CRITICAL AVIATION INFRASTRUCTURES VULNERABILITY ASSESSMENT TO TERRORIST THREATS

Cătălin CIOACĂ

"Henri Coandă" Air Force Academy, Braşov, Romania

Abstract: *The main purpose of risk assessment methods is to identify the breaches of the system, to estimate the likelihood of a threat and to propose solutions for risk mitigation. One of the critical components of the risk assessment process is to determine the vulnerability of critical infrastructure/system based on possible risk scenarios. The solutions presented by the vulnerability assessment are divided into two categories: a quantitative model built on the basis of the theory of multi-parameter values and adapted to complex systems by using morphological analysis and a model based on probability theory of assumptions.*

Keywords: *vulnerability assessment, terrorism, aviation infrastructure*

1. INTRODUCTION

The airport, as a main infrastructure of aviation system, is a favorite target of terrorist attacks first because of the human losses and material damage, but also because of the powerful psychological impact in case of a success. Any disturbance to the stability of the whole air transport systems will have a leverage effect: decrease the safety of passengers and reduce the demand of air transport services, losses in the aviation industry and ultimately disturbing economic stability (Patriot Act, 2001).

Predictive models for assessing the risk of terrorism are particularly useful, but they have limitations in case of events of unknown typology or events which happen once. A possible solution could be to identify a causal link between the initial events (movement of people considered suspicious, transfers of money in their accounts, trying to purchase some dangerous substances, etc.), frequent and observable enough in terms of consequences, and extreme event (terrorist attack), so that the results can be extrapolated (JASON, 2009).

Frequency-magnitude distribution model, originally developed for natural disasters (Newman, 2005), has been adopted and for terrorist events (Clauset et al., 2008).

The morphological model (Ritchey, 1997; Zwicky, 1969) is another descriptive analysis model of the complex situations by dividing the problem into the parameters/ variables/ components and identification all of those relationships. The use of repetitive cycles of analysis and synthesis, as well as building an internal structure as matrix type, is the main advantage of this method.

The U.S. Department of Homeland Security used for terrorist risk assessment a model built on events tree architecture, in terms of annual frequency of occurrence, the probability of successful attack and failure of countermeasures, and consequences (Cheesebrough and Wise; 2012).

Quantitative assessment approach of the level of vulnerability, identifying physical characteristics and operational attributes that expose critical aviation infrastructure to terrorist threat (DHS, 2008), become essential in achieving security and safety.

