A Concept of Simulation Based Diagnostic Support Tool for Terrorism Threat Awareness

Col. Prof. Andrzej Najgebauer PhD, DSc, member of NMSG
Col. Ryszard Antkiewicz PhD, Maj. Wojciech Kulas PhD, Capt. Dariusz Pierzchała PhD
Capt. Jarosław Rulka PhD, Capt. Zbigniew Tarapata PhD,
2nd Lt. Mariusz Chmielewski MSc
Military University of Technology, Faculty of Cybernetics
Warsaw, Poland
tel: +4822 6839429, fax: +4822 6837262

anajgeb@isi.wat.udu.pl, rantkiew@isi.wat.edu.pl, wkulas@isi.wat.edu.pl, darp@isi.wat.waw.pl,
jrulka@isi.wat.waw.pl, ztarap@isi.wat.edu.pl, mchmiel@isi.wat.edu.pl

ABSTRACT

In this paper we will describe the concept for simulation based decision support tool for predicting possible terrorist activities. Described simulator will improve NATO's capabilities on predicting possible threats concerning terrorist activities as well as developing various campaigns for antiterrorism actions that could lead to efficient reactions on such situations. The idea of such simulator will be developed using HLA standard for simulation interoperability. An approach to information model development on the basis on current taxonomies of Early Warning Systems will be proposed. Example components of such database will be presented using Unified Modelling Language. Analytical database will be the part of the system on which the simulation scenarios will be developed. The simulation process will be based on models of asymmetric conflicts that derive data from analytical part of the system. Developed scenarios and possible antiterrorist activities will concern not only short term forecast but also will enable government institutions to prepare and take long term steps to deal with possible threats. This work is strictly connected with MSG 026 project of Early Warning System considering not only developing the tool itself but also reasoning procedures for knowledge bases.

INTRODUCTION

Concerning to the years' study MSG 026 we would like to present a concept of modelling and development of an Early Warning System for diagnosis and signalling terrorist activities, and additionally simulation of probable attack and its consequences. There are many definitions of early warning system. For example Early Warning System can be considered as a part of Crisis Management System and understood as information system that processes any information from any source about escalatory developments, be they slow and gradual or quick and sudden, far enough in advance in order for a national government or an international or regional organisation to react timely and effectively, if possible still leaving them time to employ preventive measures.

For our purposes we can introduce more detailed definition not contradictory to above. We can assume that the early warning system (EWS) will be a simulation-based diagnostic support tool with its associated algorithms that realises the following processes:

- collecting information relevant to the terrorism threat estimation and intelligence data analysis from:
  - primary threat factors determination
  - aggregated threat factors (causative and executive) determination

Paper presented at the RTO NMSG Symposium on "Modelling and Simulation to Address NATO's New and Existing Military Requirements", held in Koblenz, Germany, 7-8 October 2004, and published in RTO-MP-MSG-028.

    - threat coefficient estimation
    - possible goals of terrorist attack identification

- the analysis and simulation of the information in order to predict terrorism threat over long periods of time, the stability of the threat factors and the signalling when a break-through of a pre-determined threshold is detected.
- the visualisation of EWS output for potential users.

We would like to stress the role of simulation that could be used for predicting of threat indicators value, possible methods, targets, consequences of attack and for training of analysts and decision makers in the subject of crisis management. As the first step of modelling and development of the EWS we propose the requirements definition on the basis of RUP methodology. In the next part of the paper we try to describe a scheme of method of threat factors value determination considering different techniques. The idea of simulation in two roles is presented.

EARLY WARNING SYSTEM REQUIREMENTS DEFINITION

Starting from actors and basic functions definition (RUP methodology) we can determine so-called use-cases. It is very helpful in organization analysis from an external user point of view. There is fixed the following use case diagram, where we can find such actors:

- government or president
- military staff
- police staff
- emergency staff
- security staff
- C4ISR system
- external warning system
- external data base system
- information media (press, TV, radio)
- Internet
- telecommunication system
- sensor

The basic categories of functions in the organisation (Early Warning System) are as follows:

- Collecting of primary threat information
- Evaluation of security:
    - Identification of security state
    - Prediction:
        - Prediction of security state
        - Prediction of attacks method
        - Prediction targets
        - Prediction of consequences
- Simulation of crisis
- Training

