area of Technical and Military Technologies.

The research, according to the general theme and according to the established delimitation, has the purpose of discussing the concept of vulnerability and the methodologies and processes for its evaluation in critical infrastructures (in national territory or expeditionary) in the face of a terrorist threat, with a particular focus on the development of an analysis methodology, exploring a multicriteria decision support model, in order to be able to limit the risks to the maximum extent possible.

To guide the research and reach the purpose presented, it was defined as a general objective for the present study "to develop a methodology for analysing the vulnerability of critical infrastructures."

In order to achieve this general objective, three specific objectives (SO) have been defined:

SO 1 - Classify the threats that may affect the vulnerability of an IC;

SO 2 - Evaluate the characteristics of a CI that may affect its vulnerability;

SO 3 - Develop an algorithmic method of analysis of the vulnerability of a CI, integrating a methodology to support multicriteria decision.

The methodology followed in the elaboration of this research is based on deductive reasoning (Santos et. al 2016, p.17), based on the existing knowledge base on the concepts and the dimensions under analysis, which resulted, through qualitative research, in the development of an application model for decision support.

Conceptual Framework

In Portuguese legislation, CI is a "component, system or part of the system located in national territory which is essential for the maintenance of vital functions of the society, health, safety and economic or social well-being and whose disruption or destruction would have a significant impact, given the impossibility to continue performing these functions" (Law n.º 62/MDN/2011, May 9). In a military view,

CI is "the one whose disruption is liable to cause disruption to the operation of basic needs services, generate insecurity or cause the loss of trust in the institutions, affecting the normal functioning of society and the rule of law" (CCEM 2014).

Regarding the concept of protection, from the numerous definitions found in the bibliography, the following are considered as the basis for the present investigation. Protection is defined as "all activities designed to ensure the functionality, continuity and integrity of a critical infrastructure in order to deter, mitigate and neutralise a threat, risk or vulnerability" (Directive n.º 2008/114/EC, December 8). The US National Infrastructure Protection Plan (NIPP) defines protection as "the actions necessary to deter a threat, mitigate vulnerabilities or minimise the consequences associated with a terrorist attack or a natural or technological disaster" (US DHS 2009).

The implementation of this concept is based on the identification of protective measures based on the threat assessment, identification of vulnerabilities and risk management. As part of the planning and implementation process of CI protection measures, vulnerability assessment will contribute directly to the risk assessment and, consequently, to deciding which protective measures should be implemented. Thus, associated with protection is undoubtedly the vulnerability, which, through the implementation of protection measures, will be mitigated in order to minimise the consequences of any threat.

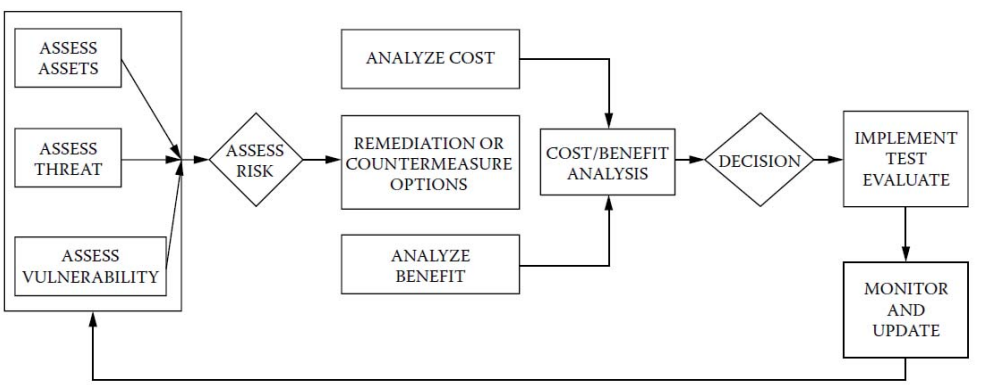

Fig. 1. Risk management approach (Krauthammer 2008, p. 10)

But what is vulnerability?

Vulnerability is the "combination of the attractiveness of a facility as a target and the level of deterrence and/or defence provided by the existing countermeasures" (Renfroe Smith 2016).

Almeida, citing Apostolakis and Lemon (2003:362), defines vulnerability as the "manifestation of inherent states of the system (whether physical, technical, organisational, or cultural) that can be exploited by adversity to damage or cause damage to the system" (Almeida 2011, p.15).