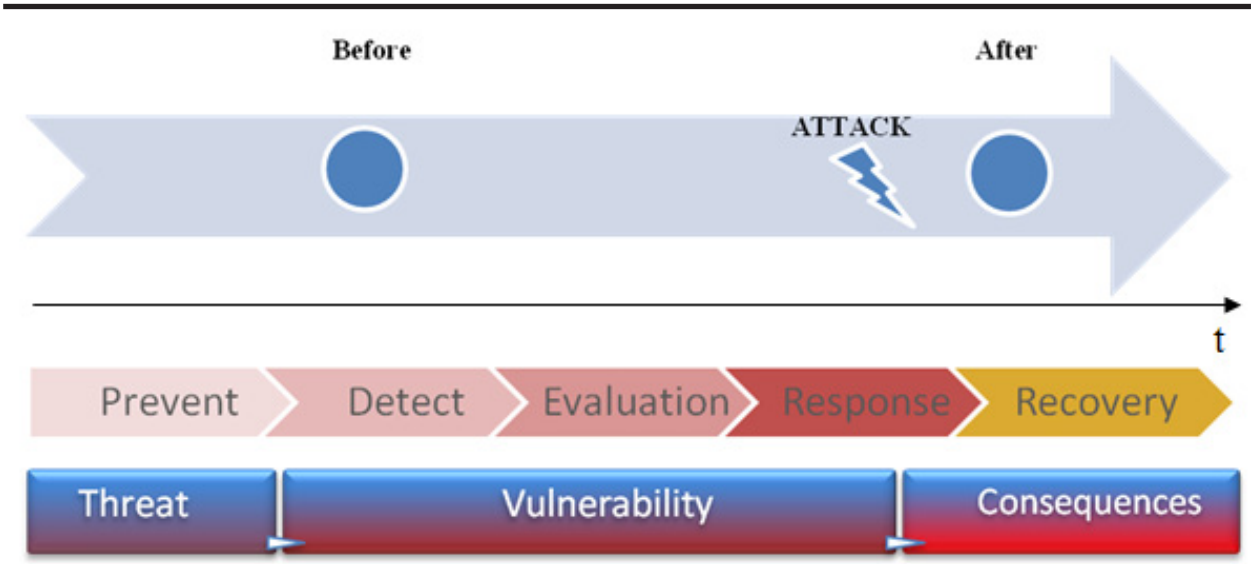

Fig. 1. The architecture of terrorism risk evaluation

In order to release the risk analysis by external pressures in setting the levels of threat, especially to assess vulnerability and consequences of possible attacks, we use a quantitative approach. Application of quantitative techniques to evaluate the risk of terrorism can bring the following advantages: reduction of attack risk for some targets, by converting them into less attractive targets for terrorists; increasing resilience of system; reduction of recovery time after the attack; preventing the spread of cascading effects.

The process of terrorism risk assessment can be thought in the context of a general framework, in which the level of vulnerability determines the effectiveness of the system (Fig. 1).

Stages of evaluation of the threat, vulnerabilities and consequences are particularly important in risk quantification approach because it requires, on the one hand, the availability of specialists in intelligence structures and to interact and provide timely information needed for further tests, and on the other hand, the definition of normality. We can talk about such a process of risk management in order to increase the level of understanding of the issue of risk. Better understanding of the threat, vulnerability and consequences of an attack by using quantitative and qualitative assessments allow decision factors to initiate mechanisms of prevention and detection before becoming a reality the potential consequences (Morar and Stefan, 2012).

2. DEFINING A SYSTEM IN TERMS OF VULNERABILITY

The main parts of the paper will be introduced by numbered titles with Arabic figures and printed in capitals, font 12pt, bold, centered. A free space will be left above the text and another one below it. Paragraphs will be 6mm indented.

The security risk is viewed as a function of the nature of the threat (T), vulnerabilities to attack of a system (V) and the consequences (C) associated with a possible attack scenario (Willis et al., 2005).

In risk analysis, vulnerability is assessed in probability known or perceived of a breakthroughs existence or a malfunction in the system/infrastructure review for a certain period of time in the context of a threat scenario type.

Vulnerability = Probability (successful attack)

Vulnerability assessment refers to the ability of the system to detect the initial event (IE), to delay it in order to prepare the answer and to act in such a way as to interrupt the spread of the system

To assess the vulnerability of aviation critical infrastructures, the following construct which defines the five functions of survival of a system is considered: detection, evaluation, response, recovery, prevention (DERRP).

Detection is the likelihood of establishing that an IE has been or will be held on the basis of the warnings. Evaluation is given by the probability of the occurrence of false alarms. The response is defined by the reaction time of the system necessary to limit or eliminate the effects of propagation. Recovery is the time to return the system to the normality. Prevention is expressed through the totality of measures taken to reduce the vulnerabilities of the system, perceived by adversary as being very difficult to pass.

Since the vulnerability is the likelihood of success of an event, once it has been initiated (V = psuccess/IE), then it can be calculated as:

$$V = 1 - \left[\begin{matrix} p(det|E) \times p(eval|E) \times p(resp|E) \times p(rec|E) \times \\ p(prev|E) \end{matrix} \right] \quad (1)$$

An event is initially combated if all stages are completed, or it becomes a failure if any of the phases fail.

3. DETERMINATION OF VULNERABILITY BASED ON PROBABILITA ASSUMPTIONS

3.1 The probability of future events. The assumptions theorem does not provide the possibility of determining the probability of events occurrence, but their distribution. Thus, in terms of the air transport system, whether within a time interval Δt occurred N events (attacks), K times that being controlled (when one or more combination of several survival functions), the question arises of determining the probability of k times controlled the next n events.