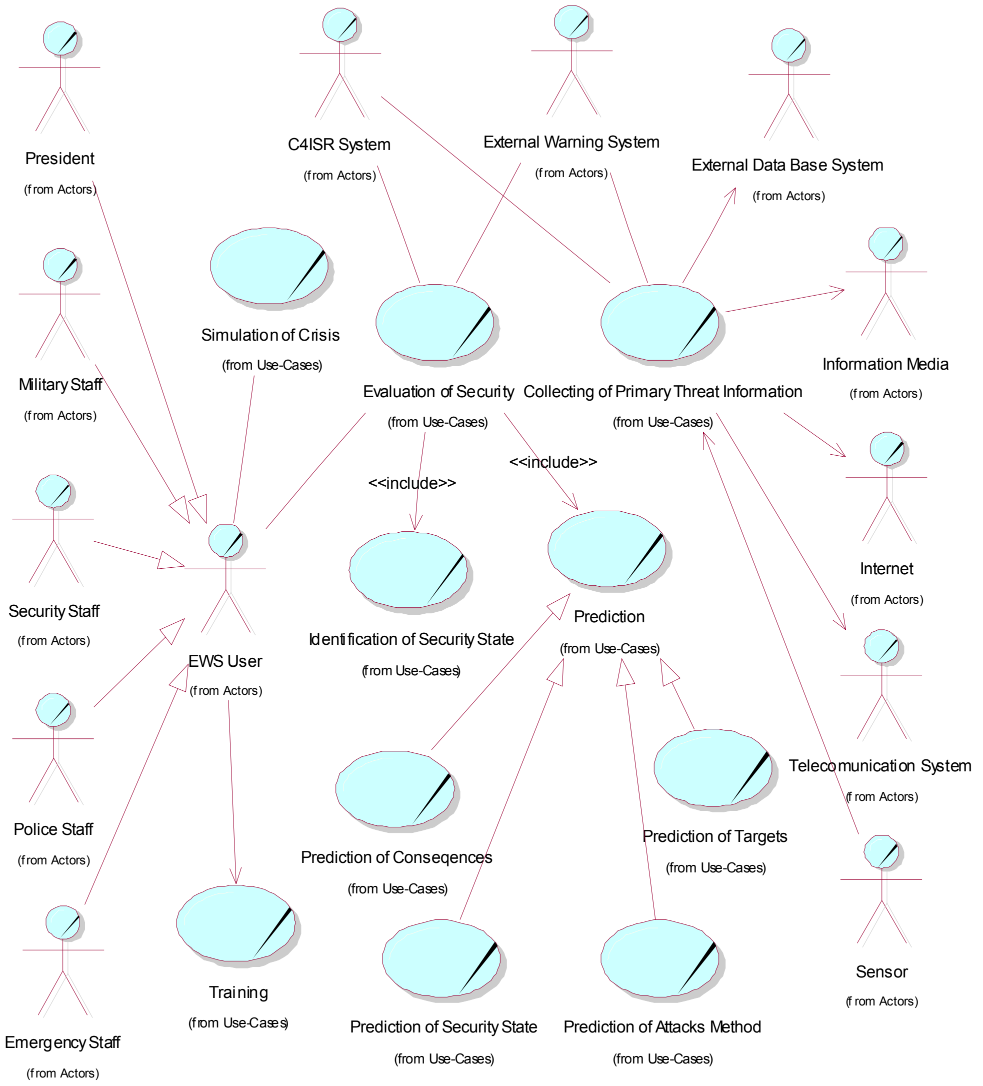

Fig. 1: Use-case diagram of EWS.

One of possible path of analysis of the organization there is sequence of events. The diagram contains activity and data objects, methods (functions and procedures that the objects realise), order of object's methods invocation. The most extensive sequence diagram is connected with Sensor actor (see the fig. 2).

On the top of the diagram there are objects as follows: Register of Primary Data, Primary Factor, Verifier, Primary Data Base, Aggregated Objects, Causative Factor, Executive factor, Secondary Data Base, Analyst, Threat Identifier, Threat Coefficient, Threat Coefficients Data Base, Predictor, Prediction, Scenario Generator, Crisis Scenario, Simulator, Scenario Data Base. Each object has own "life line" (vertical dashed line) and activities represented as rectangles on the "life line". Method's invocation or message dispatching is represented as an arrow. For example: the object "Register of Primary Data" calls "Select Primary Data()" from the object "Primary Data Base". Some of methods may be invocated conditionally (e.g. "Predicted Variable Estimation()"). This way makes easier choice of such activities that can be computerized.