From the previous definitions, there are two interpretations regarding the concept of vulnerability. At first, the vulnerability is the probability of the success of an attack, resulting in a certain threat for an infrastructure with certain characteristics. In the second, vulnerability emerges as an infrastructure characteristic (physical, procedural, etc.) that can be exploited by the threat, that is, represents a fragility. Although they are two distinct concepts, they complement each other. However, this article will focus essentially on the first concept, defined by Renfroe and Smith.

Therefore, vulnerability analysis is the process that a commander or somebody responsible for CI employs to determine the susceptibility of an infrastructure to attack by an aggressor, or the probability of the success of an attack. It responds to the question, "to what kind of attack is the infrastructure more or less vulnerable?"

The ultimate goal of the process is to identify the physical characteristics or procedures that make a particular infrastructure, area, system or event, particularly vulnerable to a range of plausible possibilities of a threat. There are two dimensions that underlie any vulnerability assessment process of a CI: the infrastructure itself and the threat.

Threat Assessment

The threat level is an integral part of any vulnerability analysis process and, therefore, risk analysis and is used to determine, characterise and quantify damage caused by a terrorist (or terrorist group) according to their tactics and types of explosive devices.

To assess the threat, it is necessary to (i) identify and distinguish its typology, the tactics and techniques and the type of armaments associated with it; (ii) analyse the threat according to internal and external factors; and (iii) to classify the threat according to the analysis made of its factors.

Characterising the threat has as its starting point an identification of the type of terrorist, which can be: (i) at domestic, local or regional level – e.g. overthrow of apostate governments (takfir); (ii) international, involving citizens in two or more States and (iii) transnational, when at least one of the actors is a non-state actor with global capacity (Pereira 2016, pp.56–57). The type of terrorism may indicate a set of features related to the tactics and techniques used and the type of explosive device to use, thus contributing to making a more or less vulnerable infrastructure.

Identify and distinguish its typology, the tactics and techniques and the type of armaments associated with it

The tactics and techniques used by terrorists, as well as the type of explosive devices, are another influencer of the vulnerability of a CI.

These depend on the form of employment, the duration and extent of the effects and site conditions, the association between the size of explosion and the load-distance is determinant to ascertain the severity of the effects and the corresponding, higher or lower, probability of success of the terrorist attack.

The tactics and techniques used by a terrorist or terrorist group to attack a CI may consist of manually-launched explosive devices, the use of moving vehicle-bombs against infrastructure, or the use of vehicle-bombs stationed near the infrastructure (US DoD 2008, p. 2-4). The choice of a particular tactic results from two factors: the aggressor's own characteristics and abilities, and the typology and characteristics of the CI.

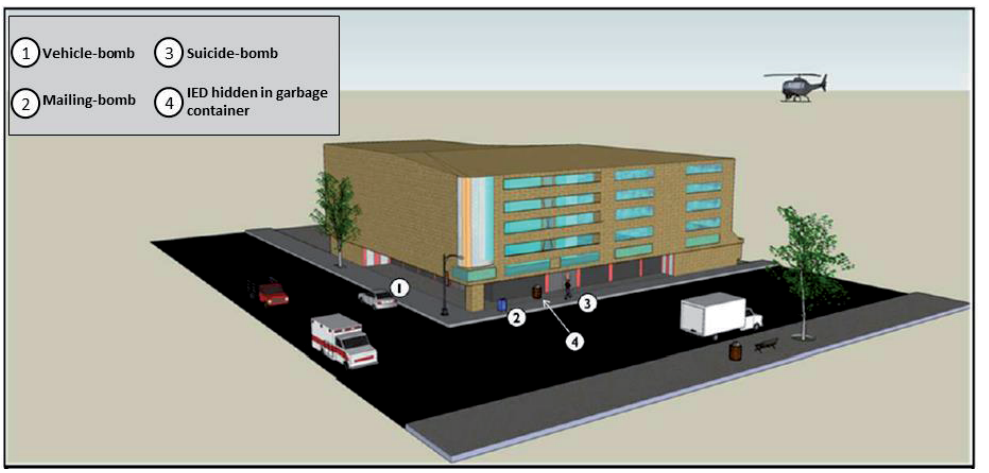

Fig. 2. Examples of attacks with explosive devices (Conceição 2008, p. 34)

The type of explosive device used is directly related to the tactic and technique used, affecting the vulnerability degree due to the greater or lesser probability of causing damage, that is, the larger the amount of explosive, the greater the probability of causing damage.