The number of possible variants to occur is C^k_n, and the probability of k times from n possible event is $p^k q^{n-k}$.

The connection between the known data (N, K) and those meant to be calculated (the probability of any variants) is attested in equation (2).

$$p^k \cdot q^{n-k} = \frac{p^{K+k} \cdot q^{N+n-(K+k)}}{p^K \cdot q^{N-K}} \quad (2)$$

The occurrence probability p is calculated by integrating the distribution densities ($p^{K+k} \cdot q^{N+n-(K+k)}$, $p^K \cdot q^{N-K}$) of the probability for a single variant in range of values from 0 to 1. The most likely value of the probability of an occurrence variant of k times of event n is given in equation (3).

$$p = \frac{\int_0^1 p^{K+k} \cdot q^{N+n-(K+k)} dp}{\int_0^1 p^K \cdot q^{N-K} dp} = \frac{\int_0^1 p^{K+k} \cdot (1-p)^{N+n-(K+k)} dp}{\int_0^1 p^K \cdot (1-p)^{N-K} dp} \quad (3)$$

Thus it can determine the occurrence probability of any variant, as the product of the number of variants and the occurrence probability of the variant (eq. 4).

$$P = C^k_n \cdot p = \frac{C^k_n \cdot C^K_N (N+1)}{C^{K+k}_{N+n} (N+n+1)} \quad (4)$$

The sum of all probabilities of possible cases should be equal to 1.

3.2 Case study: Assessing the vulnerability of the air transport system to a terrorist attack. The case study is based on data about terrorist attacks on aviation infrastructure in Europe and North America during 1990-2009. The scenario considered is bomb attack. Statistical data are presented in Fig. 2.

Of the total of 34 attacks launched, 29 have been controlled (with no loss of life or injuries). The question is to determine the probability of combat and the following four possible attacks.

Under these conditions, the problem data are as follows:

$N = 34; K = 29; n = k = 4$

Then:

$$P_4 = \frac{C^4_4 \cdot C^{29}_{34} \cdot 35}{C^{33}_{38} \cdot 39} \cong 0{,}5$$

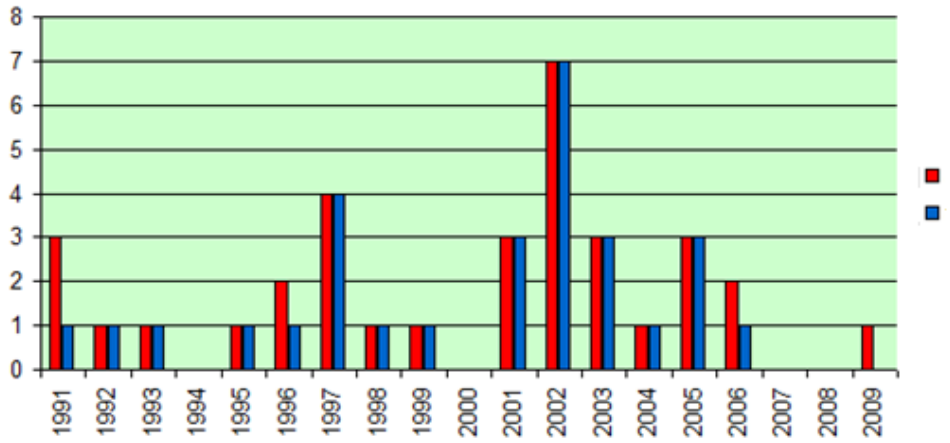

Fig. 2. Bomb terrorist attacks over aviation infrastructure in North America and Europe during 1990-2009
Source: RAND Database of Worldwide Terrorism Incidents

The result can be interpreted in terms of vulnerability, as follows: the next four attacks can be controlled entirely with a probability of 50%, which denotes a vulnerability of the system by 50%.

Similarly it can determine probabilities for other possible variants (no attack controlled in the following 4, controlled 1, 2 or 3 attacks).