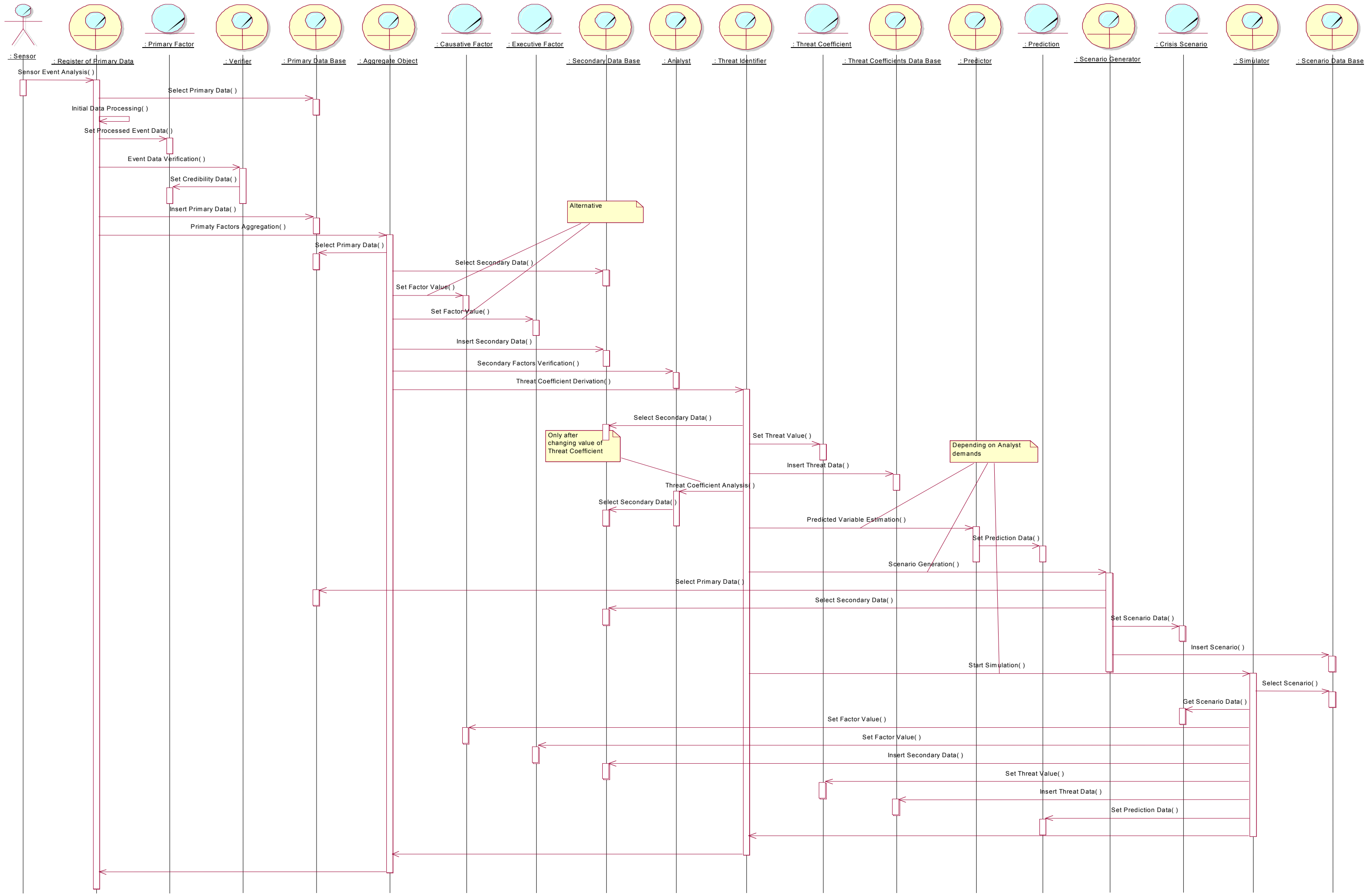

Fig. 2: Collecting of Primary Threat Information from Sensor sequence diagram.

The other examples of events sequence describe:

- identification of security state by the EWS User (Fig. 3);
- prediction EWS User (Fig. 4).

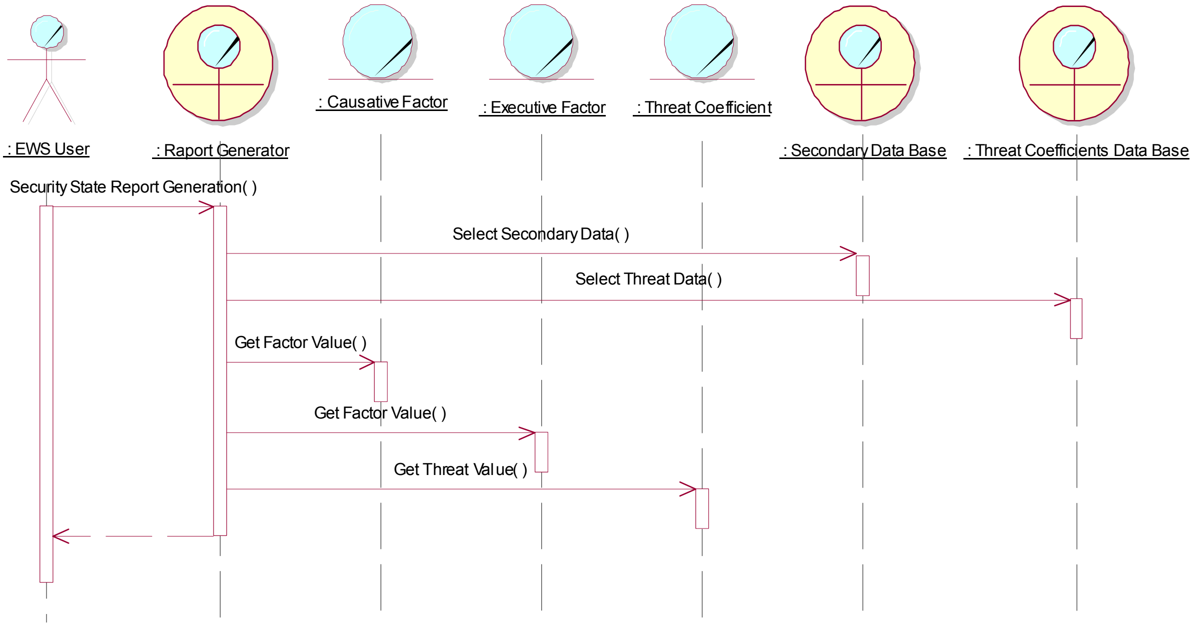

Fig. 3: Identification of Security State EWS User Sequence Diagram.