Explosive devices are classified as: (i) Improvised Explosive Devices (IEDs); (ii) Hand grenades; and (iii) Bomb vehicles (US DoD 2008, pp. 2-9 a 2-10), and they can be distinguished by the type of container or transport, their quantity, evacuation distance for the occupants of a certain conventional building (without structural reinforcement) and safe distance for unprotected people in the vicinity of the explosion.

Threat		Explosives Mass [kg]	Building Evacuation Distance [m]	Outdoor Evacuation Distance [m]
Pipe Bomb		2,3	21	256
Suicide Belt		4,5	27	330
Suicide Vest		9	34	415
Suitcase Bomb		23	46	564
Compact sedan with explosives		227	98	457
Sedan with explosives		454	122	534
Passenger/Cargo Van with explosives		1814	195	838
Small moving van or delivery truck with explosives		4536	263	1143
Moving Van or Liquid Truck with explosives		13608	375	1982
Semi-trailer with explosives		27216	475	2134

Table 1. Type of explosive devices (adapted from FEMA 2006, p. 1-7)

Analyse the threat according to internal and external factors

After the identification and characterisation of the threat, it is necessary to categorise it according to the analysis of factors associated with the level of terrorist activity.

This factor analysis is based on compiling and processing the collected information in order to develop indicators that identify and measure possible terrorist activity.

We identified four factors, and their respective indicators, for threat assessment: Threat Operational capability (Oc) to conduct a terrorist attack, the Intention (In) to execute the attack, the Activities (At) developed around an attack, namely planning and logistical support activities and the Operational Environment (Oe) that involves the planning, preparation and execution of the attack (US DoD 2004, pp. 66-69).

Classify the threat according to the analysis made of its factors

Once the main threats have been identified, featured and analysed, it is necessary to determine the likelihood of these taking place, allowing threats to be classified at different levels. The threat level is an integral part of any vulnerability analysis process and, therefore, risk analysis and is used to determine, characterise and quantify damage caused by a terrorist (or terrorist group) according to their tactics and type of explosive devices.

There are several types of possible scales to be used, varying the number of levels and the description of the indicators associated with them. The scale adopted by us to classify the threat level is a combination of a linguistic scale of five states and a numerical scale with 20 levels. This classification is made, qualitatively or quantitatively, in terms of the probability and credibility of the threat, taking into account the factor analysis presented in the previous section, and the effects of tactics, techniques and the type of explosive devices.

Threat Level		
Qualitive Scale	**Numeric Scale**	**Description**
Very High	17- 20	The occurrence of an attack is imminent. Terrorist cells are operationally active. Security forces, military forces and intelligence services confirm the threat. The operational environment favors the terrorist.
High	13 - 16	The occurrence of an attack is likely. Security forces, military forces and intelligence services confirm the credibility of the threat. The operational environment favors the terrorist.
Moderate	8 - 12	The occurrence of an attack is possible. The security forces, military forces and intelligence services confirm the existence of a threat, but their credibility has not been verified. The operational environment is neutral.
Low	4 - 7	The occurrence of an attack is unlikely. Security forces, military forces and intelligence services confirm the existence of a threat, but not the likelihood that it will materialize. The operational environment favors the country or host nation.
Very Low	2 - 3	The probability of an attack is negligible. According to the security forces and information services the threat does not exist or is virtually non-existent. The operational environment favors the country or host nation.

Table 2. Threat Level (adapted from FEMA 2005, pp. 1-25 and US DoD 2004, p. 70)

Infrastructure Assessment

After assessing the threat, it is necessary to carry out the infrastructure assessment. An infrastructure is an asset and it is therefore necessary to determine how it represents a target for a terrorist attack.

Determining the value of an infrastructure as a target makes it possible to determine the liability of this being attacked, due to both tangible and intangible factors, influencing the level of protection to be adopted (Renfroe and Smith 2016, p. 2).

The process for the infrastructure assessment should include the following steps (FEMA 2005, pp. 2-1):

(i) Identification and characterisation of the infrastructure security perimeters;
(ii) Identification of the critical assets and core functions of the infrastructure;
(iii) Applying the analysis factors to determine the value of an infrastructure.

