

VULNERABILITY EVALUATION OF PERSONNEL, EQUIPMENT AND ACTIVITIES AS A BASE FOR TAKING OF ENGINEER FORCE PROTECTION MEASURES

Jaroslav ZÁLESKÝ, Tibor PALASIEWICZ

University of Defence in Brno, Brno, Czech Republic
jaroslav.zalesky@unob.cz, tibor.palasiewicz@unob.cz

Abstract: *The article describes a vulnerability of personnel, equipment and activities as a factor determining consequences caused by threats. It defines levels of vulnerability and provides a possibility to quantify its levels for all hazards affecting each resource. In conjunction with critical assessment vulnerability evaluation enables to describe severity of each threat impact on particular resource more specifically. The threat severity together with its occurrence probability creates key factor of risk assessment being a base for appropriate engineer force protection measure development.*

Keywords: vulnerability, threat, risk assessment, force protection.

1. Introduction

Vulnerability is an inherent exploitable weakness in an asset. Vulnerabilities include deficiencies in planning, preparedness, training, awareness, warning, physical security, hardening, redundancy/back up, and response capability. [1] It seems to be one of many characteristics predetermining personnel, equipment, infrastructure and activities to be a reason why force protection has become one of key functions of all military operations or activities.

Vulnerability assessment enable planning staff particularize a specific impact level of specific threat to each resource critical for mission accomplishment. The impact together with a hazard occurring probability are base parts of risk assessment resulting to a force protection measures development. Such measures represent a risk management's response on the threat's exploitation of critical asset's vulnerability. If force protection measures are expected to be successful and efficient, each particular risk have to be evaluated as accurate as

possible. It presumes also properly performed vulnerability assessment. Although, the assessment of vulnerability takes a part of hazard identification as stated in NATO doctrine AJP-3.14 Allied Joint Doctrine for Force Protection, no rules for such process in contrast to threat probability or impact has been never mentioned there or in other similar publications.

The article attempts to indicate one of possible attitude how to deal with vulnerability assessment as a base for threat's impact evaluation.

2. Base idea of possible vulnerability assessment approach

Vulnerability assessment as mentioned above hand to hand with criticality assessment and threat assessment forms part of hazard & thread identification step of a force protection model developed in AJP-3.14 (see Figure 1).

DOI: 10.1515/kbo-2018-0161

© 2015. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 3.0 License.

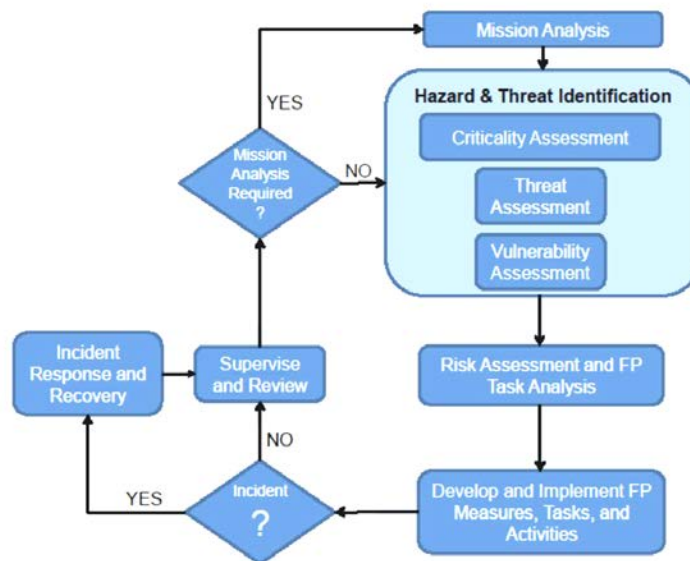


Figure 1: Force protection model [1]

