ANNALS OF THE ORADEA UNIVERSITY
Fascicle of Management and Technological Engineering
ISSUE #1, MAY 2013, http://www.imtuoradea.ro/auo.fmte/

CRITICAL INFRASTRUCTURES PROTECTION THROUGH THREAT ANALYSIS FRAMEWORK

Cristina Petronela SIMION[1], Olga Maria Cristina BUCOVETCHI[2], Cristian Aurelian POPESCU[3]
[1]University "Politehnica" of Bucharest, Romania, cristinas_upb [at] yahoo.com
[2]University "Politehnica" of Bucharest, Romania, olgabucovetchi [at] yahoo.com
[3]University "Politehnica" of Bucharest, Romania

Abstract. Nowadays it becomes more and more difficult to prevent malicious attacks as pieces of information are confidential and therefore stakeholders cannot be informed properly in order to react in real time. The present study presents the threat analysis framework as a suitable model to use in this situation as it allows you to quantify threats and develop means that makes possible transformation from classified into non-classified information and their communication. The authors took into consideration three different types of critical infrastructures to verify if the threat analysis framework represents a suitable model or not.

Keywords: Critical infrastructures, threat analysis framework, vulnerability

I. INTRODUCTION

DEFINING threat to critical infrastructures (CI) represents a key aspect of risk assessment. Critical infrastructures protection is a must in the national defense strategy every CI is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people [1]. Un-developed defense methods that are used for most CI are enough to defeat the resources and the capabilities of low-ranking threats; yet, as the enemies' capabilities grow, it becomes less likely for present defense systems to defeat enemies' attacks and the risk becomes greater and more difficult to diminish. [2].

As there is a great variety of threats, it is important for them to be described in such a manner in order to allow their classification. In this case, it isn't that important the threat itself, but the enemy represented by the threat in discussion. The most interesting feature to be known are the capabilities of the threats attacking a CI in order to be able to defend the CI against the vector of complex attack that can be drown by a threat. This feature allows the CI to develop appropriate defense strategies, yet not to react step-by-step to each individual threat. As a consequence, the threat "market" shall be divided using enemies' capabilities understanding in order to select the most efficient strategy against real threats' classes. There must be developed several non-secret threat analytical elements in order to communicate information regarding likely consequences of a threat useful when enhancing CI defense strategies. Nowadays, most information concerning high-level threats is confidential in order to protect sources and collecting information manner. This prevents dissemination in real time. To avoid this drawback, there has to be developed a Threat Analysis Framework which does not obey the rules of classification, yet, it provides a method able to use secret information that keeps some classified items within [3].

II. THREAT ANALYSIS FRAMEWORK MODEL

Threat Analysis Framework is a technique that allows you to quantify the threats to CI and it provides a means of information distribution related to possible action in order to protect those CI.

Threat Analysis Framework starts with key elements associated threats identification, impact and neutralization (diminishing). Threat Analysis Framework method does a complete analysis of the threat through identifying and describing five key aspects: enemies' identification, general threat profile development, general pattern of attack identification, malicious intent determination and mitigation and diminish strategies identifying **[**4**].**

The first element is the enemies' identification. This is usually confidential and therefore it is not allowed to communicate to the stakeholders the information concerning likely actions to put into practice. This is why the second element concerns enemies' characteristics identification and a threat profile development in order to describe the enemy's capabilities (non-classified information). The third element, based on the capabilities developed under the second element, identifies the general ways to attack the enemy (the opponent). The fourth element is based on a process due to which it can be discovered in an estimated real period of time the enemy-related activities that may provide an early warning of the enemy's intention to take advantage of a vulnerability/ weak point of the critical infrastructure. The final element of the Framework for Analyzing the Threat identifies the best strategies to mitigate and reduce the overall risk for the critical infrastructure not to be compromised.

Fig. 1. represents the necessary elements to provide adequate information to protect the CI against an enemy attack [4].