Identification and characterisation of the infrastructure security perimeters

Looking at the infrastructure from the security point of view, it is important to analyse it on three levels, according to the three security layers, identifying and distinguishing all the characteristics that affect the security of the infrastructure, minimising or exposing the effects of a terrorist attack. These characteristics constitute an obstacle to the terrorist action.

Contributing to it, among other things, are the type of construction, occupation density and the nature and intensity of activities in the surrounding area (first security line - faraway zone), infrastructure accesses (people and vehicles), parking areas, outdoor lighting and surveillance in the second security line (intermediate zone) and structural and non-structural systems, as well as other features inherent in the infrastructure construction (third security line - next zone).

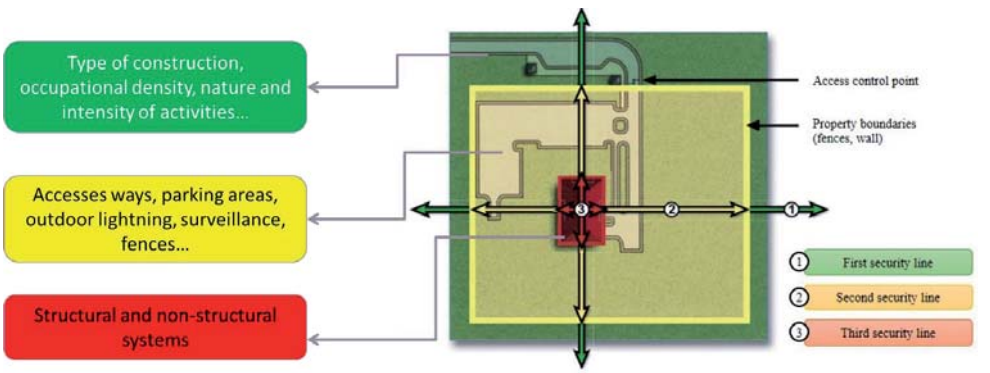

Fig. 3. Security Layers (adapted from FEMA 2005, pp. 2-3)

Identification of the critical assets and core functions of the infrastructure

Taking into account the potential effects of a terrorist attack, it is essential to determine the set of functions, with direct connection to the construction, operation and maintenance of an infrastructure necessary for its operation after the attack. Core functions are directly associated with the CI typology, namely with the main existing services, the most critical activities, the occupants and users and the degree of dependence on external factors (FEMA 2005, p. 2-17).

The main assets are derived from the core infrastructure functions. The infrastructure assets consist of all its essential components in its operation, given the core functions of the same (Morgeson, J. *et al* 2011, pp. 9-10). The identification of the major assets allows the major elements of an infrastructure whose protection is essential for its operation after a terrorist attack to be determined.

In the face of a threat, it is easier and less expensive to adopt measures to protect the major assets of an infrastructure than to protect the infrastructure as a whole. However, the infrastructure itself can be considered as an asset whose value requires the adoption of protective measures as a whole.

Apply the analysis factors to determine the value of an infrastructure

An Infrastructure assessment must be made from two points of view: (i) the value that the infrastructure or its assets have for the user and for the country; (ii) and the value as a target for the attacker.

This was done by combining two methods used for decision-making support applied to vulnerability analysis: the MSHARPP method and the CARVER method, both developed by the U.S Department of Defense.

The MSHARPP method, primarily developed as a support tool to mitigate terrorist attacks, presents a set of factors that determine the infrastructure value for the user, from an internal perspective, based on the concept of inside to outside protection (Schnaubelt *et al*. 2014, p. 107).

The CARVER method, developed as a tool to evaluate and determine the value of a target in a military attack, allows us to identify the factors that should be considered to assess the CI from the point of view of the terrorist, that is, from an external perspective, based on the concept of outside to inside protection (Schnaubelt *et al*. 2014, p. 107).

The combination of these methods allows the factors to be used to analyse the CI and determine its value to be identified and, consequently, to identify the physical and procedural vulnerabilities.