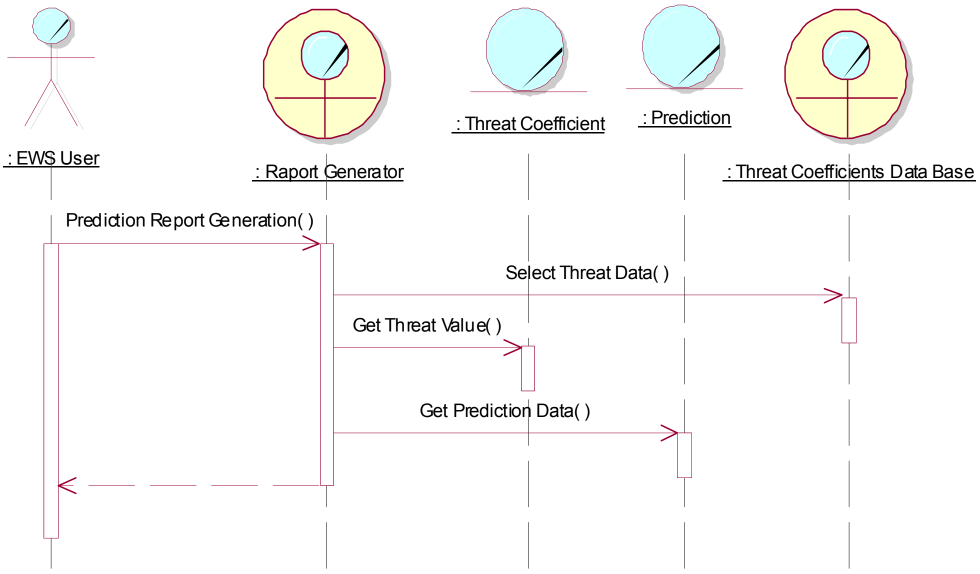

Fig. 4: Prediction EWS User Sequence Diagram.

Complementary view of EWS is presented using activity diagram. This type of diagrams shows general algorithm realisation of basic EWS functions (use-cases). The following diagrams present algorithms for:

- Collecting of Primary Threat Information (Fig. 5);
- Identification of Security State (Fig. 6);
- Prediction (Fig. 7);
- Simulation of Crisis (Fig. 8);
- Training (Fig. 9).

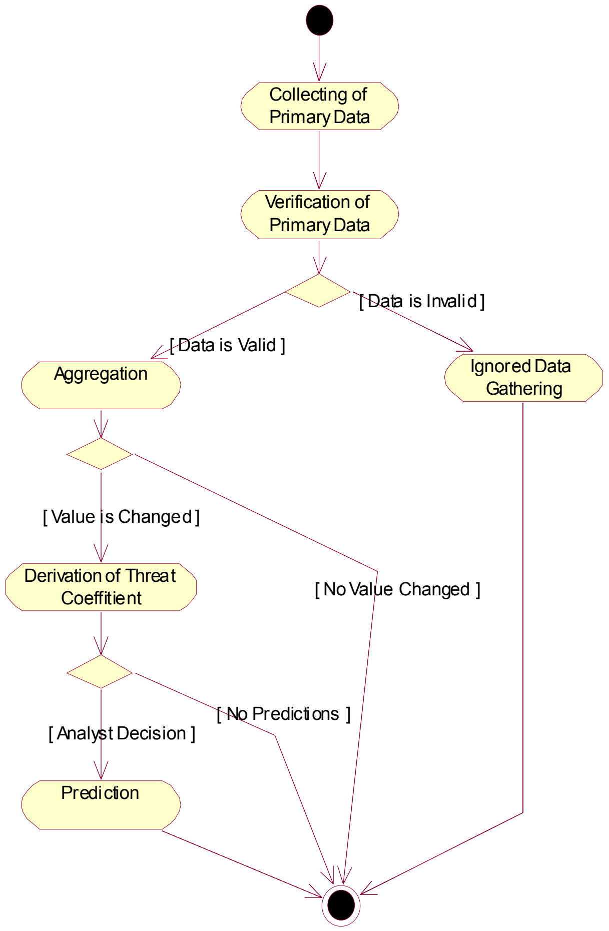

Fig. 5: Collecting of Primary Threat Information Activity Diagram.