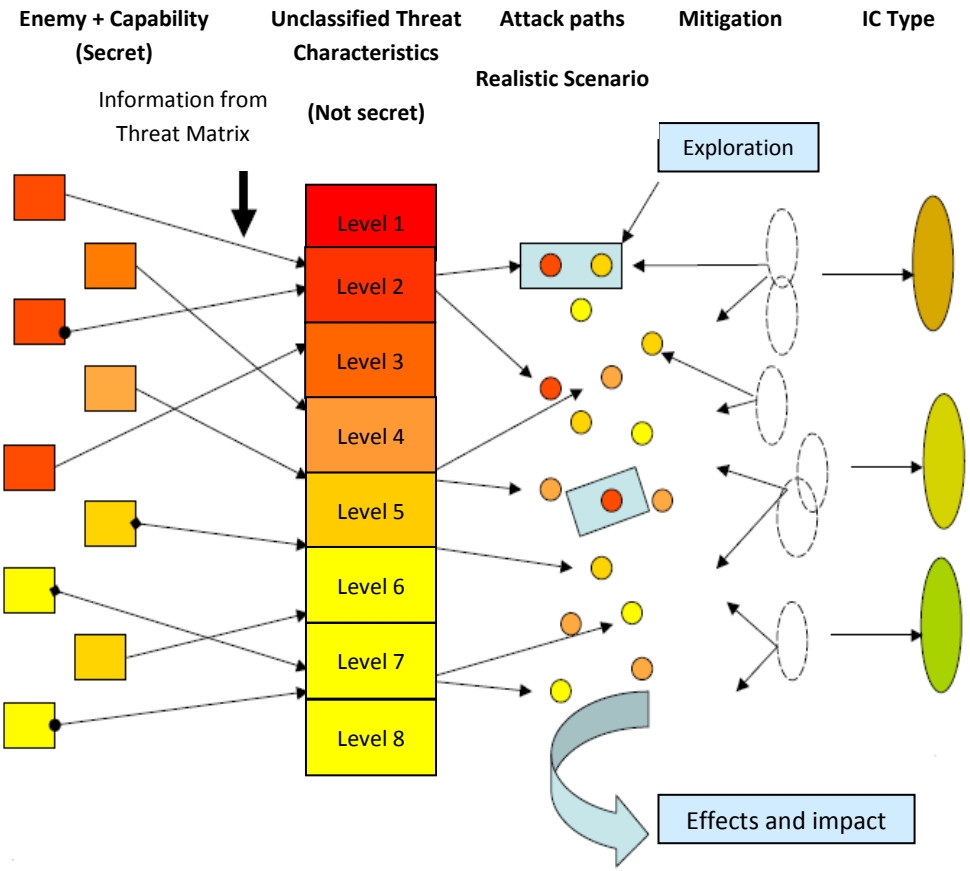

Fig.1 Threat Analysis Framework
Adapted from: D.P Duggan., J.T. Michalski [4]

III. THE DEVELOPMENT OF GENERAL THREATS PROFILES

The first necessary action to declassify secret information related to enemy is to characterize the threat by developing its general profiles, named *Threat Analysis Framework* [5]. This matrix ranks the threat in a general manner, even if it is impossible to include each different type of threat. Therefore, different threat profile levels and their capacities to set off an attack on CI are determined, without associating secret information (for example, the enemy identity). After level ranking of the threat capacities, the general attack vectors (the possible attack paths), that can be sustained by these capacities, can be identified and then the consequent attenuation and reduction actions against the attack are developed.

The development of the Threat Analysis Framework is a qualitative research, meaning that the analysis used to determine the nature of attributes and the behavior of the analyzed threat are based on rational judgment. The procedure to determine the matrix implies mainly two important steps [5]:

1) Identification and definition of *threat attributes* and establishment of a scale for each attribute, used to assign a threat intensity;

2) Usage of attributes to characterise the threat general profiles and the actual implementation of the matrix.

A *threat attribute* represents a discrete characteristic or a distinctive property it possesses. The combined characteristics of the threat describe the threat ability and consistency to follow its goal. There are two categories of threats: the category of attributes aiming *commitment*, which describe the potential of the threat and the category of attributes related to *resources*, which describe the threat's ability.

The *commitment attributes* are the characteristics of a threat which quantify the threat to follow its goal. The threats with the most pronounced consent won't be stopped by anything in their attempt to follow their goal, while those with the smallest consent won't have the same ambition and determination.

There are three attributes in the category of those related to commitment: *intensity*, *discretion* and *time*.

The *attribute of intensity* describes the persevering determination, the passion with which the threat follows its goal. This attribute is a measure of how far a threat

can go and how much is willing to risk to reach its goal. Therefore, the threats with higher intensity are more dangerous. The intensity is ranked on three levels: high, medium and low [6].

The *attribute of discretion* describes the ability of a threat to keep its necessary level of secrecy (discretion) in reaching its goal. Maintaining the threat secret requires the ability to hide details (partially of totally) related to the threat, including goals, structure or internal activities. A high level of discretion permits the threat to hide its intentions and internal structure from the outside world. Discretion is also ranked on three levels: high, medium and low.

The *time attribute* quantifies the period of time which a threat is able to dedicate for planning, development and progress of methods to reach its goal. In the case of cybernetic or kinetic threats, it includes the period of time needed for all the implementation steps until execution. As the threat is more willing and able to engage in the attack preparation, the greater is the threat potential to have a devastating impact. There are four levels of time: from years to decades, from months to years, from weeks to months, from days to weeks.

The category of attributes related to *resources* represents characteristics of the threat which quantify the human resources, knowledge and available access. The resources are indicators related to the threat capability because the abundant resources permit the threat to reach its objectives easier and with a greater adaptability. There are three attributes in this category: *technical staff*, *knowledge* and *access*.

Using the attributes previously described, The Threat Analysis Framework matrix can be developed (Table I).

These profiles can be then used to identify the potential attack paths and to take the necessary measures of attenuation and reduction of their effects.