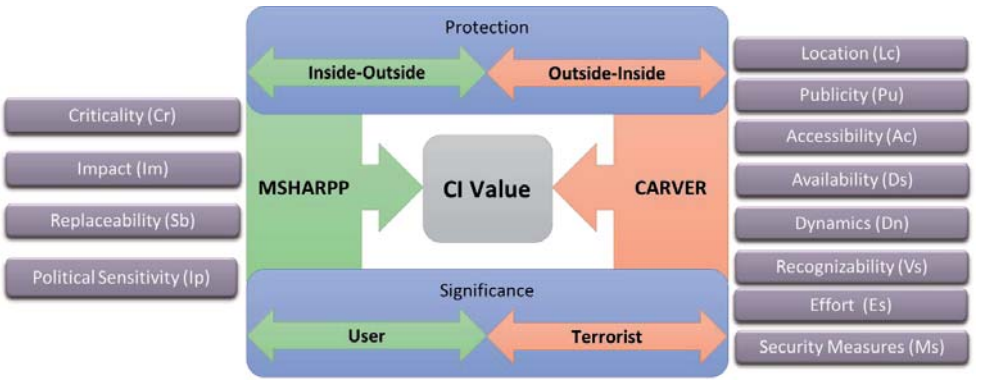

Fig. 4. Combination of MSHARPP and CARVER method to define Infrastructure analysis factors

The value of the infrastructure for the user represents the consequence that it will have if the assets are compromised by the terrorist. The greater is its value, the more important it is to the user, greater is the need to implement protective measures to reduce vulnerability. To determine the value of the infrastructure, for the user, we identified four analysis factors: (i) What is critical (Cr) for the mission; (ii) The Impact (Im) that the CI has on the system operation and the influence it has on other systems; (iii) Replaceability (Rp), the ease with which the asset can be replaced or the infrastructure resumes activity; (iv) Public and political repercussions – Political Sensitivity (Ps) - associated with the loss or destruction of the infrastructure or assets and the consequent impact on their activity (US DoD 2004, pp. 66-69).

The CI must also be analysed from the point of view of how it constitutes a high-paid target for the achievement of the aggressor's goals. The higher the CI value, the more rewarding it is as a target, the greater is the exposure to an attack and the greater is the likelihood of success.

To determine the value of an asset and, consequently, of the infrastructure, for the aggressor, we identified eight analysis factors (US DoD 2008, pp. 3-31): (i) the infrastructure Location (Lc); (ii) the Publicity (Pu) level related with the infrastructure; (iii) the Accessibility (Ac) to the infrastructure; (iv) the Availability (Av), with regard to the existing amount of the same type of infrastructure; (v) Dynamics (Dn), associated with the mobility of the assets; (vi) Recognisability (Rc), represented by the probability of an attacker identifying the CI and its location; (vii) Effort (Ef) that an attacker has to employ to carry out the attack, including the level of resources; and (viii) the existing Security Measures (Sm) to prevent or avoid the access to the CI.

Vulnerability Analysis Model

The vulnerability degree of a CI consists in a qualitative or quantitative expression of the level at which a particular infrastructure is liable to be damaged in the face of a given hazard (Morgeson *et al.* 2011, p. 24), being, as demonstrated in previous chapters, a function dependent on threat and infrastructure.

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 qualitative judgments into quantitative values that can be used mathematically to calculate, as a percentage, the probability of the success of a terrorist attack using explosive devices against a CI.

This analysis is based on the general mathematical expression (1) later broken down into subsidiary mathematical expressions:

$$\begin{gathered} Vulnerability = Probability\ (Success|Attack) \\ V = P(S|A) \end{gathered} \tag{1}$$

To analyse the vulnerability of CI and give body to the expression (1), an algorithmic model illustrated in Figure 4, resulting from a partial adaptation of theoretical models presented by US DoD and FEMA.

This model consists of six steps, based on the analysis of the Threat and infrastructure.

The proposed analysis model is composed, in addition to the algorithm, by a set of worksheets used to calculate and register the values and which will sustain the final results.

