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].

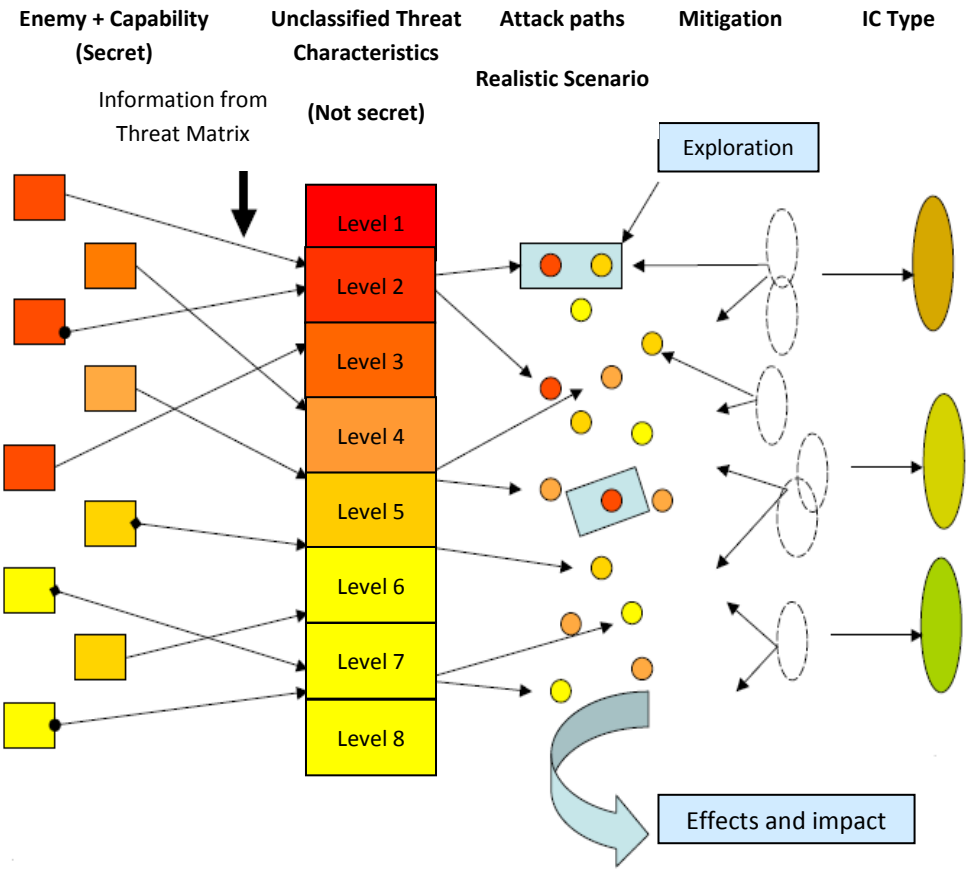

Fig.1 Threat Analysis Framework
Adapted from: D.P Duggan., J.T. Michalski [4]

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