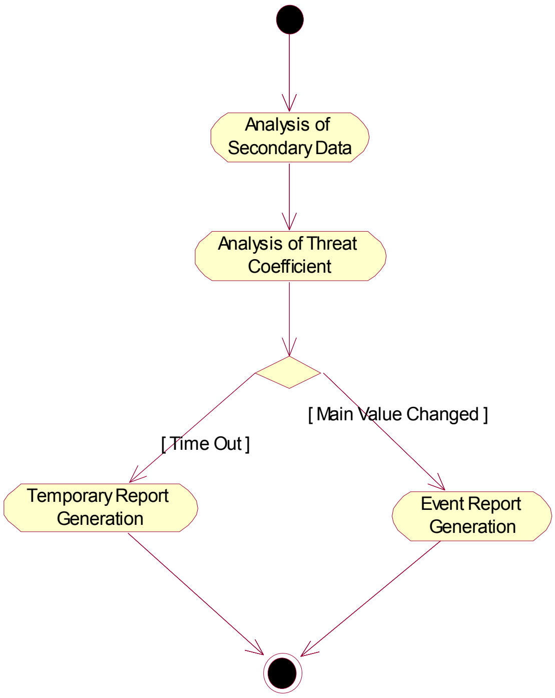
Analysis of Secondary Data
Analysis of Threat Coefficient
[Main Value Changed]
[Time Out]
Temporary Report Generation
Event Report Generation

Fig. 6: Identification of Security State Activity Diagram.

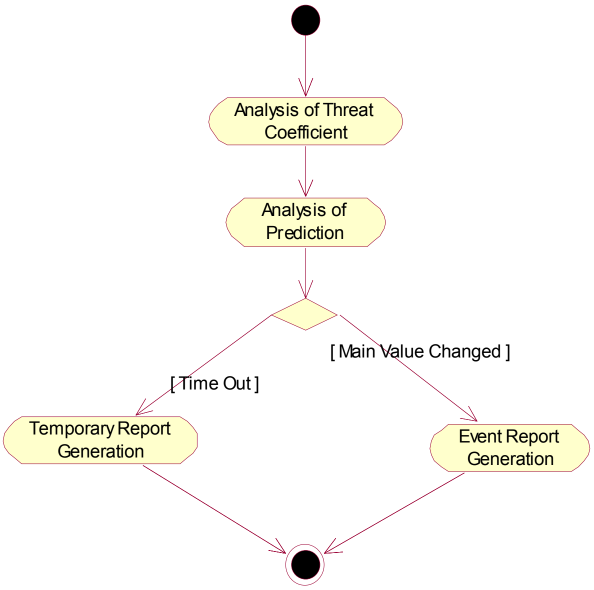

Fig. 7: Prediction Activity Diagram.

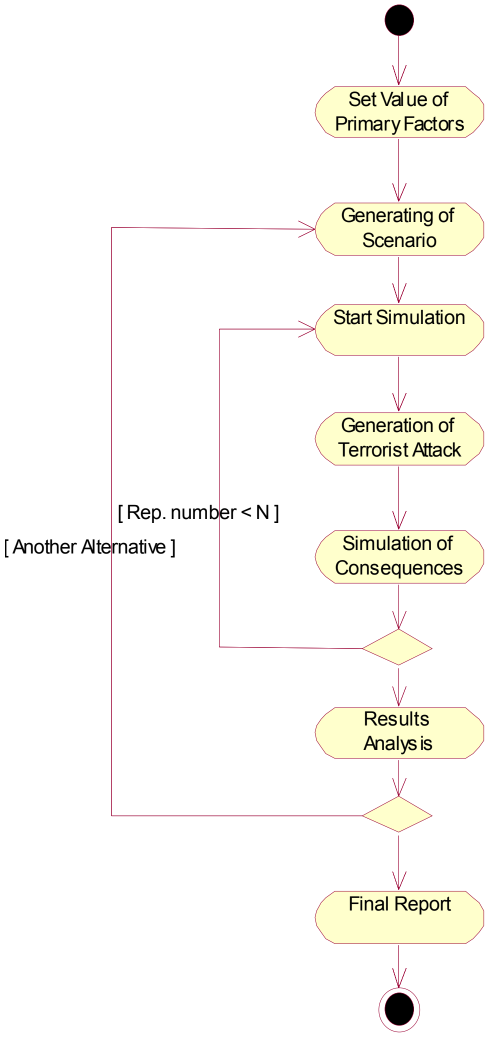

Fig. 8: Simulation of Crisis Activity Diagram.

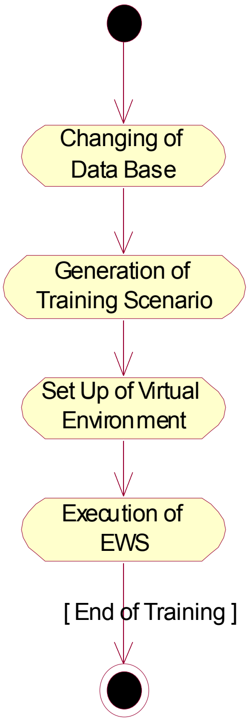
Changing of Data Base
Generation of Training Scenario
Set Up of Virtual Environment
Execution of EWS
[End of Training]

Fig. 9: Training Activity Diagram.

FORMAL MODELLING OF TERRORIST THREAT

Terrorist threat model:

$$TTM(t) = \left\langle (E_n(t))_{n=1..N(t)}, \boldsymbol{ToE}, (Cr_k(t))_{k=1..K(t)} \right\rangle$$

$\boldsymbol{ToE} = \{1,..,M\}$ number set of entrant types.