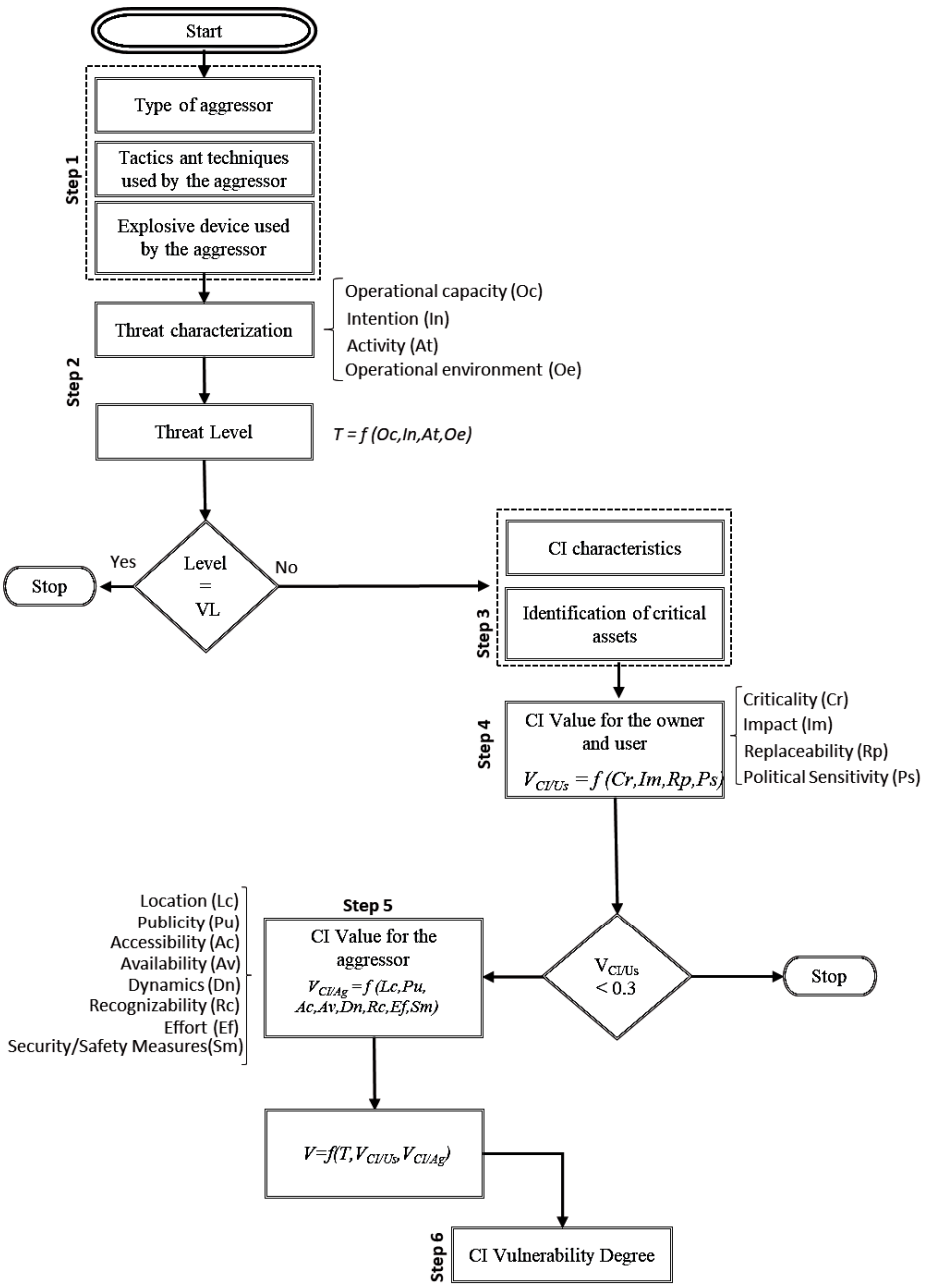

Fig. 5. Algorithm for Vulnerability Analysis

The algorithmic process must be sequential, both in terms of dimensions and variables and in terms of tasks. That is, working first on the threat dimension and then on infrastructure (since the study takes into account the effects that the threat produces) and we should do the identification, characterisation, analysis and classification or categorisation.

The process must be interactive, in order to allow the analyst to adapt the factors analysis to the perceptions and preferences of the decision maker.

The process must be analytical, based on pre-defined analysis factors and on common standards.

The process should be algebraic, in order to quantify the analysis numerically and to support the decision to be taken on the measures to reduce the vulnerability of a CI on a realistic and objective, non-subjective basis.

Since the vulnerability is a value depending on the probability of the success of an attack, the calculation of its value is directly related to the threat level, to the CI value for the user and to the IC value for the aggressor.