4. DETERMINATION OF VULNERABILITY BASED ON THE THEORY OF MULTI-PARAMETER VALUES

4.1 I-VAM model application. The vulnerability is a state of the system/ infrastructure and can be quantified by using the model for assessing the vulnerability of the infrastructure I-VAM (Ezell, 2007). The model is quantitatively, based on the theory of multi-parameter values and adapted for complex systems by using morphological analysis.

Model's architecture is projected onto five functions that measure the level of protection of each subsystem/component. To each of these functions (detection, assessment, response, recovery, and prevention) values are assigned, in a scale of 1 to 100 based on experience or opinion of the experts. The data acquisition process from experts (NUREG 1150, 1990) takes place in six stages:

1. identification and selection of experts;
2. lecture about probability theory;
3. presentation of the risk scenarios and system architecture;
4. collection and analysis of data (software support);
5. presentation and discussion of results;
6. development of risk plan.

The DERRP model is constructed so that each stage contributes to changing the perception of the attacker, in the sense of transmitting the feeling *unable to pass*.

The aggregate value of the function is expressed in relation (5), where m is the size of the assessment, x_m the level of m measurement, $v_m(x_m)$ value of the function at x_m level, and w_m is the product of the weights for each hierarchical level above the calculated (Parnell, 1998).

$$V(x) = \sum_{m=1}^{n} w_m v_m(x_m) \tag{5}$$

The initial data required for the model, represented by the relative importance score and weight of components, are provided by experts and obtained on the basis of an assigning procedure.

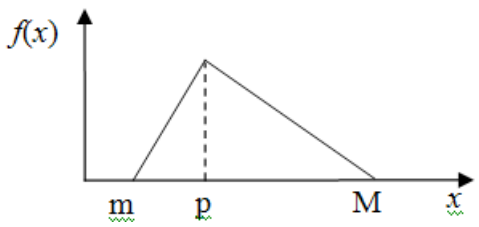

Fig. 3. Triangular distribution

The calculation of the expected conditional value is made using triangular distribution (Haimes, 2004). Considering the minimum (m), maximum (M) and probable (p) values provided by experts as representing values of a triangular distribution, resulting probability density function *f(x)* depending on the random variable *x* (Fig. 3).

The calculation of the expected value E[x] for a triangular distribution is made using the equation (6).

$$\mathrm{E}[x]=\int_{x}^{\infty} xf(x)\mathrm{d}x \tag{6}$$

To create the structure of the value model, a functional decomposition of the system into subsystems and components is required. For example, it is considered the airport infrastructure as a complex system whose functional structure is shown in Fig. 4 (Nisalke, 2009).

On the basis of functional architecture, the I-VAM model can be build. Thus, considering the *aircraft* (1.1.1) as being made up of the *fuselage* (1.1.1.1), *engines* (1.1.1.2), *flight control equipment* (1.1.1.3), you can calculate the value of this component according to the equation (7).

$$v_{1.1.1}(x_{1.1.1}) = w_{1.1.1.1}\cdot v_{1.1.1.1}(x_{1.1.1.1}) + w_{1.1.1.2}\cdot v_{1.1.1.2}(x_{1.1.1.2}) + w_{1.1.1.3}\cdot v_{1.1.1.3}(x_{1.1.1.3}) \tag{7}$$

The vulnerability of the *aircraft* ($\Omega_{1.1.1}$) is calculated (eq. 8) according to the value of the maximum possible score (v^*) and the calculated value ($v_{1.1.1}$).

$$\Omega_{1.1.1} = v^*(x) - v_{1.1.1}(x) \tag{8}$$

The score value of *air operations* subsystem (1.1) is the sum of the products of all the associated components and weight associated. For this case, the subsystem value is given by equation (9).

$$v_{1.1}(x) = w_{1.1.1}\cdot v_{1.1.1}(x) + w_{1.1.2}\cdot v_{1.1.2}(x) + w_{1.1.3}\cdot v_{1.1.3}(x) + w_{1.1.4}\cdot v_{1.1.4}(x) \tag{9}$$

Calculate the subsystem vulnerability ($\Omega_{1.1}$).