The entrant $n \in \boldsymbol{N}$ is described as follows:

$$E_n(t) = \left\langle e_{n,1}(t), e_{n,2}(t), e_{n,3}(t) \right\rangle$$

$e_{n,1}(t)$ – number of entrant type ($e_{n,1}(t) \in \boldsymbol{ToE}$)

$e_{n,2}(t)$ – set of entrant numbers, if the coalition of the entrant and an entrant from the set is possible,

$e_{n,2}(t) \subset \{1,..,N(t)\}$

$e_{n,2}(t) = \varnothing$ => n-th entrant can’t be in a coalition.

$e_{n,3}(t)$ – description of entrant, according to appropriate entrant type description $e_{n,1}$

m = 1 – terrorist organization

$$E_n(t) = \left\langle e_{n,1}(t), e_{n,2}(t), e_{n,3}(t) \right\rangle$$

if $e_{n,1}$(t)= 1 then $e_{n,3}(t) = \left\langle e^1_{n,3}(t), e^2_{n,3}(t), ,..., e^{16}_{n,3}(t) \right\rangle$

$e^1_{n,3}(t)$ - estimated number of members in the organization

$e^2_{n,3}(t)$ - set of countries where the organization is active

$e^3_{n,3}(t)$ - set of activity area for all countries

$e^4_{n,3}(t)$ - degree of the terrorist professionalism

$e^5_{n,3}(t)$ - complexity of the terrorist organization structure

$e^6_{n,3}(t)$ - financial resources

$e^7_{n,3}(t)$ - set of known financial sponsors

$e^8_{n,3}(t)$ - level of members discipline

$e^9_{n,3}(t)$ - applied methods of terrorist attacks

$e^{10}_{n,3}(t)$ - intensities of each type of attack

$e^{11}_{n,3}(t)$ - result size of each type of attack

$e^{12}_{n,3}(t)$ - description of known members and followers of the organization

$e^{13}_{n,3}(t)$ - set of types of attacked objects

$e^{14}_{n,3}(t)$ - owners of attacked objects

$e^{15}_{n,3}(t)$ - country where the attacks took place

$e^{16}_{n,3}(t)$ - predicted current terrorist activities

m = 2 – country

$$E_n(t) = \left\langle e_{n,1}(t), e_{n,2}(t), e_{n,3}(t) \right\rangle$$

if $e_{n,1}$(t)= 2 then $e_{n,3}(t) = \left\langle e^1_{n,3}(t), e^2_{n,3}(t), ,..., e^{15}_{n,3}(t) \right\rangle$

$e_{n,3}(t) = \left\langle e^1_{n,3}(t), e^2_{n,3}(t), ,..., e^8_{n,3}(t) \right\rangle$

$e^1_{n,3}(t)$ – general description (name, location, area, number of citizens...)

$e^2_{n,3}(t)$ – set of countries substantial from bilateral relations point of view:

$e^3_{n,3}(t)$ – political parameters,

$e^4_{n,3}(t)$ – social parameters

$e^5_{n,3}(t)$ – economic parameters

$e^6_{n,3}(t)$ – ecologic parameters

$e^7_{n,3}(t)$ – military parameters

$e^8_{n,3}(t)$ - objects of alliance externally used m = 3 – alliances

$$E_n(t) = \left\langle e_{n,1}(t), e_{n,2}(t), e_{n,3}(t) \right\rangle$$

if $e_{n,1}$(t)= 3 then $e_{n,3}(t) = \left\langle e^1_{n,3}(t), e^2_{n,3}(t),,..., e^8_{n,3}(t) \right\rangle$

$e^1_{n,3}(t)$ - set of members (countries) of alliance

$e^2_{n,3}(t)$ - main aim of alliance

$e^3_{n,3}(t)$ - global political parameters which characterizes the coalition

$e^4_{n,3}(t)$ - global social parameters which characterizes the coalition

$e^5_{n,3}(t)$ - global economic parameters which characterizes the coalition

$e^6_{n,3}(t)$ - global ecologic parameters which characterizes the coalition

$e^7_{n,3}(t)$ - global military parameters which characterizes the coalition

$e^8_{n,3}(t)$ - objects of alliance externally used

m = 4 – objects (business group, institution, organization)

$$E_n(t) = \left\langle e_{n,1}(t), e_{n,2}(t), e_{n,3}(t) \right\rangle$$

if $e_{n,1}$(t)= 4 then $e_{n,3}(t) = \left\langle e^1_{n,3}(t), e^2_{n,3}(t),,..., e^6_{n,3}(t) \right\rangle$

$e^1_{n,3}(t)$ - type of object

$e^2_{n,3}(t)$ - localization

$e^3_{n,3}(t)$ - (business group, institution, organization) owner country

$e^4_{n,3}(t)$ - sensitivity of the types of attacks

$e^5_{n,3}(t)$ - applied counter-terrorist system

$e^6_{n,3}(t)$ - (business group, institution, organization) owner country

Model of crisis

$$Cr_k(t) = \left\langle cr_{k,1}(t), cr_{k,2}(t), cr_{k,3}(t), cr_{k,4}(t) \right\rangle$$