The step follows task analysis and it is followed by risk assessment and force protection task analysis. The goal of the sub step is defined as *identification of vulnerabilities that could be exploited by threats and the impact of incidents on the force's effectiveness and Allied political will, thereby affecting mission success* [1]. The purpose of vulnerability assessment (VA) process is to *determine the susceptibility of assets to attack from threats or degradation due to hazards identified in the task analysis. Each vulnerability assessment is accomplished by multi-disciplinary subject matter experts who conduct operational analyses and assess the vulnerability of personnel, materiel, information, facilities, and other assets. The result of a VA is the identification of deficiencies or weaknesses that render critical assets, areas or special events vulnerable to a range of known or likely threats or hazards* [1]. The purpose and the definition of VA has been therefore explained sufficiently. However, its method of execution depends on procedures used by each NATO state or organisation.

Before creating potential way of VA authors had conducted research including publications study and knowledge interviews with Czech army experts and staff officers and other employees as well as with similar specialists from abroad. The result has verified an expectation that ways of vulnerability assessment vary in each army force of each NATO state in a comprehensiveness and a range of usage from numerical scales, to verbal evaluation. Especially, Czech attitude is limited to quite common usage of the SWAT analysis.

The necessity to develop a vulnerability method evaluating it more thoroughly to include all aspects of resources and threats in conjunction with its quick and not so complicated execution formed a base for a following draft.

3. Vulnerability rate scale model

As a baseline for vulnerability assessment the vulnerability rate scales have been established. Example of vulnerability degrees set for personnel and equipment is introduced in table 1.

Table 1 Vulnerability degree definitions for personnel and equipment [4]

Degree of Vulnerability	Personnel	Equipment
5	Threat causes fatal injuries to personnel	Threat causes total destruction of equipment or damages requiring more 1000 man-hours to be repaired
4	Threat causes major to fatal injuries to personnel	Threat causes damages requiring 400 to 1000 man-hours to be repaired
3	Threat causes minor to major injuries to personnel	Threat causes damages requiring 100 to 400 man-hours to be repaired
2	Threat causes no injury to major injuries to personnel	Threat causes damages requiring 60 to 100 man-hours to be repaired
1	Threat causes no injury to personnel	Threat causes no damages or damages requiring 40 to 60 man-hours to be repaired

Proceeding from the assumption that each threat may harm each asset by the way typical for the interaction specific threat – specific asset each degree of vulnerability is described by words. There are four potential relationships between hazards and resources:

- Threat may jeopardize more than one resource critical for successful mission accomplishment.

- Resource can be jeopardized by more than one threat.
- Only one threat can jeopardize just one resource.
- There is not a relationship between threat and a resource.

Based on fact mentioned above the model of hazard displayed on figure 2, may be developed for particular type of personnel, equipment, stock, structure or activity.

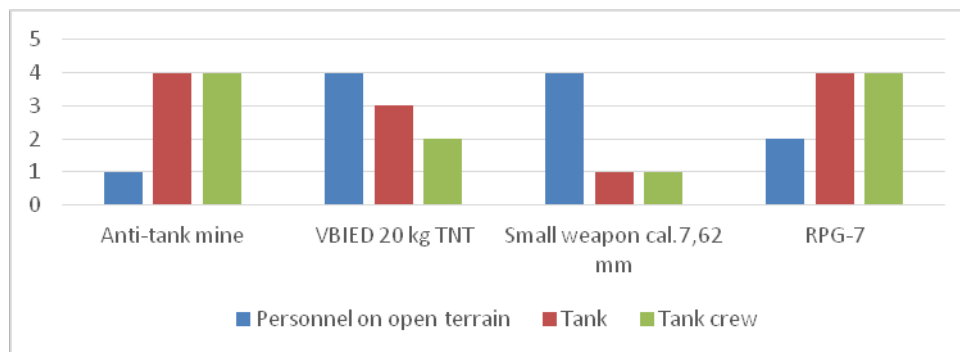


Figure 2: Example of Equipment and Personnel Vulnerability Model [author]

The model can be used for assessment of risk caused by certain threat threatening certain asset or using a synergy effect assess the level vulnerability of the asset threaten by more hazards in the operational area or during mission accomplishment. The connection of more vulnerability models (see figure 2) makes a possibility to identify a vulnerability degree of asset using other asset as a protection measure.