Similarly to all other subsystems, resulting in final the vulnerability of the system, expressed in the relation (10).

$$\Omega = V^*(X) - V(X) \tag{10}$$

where $V^*(X)$ represents the maximum value (100) and $V(X)$ is the total value of the system (eq. 11).

$$V(X) = w_{1.1}\cdot v_{1.1}(x) + w_{1.2}\cdot v_{1.2}(x) \tag{11}$$

The following assessment is used to verify the model:

- on every hierarchically level, the sum of the weights must be equal to 1 (eq. 12);

$$\sum_{i=1}^{m} w_m = 1 \tag{12}$$

- the sum of values' products at component level has to be equal to the sum of the products at the subsystem level (eq. 13), and parameters are positive (eq. 14).

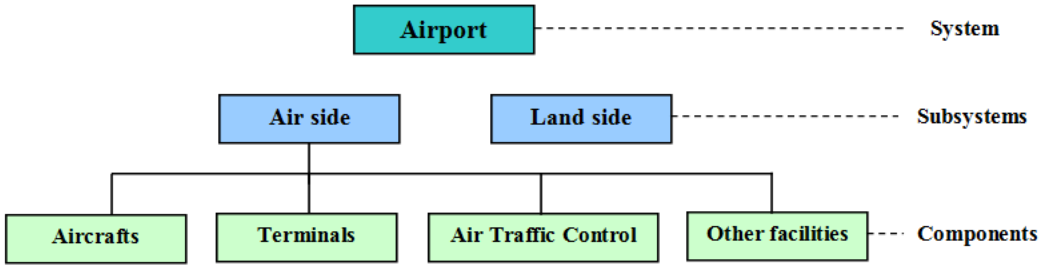

Fig. 4. Simplified functional architecture model of an airport

$$\sum_{i=1.1}^{1.2} w_m \cdot v_m(x_m) = \sum_{i=1.1.1}^{1.2.3} w_m \cdot v_m(x_m) \quad (13)$$

- $x, v(x), w \geq 0$ (14)

I-VAM model carries out the vulnerability assessment of a critical infrastructure/system according to possible scenarios, which realize in fact the link between vulnerability and risk. In the example shown, we have demonstrated that the vulnerability can be quantified through measures contained in the management of extreme events, and the omega value of vulnerability can be easily compared to the system score.

4.2 Case Study: Assessing vulnerability of an airport to a terrorist attack.

The initial data required for the model, represented by relative importance score and weights of components, were supplied by three experts in the field of airport security, on the basis of an assigning procedure. Determination of submitted scores weight was carried out according to the specialty and experience in the security field.

In the shown example was considered, as a measure of protection for each component in the system, the function of detection.

The scenario considered is a terrorist bomb attack on an international airport.

Vulnerability assessment stages are:

1. The functional architecture of the attacked system (theoretical model) (Fig. 4).

2. Assigning relative importance and the calculation of weights for detection function (Table 1).

Table 1. Assigning relative importance

Component	Relative importance	Weight
Aircraft (1.1.1)	10	0.33
Terminal (1.1.2)	9	0,30
Air Traffic Control (1.1.3)	6	0,20
Technical Support (1.1.4)	5	0,17
Access Point (1.2.1)	7	0,39

3. System analysis - data provided by the 3 evaluators were modeled after a triangular distribution (Table 2).

Table 2. Assigning values for each component

Component	Assessor 1 (0,3)		
	Min	Prob.	Max
Aircraft (1.1.1)	0,0	0,1	0,3
Terminal (1.1.2)	0,2	0,5	0,7
Air Traffic Control (1.1.3)	2	10	20
Technical Support (1.1.4)	1	5	15
Access Point (1.2.1)	20	45	90
Registration area (1.2.2)	10	30	45
Public facilities (1.2.3)	15	35	60

4. Calculation of expected value (Table 3).

Table 3. Determine the expected value of vulnerability

Component	Weight	*v(x)*	Ω
(1.1.1)	0.33	0,16	0,14
(1.1.2)	0,30	0,46	0,24
(1.1.3)	0,20	13,0	6,5
(1.1.4)	0,17	6,96	5,94
(1.2.1)	0,39	46,0	32,0
(1.2.2)	0,33	30,1	19,4
(1.2.3)	0,28	39,8	29,2

The value of vulnerability for entire system is 82.89%. The model highlighted a very large system vulnerability (the airport) to the threat (bomb attack) for two reasons:

1. only the detection function was taken into account;

2. identification of the fact that the *land side* induces a significant vulnerability in the system, with all the security measures taken so far.