$cr_{k,1}(t)$ - set of threatened entrants

$cr_{k,2}(t)$ - set of terrorist organizations

$cr_{k,3}(t)$ - set of secondary factors

$$cr_{k,3}(t) = \left\langle cr^1_{k,3}(t), cr^2_{k,3}(t) \right\rangle$$

$cr^1_{k,3}(t)$ - causative factors

$$cr^1_{k,3}(t) = \left\langle cr^{1,1}_{k,3}(t), cr^{1,2}_{k,3}(t), \ldots, cr^{1,J}_{k,3}(t) \right\rangle$$

$cr^{1,1}_{k,3}(t)$ - type of conflict source (religious, economic, political, ecological)

$cr_{k,3}^{1,2}(t)$ - intensity of the conflict

$cr_{k,3}^{1,3}(t)$ - duration of the conflict

$cr_{k,3}^{1,4}(t)$ - loses due to the conflict

$cr_{k,3}^{1,5}(t)$ - ratio of military potential for the conflict

$cr_{k,3}^{2}(t)$ - executive factors

$$cr_{k,3}^{2}(t) = \left\langle cr_{k,3}^{2,1}(t), cr_{k,3}^{2,2}(t), \ldots, cr_{k,3}^{2,J}(t) \right\rangle$$

$cr_{k,3}^{2,1}(t)$ - ability to execute specified type of terrorist attack

$cr_{k,3}^{2,2}(t)$ - level of possible support in the threatened country

$cr_{k,3}^{2,3}(t)$ - number of critical infrastructures which might be attacked

$cr_{k,3}^{2,4}(t)$ - terrain influence on planned attack effectiveness

$cr_{k,3}^{2,5}(t)$ - ratio between the professionalism of the terrorist group members and the effectiveness of applied counter-terrorist system

$cr_{k,4}(t)$ - vector of threat coefficients

$$cr_{k,4}(t) = \left\langle cr_{k,4}^{1}(t), cr_{k,4}^{2}(t), \ldots, cr_{k,4}^{R}(t) \right\rangle$$

$cr_{k,4}^{1}(t)$ - possibility of terrorist attack occurrence

$cr_{k,4}^{2}(t)$ - possibility of defined type of terrorist attack against defined object

$cr_{k,4}^{3}(t)$ - distribution of time to next terrorist attack occurrence

$cr_{k,4}^{3}(t)$ - distribution of losses caused by the terrorist attack

SECONDARY FACTOR AND THREAT COEFFICIENT EVALUATION

As a method for secondary factor calculation we propose to apply several known methods for pattern recognition. The idea of the tool is to generate the training data set based on the expert opinion and in the next step to use the data to calibrate given method of pattern recognition (See Fig. 10).

Their main aim is to, considering series of data (primary factor values) introduced to the system, produce the output value of aggregated factor (based on expert opinion). In other words we are seeking the tool that could produce the aggregated factor value from specified primary factors basing on expert decision used to calibrate the tool.

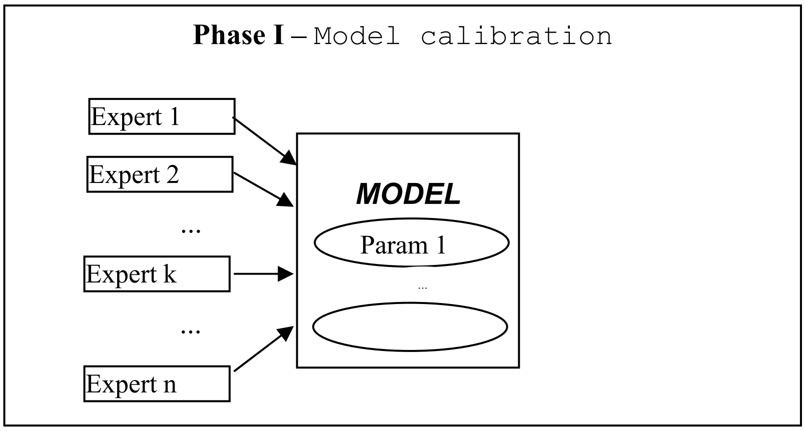

Fig. 10: Calibration of the pattern recognition method.

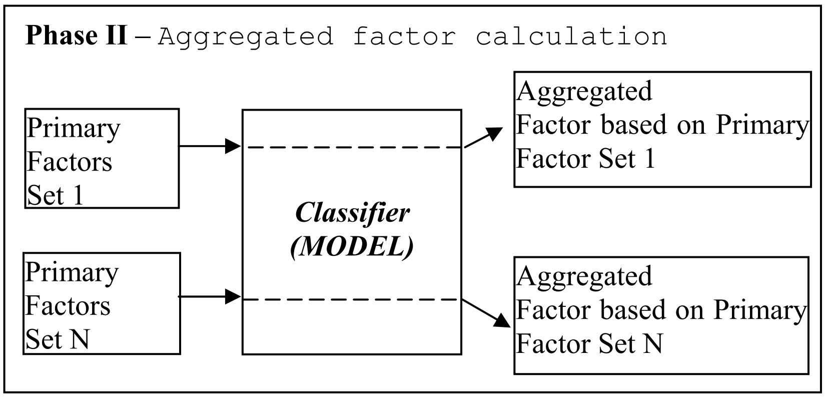
Phase II – Aggregated factor calculation
Primary Factors Set 1
Primary Factors Set N
Classifier (MODEL)
Aggregated Factor based on Primary Factor Set 1
Aggregated Factor based on Primary Factor Set N

Fig. 11: Calculation of second level factors.