TABLE I.
THREAT ANALYSIS FRAMEWORK

Threat level	THREAT PROFILE						
	COMMITMENT			RESOURCES			
	Intensity	Discretion	Time	Technical staff	Knowledge		Access
					Cybernetic	Kinetic	
1	H	H	> years	Hundreds	H	H	H
2	H	H	> years	> dozens	M	H	M
3	H	H	> months	> dozens	H	M	M
4	M	H	> weeks	Dozens	H	M	M
5	H	M	> weeks	Dozens	M	M	M
6	M	M	> weeks	individuals	M	M	L
7	M	M	> months	Dozens	L	L	L
8	L	L	> days	individuals	L	L	L

The threat situated on level 1 will always be the most capable to reach the goal, while the one on level 8 will be the least capable. Each threat level, from 8 to 1, represents a more dangerous threat than the one situated on the previous ranking level. Even if a threat ranked on level 8 is able to reach the same goal as one on level 1, this situation can be due to the existence of an unprotected vulnerability, to a random synchronization of attack or simply can be a matter of luck, without the threatening organization to have a capability characteristic [3, 7].

If a threat does not perfectly match one of the levels presented in the matrix, then it will be ranked on the closest level to its profile.

The threats that can have the profile checked as mentioned in the model have been identified through a rigorous study on three different sectors of CI: energy, chemistry and nuclear industry and financial sector. Furthermore, the result of this study is represented by the identification of the inside and outside threats to these CI.

The identified inside threats have as sources:

1) the employees (the insiders);
2) equipment's reliability;
3) the used procedures.

These threats can have different motivations; they can be passive or active, violent or non-violent, rational or irrational. The term "motivation" is used in order to describe the motivational forces that drive one insider to try or even put in practice a malicious attack. Motivation may include factors such as ideology, personal believes, financial or psychological motivation and also other

factors such as coercive actions driven against himself or his family members. The insider may act individually or within a group, driven by a stimulus or premeditated and well prepared, everything depending on his motivation.

The passive insiders are non-violent and they limit their actions to providing information to those who are to carry out or at least try to carry out a malicious attack.

On the other hand, the active insiders are willing to provide information and also to carry out malicious actions; they can be both violent and non-violent. The non-violent ones are not willing to be identified or be engaged in action of force. The violent ones, on the contrary, they can use force and act rationally or irrationally.

The outside threats that follow the model when we validated are:

- threats resulting from human activity;
- threats from cyberspace: the increasing activity of hackers, cyber terrorism.

Human threat sources are represented by password crackers, identity forgery, information destruction, cybercrime, information illegal disclosure, illegal financial earnings, system penetration, theft of information, industrial or economic espionage, sabotage of system…

IV. CONCLUSIONS

The analysis of the threats to critical infrastructures by development of their general profiles leads to the following conclusions:

1) The threats with the profile on level 1 of the matrix will have the greatest capabilities for each attribute;

2) The threat levels from the technical staff attribute permit the understanding of the other threat attributes; therefore, the threat with more technical staff will have greater levels of intensity, knowledge and access; the threats with technical staff employed on individuals will not possess advanced knowledge due to the fact that these threats have a small capacity to distribute information or to run research and development programs; also, these threats will not have greater intensity because they are unlikely to auto-sacrifice.

3) The knowledge level follows a certain pattern; therefore, threats with great cybernetic knowledge will not have reduced kinetic knowledge and vice-versa, due to the application of expert competences in both theoretical and practical domains.

4) On the access ability, it can be said that threats with great knowledge, cybernetic or kinetic, will have at least one access of medium level due to the fact that it is easier to obtain and more difficult to discover the access obtained with the help of a high competence.

Given a continuously growing number of threats, the key managerial strategies to find appropriate protection of CI is the thorough understanding of the capabilities of these threats.

Threat Analysis Framework provides a comprehensive approach to threat management. This method enables, in a ration and comprehensive manner, to find the most efficient and effective responses to the problems posed by the threats against CI.

REFERENCES

[1] Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

[2] P. Baybutt „Assessing risks from threats to process plants: Threat and vulnerability analysis", *Process Safety Progress*, Vol.21, No.4, 2012, pp. 269-275, DOI: 10.1002/prs.680210403.

[3] P.C. Simion, „Vulnerability management in case of nuclear critical infrastructures exposed to multiple threats", *PhD Thesis*, 2012 („Managementul vulnerabilitatilor infrastructurilor nucleare critice expuse amenintarilor multiple", Teza de doctorat)

[4] D.P Duggan and J.T. Michalski, „Threat Analysis Framework", *Tech.Rep. SAND2007-5791*, 2007, Sandia National Laboratories, USA.

[5] C.P. Simion, A. Gheorghe, C.A. Popescu, "Methods of Threats Assessment Applied For Managing NPP Critical Infrastructure". *The 5th International Conference of Management and Industrial Engineering, Change Management in a Dynamic Environment*, (20-21) October 2011, Bucharest, Romania, pp. 427-431, ISBN: 978-973-748-658-5.

[6] D.P. Duggan, S.R. Thomas, C.K.K. Veitch and L. Woodard, „Categorizing Threat Building and Using a Generic Threat Matrix", *Tech.Rep. SAND2007-5791*, 2007, Sandia National Laboratories, USA.

[7] J. Agarwall, D. Blockley, N. Woodman, "Vulnerability of Structural Systems", *Structural Safety*, Vol. 25, No.3, 2003, pp. 268÷286.