5. CONCLUSIONS

Quantifying the vulnerability of critical infrastructure according to the threat scenario and the measures of protection that can be applied (detection, evaluation, response, recovery, prevention) is the great reward of the study.

The aim of this study is to define the most appropriate model for the analysis of the vulnerability of the aviation system from the risk of terrorism, allowing an improvement in security and safety. Quantification does not mean certainty, but the adequate surprise growth processes, allowing an understanding of the mechanisms of risk assessment of terrorism in aviation.

Vulnerability assessment challenges come from: reduced number of terrorist attacks and the diversity of strategies used, the fact that one cannot extrapolate the data to estimate the risk of terrorism in the future; the danger of underestimation (to avoid criticism), or overrating (to justify security investments); the call to the community of information (some data collected cannot be used due to the classified nature).

BIBLIOGRAPHY

1. Cheesebrough, T., Wise, R. (2012). *Applying Modeling and Simulation to Estimate Risk Reduction Benefits for Regulatory Benefit-Cost Analysis*, Conference Proceedings Assessing the Benefits of U.S. Customs and Border Protection Regulatory Actions to Reduce Terrorism Risks, Santa Monica, CA: RAND Corporation.

2. Clauset, A., Young, M., Gledistch, K. S. (2007). On the Frequency of Severe Terrorist Events, *Journal of Conflict Resolution*, 51(1), 58-88.

3. Ezell, B. C., (2007). Infrastructure Vulnerability Assessment Model (I-VAM), *Risk Analysis*, 27(3), 571–83.

4. Haimes, Y.Y. (2004). *Risk Modeling, Assessment, and Management*, Second Edition, John Wiley & Sons, New Jersey, U.S.A., 276-294.

5. JASON, (2009). *Rare Events*, Report no. JSR-09-108, The MITRE Corporation, JASON Program Office, Virginia, 21-31.

6. Morar, R., Ştefan, C.E. (2012). On Some Security Measures to Prevent and Fight Aircraft Terrorism. In *Review of the Air Force Academy*, Vol. IX, No. 1(20), 61-65.

7. Newman, M.E.J. (2005). Power Laws, Pareto distribution and Zipf's law, *Contemporary Physics*, No.5, 323-351.

8. Nissalke Jr., T.E., (2009). The Air Transportation System in the 21st Century, *Sustainable Built Environment*, vol. II, EOLSS Publishing House, 365-385.

9. NUREG, (1990). *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, U.S. Nuclear Regulatory Commission:

Final Summary Report, Vol.1, Washington, DC, 52-54.

10. Parnell, G.S., Jackson, J.A., Jones, B.L., Lehmkuhl, L.J., Conley, H.W., Andrew, J.M. (1998): Foundations 2025: A Value Model for Evaluating Future Air and Space Forces, *Management Sciences*, 44:10, p.1336-1350.

11. Ritchey, T., (1997). *Scenario development and risk management using morphological field analysis*, Proceedings of the 5th European Conference on Information Systems, 1053–1059,

12. U.S. Congress (2001). *U.S. Patriot Act of 2001*, P.L. 107-56, Sec. 1016(e), The Library of Congress, 2001.

13. Willis, H., Morral, A., Kelly, T., Medby, J. (2005). *Estimating Terrorism Risk*, MG-388, RAND Corporation, 5-11.

14. Zwicky, F., (1969), *Discovery, Invention, Research - Through the Morphological Approach*, Toronto: The Macmillan Company, 73-84.