Mathematically:

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

Wherein:

The threat level is a function of these four factors: operational capability, intent, activity, operational environment.

$$\text{Threat} = \text{function (Operational Capability, Intent, Activity, Operational Environment)}$$
$$A = f\,(Oc,In,At,Oe) \quad (3)$$

To determine the level of threat, we should add the values assigned to each of the four factors.

$$A = \sum (Oc,In,At,Oe) \quad (4)$$

The CI Value for the user is a function of these four factors: criticality, impact, replaceability, political sensitivity.

CI Value for the user = function (criticality, impact, replaceability, political sensitivity)

$$V_{CI/Us} = f\,(Cr,Im,Rp,Ps) \tag{5}$$

or

$$V_{CI/Us} = \frac{\sum(Cr,Im,Rp,Ps)}{\sum Max(Cr,Im,Rp,Ps)} \tag{6}$$

The CI Value for the aggressor is a function of these eight factors: location, publicity, accessibility, availability, dynamics, recognisability, effort, and security measure.

CI Value for the aggressor = function (location, publicity, accessibility, availability, dynamics, recognisability, effort, and security measure)

$$V_{CI/Ag} = f\,(Lc,Pu,Ac,Av,Dn,Rc,Ef,Sm) \tag{7}$$

or

$$V_{CI/Ag} = \frac{\sum(Lc,Pu,Ac,Av,Dn,Rc,Ef,Sm)}{\sum Max\,(Lc,Pu,Ac,Av,Dn,Rc,Ef,Sm)} \tag{8}$$

In summary, the calculation of the probability of the success of an attack consists of the sum of the 16 factors regarding the characteristics of the threat and infrastructure and divided by the sum of their maximum values:

$$V = \frac{\sum(Oc,In,At,Oe,Cr,Im,Rp,Ps,Lc,Pu,Ac,Av,Dn,Rc,Ef,Sm)}{\sum Max\,(Oc,In,At,Oe,Cr,Im,Rp,Ps,Lc,Pu,Ac,Av,Dn,Rc,Ef,Sm)} \tag{9}$$

The value obtained through this formula represents, in addition to the probability of the success of a terrorist attack, the percentage of vulnerability of a CI.

Associated with a certain range of probability of the success of an attack, or percentage of vulnerability, is a certain degree of vulnerability, which is determined applying Table 3.

Vulnerability Degree	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				

Table 3. Vulnerability Degree Chart (adapted from US DoD 2008, pp. 3-34)

Integration of MACBETH method

Like any assessment process and, consequently, decision-making process, the human factor is preponderant 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 application of a multicriteria decision support model, which allows the decision maker to manipulate the weights of the criteria used in the vulnerability assessment, in order to bring his qualitative observation of the problem closer to a quantitative solution, is undoubtedly of more- value for this process.

The method MACBETH (Measuring Attractiveness by a Categorical Based Evaluation Technique) developed by Carlos Bana e Costa, Jean-Marie De Corte and Jean-Claude Vansnick, is a decision-making support method that allows options using multiple criteria to be evaluated.

It is distinguished from other multicriteria methods by basing the weighting of the criteria and the evaluation of the options in qualitative judgments about differences in attractiveness (Bana e Costa e Oliveira 2013).

The integration of the Macbeth method into the CI vulnerability analysis model is based, essentially, on the structuring of the criteria and the evaluation of the weights, allowing, in an interactive way, the weights of the criteria and indicators to be handled, transforming qualitative judgments into quantitative information based on the concept of attractiveness between two options.

In a process of vulnerability analysis of a CI (particularly in the proposed), the decision maker may not have a complete understanding of the problem and / or

a perception of the importance that should be given to the various criteria. Being knowledgeable about the process, the analyst must support the decision maker throughout the process so that the decision maker builds a solution that is closer to the appropriate solution of the problem.

In the model we have developed, the values of the weights given to the criteria are proposed and predefined and with which the decision-maker may not feel comfortable because of their interpretation of the problem or the lack of clarity concerning the weight of the value given to the criteria.

Using the Macbeth method, facilitated by its own software, the analyst can structure the vulnerability analysis model according to the perceptions and preferences of the decision maker, transforming the qualitative judgments of the decision maker in quantitative values, adjusting the weights of the various criteria to the solution sought by the decision maker.

This process of transforming a qualitative judgment into quantitative information is based on the concept of attractiveness between two options.

The Macbeth methodology also allows sensitivity analyses to be carried out (verify if other weights or preferences of the decision maker affect the final order of the analysis's criteria) and the robustness of the obtained results.