The example could be a tank crew. If taken in account protective properties of tank, it will significantly reduce human vulnerability to small arms in comparison with persons operating on opened terrain. However, when accidental claustrophobia is taken in account it will influence the degree of human's vulnerability as well. Vulnerability scale model designed here can be therefore a method of vulnerability

assessment, which seems to be useful, easy applicable and flexible in usage.

4. Vulnerability rate scale model implementation into the risk

management

Process of risk assessment is based on risk assessment matrix (see figure 3).

RISK ASSESSMENT MATRIX						
Severity		Probability				
		Frequent A	Likely B	Occasional C	Seldom D	Unlikely E
Catastrophic	I	E	E	H	H	M
Critical	II	E	H	H	M	L
Marginal	III	H	M	M	L	L
Negligible	IV	M	L	L	L	L
E – Extremely High		H – High		M – Moderate		L – Low

Figure 3: Risk Assessment Matrix [3]

The method takes in account the probability and the severity of threat's exploitation of asset's vulnerability. The degree of vulnerability described above will find expression in setting of severity degree if matrix is expressed as numerical.

Level of risk can be determined using equation

$$R_u = D_z \cdot P_v \quad (1)$$

where, R_u = expected level of risk, D_z = level of severity and P_v = level of probability.

The degree of vulnerability ST_{zr} can affect level of severity D_z along with level of asset criticality H_d expressing how critical is the asset for successful mission accomplishment. The relationship can be formulate as

$$D_z = ST_{zr} \cdot H_d \quad (2)$$

where, D_z = level of severity, D_z = degree of vulnerability and H_d = level of criticality.

It is clearly visible, that force protection measures taken in order to reduce assessed level of risk will also reduce vulnerability degree apart from other things.

5. Engineer force protection measures

They are four approaches of dealing with risk:

- To avoid the risk.
- To reduce probability.
- To reduce severity.
- To accept the risk.

Apart from the last possibility, engineer force protection measures can be taken to support all approaches mentioned above. They may be both active and passive providing mainly a survivability support. They are:

- Preparation and construction of field fortifications.
- Hardening and construction of protective infrastructure works.
- Camouflage, concealment and deception.
- Clearance of fields of fire.
- Explosive threat Management. [2]

Depending of risk level and risk management approach, they could decrease a vulnerability of particular source that is critical for specified mission.

After they are developed and applied, it will

be necessary to reassess a level of risk including a vulnerability degree evaluation. If the degree of vulnerability and consequently the level of risk are decreased, measures will be successfully used as risk mitigation means.

6. Conclusion

Engineer force protection measures may support risk mitigation helping to avoid risk and to reduce a severity or probability of threat's exploitation of particular asset vulnerability. The vulnerability assessment is a part of risk assessment giving a reply to

question, how such asset may be harmed or damaged by particular hazard affection. Although appropriate NATO document mentions that the vulnerability assessment has to be conducted, a method of such evaluation has not been described and each NATO state has been responsible to create their own VA approach.

One possible approach has been developed and publically reported in this article.

References

- [1] NATO Standardization Office (NSO), *AJP-3.14 Allied Joint Doctrine for Force Protection*, NATO standard, Brussels, NSO, 2015, 80 p.
- [2] NATO Standardization Office (NSO), *ATP-3.12.12 Allied Tactical Doctrine for Military Engineering*, NATO standard, Brussels, NSO, 2016, 80 p.
- [3] Headquarters Department of the Army, *FM 5-19 (FM 100-14) Composite Risk Management*, US Field manual, Washington, DC, MoD, 2006, 101 p.
- [4] CAPT. Ing. Jaroslav Záleský, *Ženíjní opatření ochrany vojsk v operacích mimo území České republiky*, Doctoral Thesis, Brno, University of Defence, 2012, 162 p.