In the end, the results obtained from Macbeth, including the value functions (quantitative descriptive) and the weights of the criteria are introduced in the vulnerability analysis model.

Conclusions

The present investigation aimed at discussing the concept of vulnerability and the methodologies and processes for its evaluation in critical infrastructures (in national territory or expeditionary) facing a terrorist threat, with particular focus on the development of an analysis methodology, exploring a model of multicriteria decision support in order to be able to limit risks to the maximum extent possible. For this purpose, it was defined as a research general objective to develop a methodology for analysing the vulnerability of critical infrastructures.

The main lines of the methodological research procedure were based on a literature review of European and national legislation on CI protection, NATO and USA doctrine of NATO, and, with great focus, technical manuals of North American institutions alluding to the subject under study. The results were obtained through the analysis model that was developed, based on the concept of vulnerability and its Threat and Infrastructure dimensions, which were categorised based on the characterisation and analysis of their variables.

Also, as part of the analysis model, the theoretical concept of vulnerability was transformed into an algebraic expression, based on the factors and indicators associated with the dimensions and variables, which materialises the degree of vulnerability of a CI through a real and positive value.

Based on the Threat and Infrastructure dimensions and their respective factors, the CI vulnerability consists of the likelihood of an attack being successful by a threat - properly identified, characterised, analysed and categorised - against an infrastructure, with certain characteristics, which define its value to the user and to the aggressor.

To that end, we identified a set of analysis factors that support the characterisation and evaluation of the Threat and Infrastructure dimensions: operational capacity, intention, activity, operational environment, criticality, impact, replaceability, political sensitivity, location, publicity, accessibility, availability, dynamics, recognisability, effort and security measures.

The development of an algorithmic model of vulnerability analysis, complemented by calculation and registry tools, allows, through a rational, scientific and algebraic process, a qualitative analysis of factors to be transformed into measurable and quantifiable values whose algebraic operation integrates them in a final result that expresses, as a percentage value, the degree of vulnerability of a critical infrastructure to a terrorist threat.

The integration of the Macbeth method in the vulnerability analysis model allows the analyst, based on the perceptions and preferences of the decision maker, to fabricate their own criteria weights, and then re-integrate them into the developed model.

References

Almeida, A., 2011. *Multicriteria methodology for identification and prioritization of Critical Infrastructures*. Thesis for Master Degree in Industrial Engineering and Management, Instituto Superior Técnico.

Bana e Costa, C., Angulo-Meza, L. and Oliveira, M., 2013. *MACBETH method and its aplication in Brazil*. Engevista, 15(1), 3–27.

Conceição, L., 2008. *Building Security and Protection against terrorists attacks*. Thesis for Master Degree in Military Engineering, Instituto Superior Técnico.

CCEM, 2014. *Military Strategic Concept.* National Defense Ministery, Lisbon.

European Council, 2008. Identificação e designação das infra-estruturas críticas europeias e à avaliação da necessidade de melhorar a sua protecção (Diretiva 2008/114/CE de 8 de dezembro de 2008), Jornal Oficial da União Europeia, Brussels.

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

FEMA, 2006. *FEMA 453 – Design Guidance for Shelters and Safe Rooms. Risk Management Series*. Federal Emergency Management Agency.

Ferreira, H., 2016. *Critical Infrastructure Identification and Characterization - a Methodology*. Military University Institute.

Krauthammer, T., 2008. *Modern Protective Structures*. CRC Press, Florida.

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

Santos, L.A. *et al*., 2016. *Methodological Guidelines for research*. IESM, Lisbon.

Schnaubelt, C. *et al*. 2008. *Vulnerability Assessment Method. Pocket Guide. A tool for center of gravity analysis*. Rand Corporation, Washington D.C.

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

Security and Forensic Sciences, 2012. Critical Infrastructures Protection. [online]. *Security and Forensic Sciences*. Available from: https://segurancaecienciasforenses.com/ 2012/03/04/proteccao-de-infra-estruturas-criticas-2/ [Accessed 9 Dec 2016].

US DHS, 2009. *National Infrastructure Protection Plan*. Department of Homeland Security.

US DoD, 2004. *DoD Antiterrorism Handbook*. Department of Defence.

US DoD, 2008. *UFC 4-020-01 DoD Security Engineering Facilities Planning Manual*. Department of Defence.