There are several methods for classification tool, in this work we will introduce the concept based on:

- Neural networks,
- Decision trees,
- Regression Analysis.

The most popular form of neural network architecture is the multilayer perceptron. A multilayer perceptron characterizes as follows:

- has any number of inputs,
- has one or more hidden layers with any number of units,
- uses linear combination functions in the hidden and output layers,
- uses sigmoid activation functions in the hidden layers,
- has any number of outputs with any activation function,
- has connections between the input layer and the first hidden layer, between the hidden layers, and between the last hidden layer and the output layer.

The idea of adapting the neural network as a primary factors classification tool is as follows:

1. Introduce the set of primary factors used to calculate the aggregated factor;
2. Build the structure of the network considering:
   - number of input parameters (number of neurons in the input layer);
   - maximum value of every primary factor (number of inputs of the individual neuron in the first layer);
   - maximum value of aggregated factor – number of outputs in the output layer;
   - number of neurons in hidden layer is a result of combining the input layer neurons and output layer neuron/neurons;
3. Prepare the data for training process – we are gathering the expert opinion on different set of primitive factor values and the resulted aggregated factor value;
4. Train the neural network (change value of the neuron's weights) using prepared training data sets (calibration of the model);
5. Verify the correctness of the training process (using different sets of primitive factor values we calculate the resulted aggregated factor value).

Decision trees

An empirical tree represents a segmentation of the data that is created by applying a series of simple rules. Each rule assigns an observation to a segment based on the value of one input. One rule is applied after another, resulting in a hierarchy of segments within segments. The hierarchy is called a tree, and each segment is called a node. The original segment contains the entire data set and is called the root node of the tree. A node with all its successors forms a branch of the node that created it. The final nodes are called leaves. For each leaf, a decision is made and applied to all observations in the leaf. The type of decision depends on the context.

The problem of choice the method of evaluation of secondary factors and threat coefficient is open. In this case it strictly depends on real data value of primary factors, definition of secondary factors and threat coefficient and level of possible expert knowledge of security analysts.

Gathering of historical values of primary factors, secondary factors, threat coefficients enables time series and econometric models identification and then use them to prediction above variables or functions. Having such model we are able to simulate trajectories of threat processes and statistically estimate future values of the threat factors and coefficients.

CONCEPT OF SIMULATION ENVIRONMENT FOR EWS

Real terrorist organizations, their activities, relations and interests are very complex, that's why no single, monolithic simulation model can satisfy the needs of future EWS users. It is better to represent such complex system as a distributed simulation environment. There is a lot of specialized and verified simulators, that have been developed during the last 20 years. Some legacy simulators properly describe represented domain but another are already not adequate and frequently obsolete. They use different data structures, algorithms and interfaces. A good solution is to modernize software in order to increase simulation interoperability, software portability and user interface quality or to build new simulators. In that situation we propose an approach based upon the High Level Architecture idea.

Interactive distributed simulators for a modelling, identification, prediction and analysis of terrorist activities can be realized and executed in many various ways. Current state of information technology enables a construction of software environment with well known and useful methodologies, tools and software. The best known standards in the simulation domain are: High Level Architecture (HLA) and Federation Development and Execution Process (FEDEP). High Level Architecture is a standard framework that supports simulation (called federation) composed of different simulation components (called federates). HLA was developed in order to meet the needs of reusability and interoperability in virtual, constructive and live simulations. HLA consists of three components: Federation Rules, Interface Specification and Object Model Template (for documenting the Federation Object Model – FOM, the Federate Object Model – SOM and the Management Object Model – MOM). A process for building and integrating HLA federation is described by FEDEP that describes a high – level framework for the development and execution of HLA federations. The use of FEDEP assures us that a final computer environment's software will be HLA compliant. The only way to send or obtain data in a federation is to use a common Federation Object Model and supporting Runtime Infrastructure. FOM is an identification of the essential classes of objects, object attributes, and object interactions that are supported by a federation.

The distributed simulation environment we proposed will be composed of specialized simulators, databases, expert systems and statistical packages. An important step is to define an initial prototype FOM as a starting point for establishing the type of data and interactions to be shared through the Run-time Infrastructure (RTI) during a federation execution. This FOM should contain (1) a set of objects representing a real system state, factors and threat indicators and (2) interactions for defining events and messages. In developing the initial prototype FOM we have to gather and synthesize the results of object-oriented modelling (see UML diagrams) and map this information into a minimal FOM representation. Having HLA Federation it is possible to extend a simulation environment depending on new requirements or models.

CONCLUSIONS

The study is in the modelling phase. In the paper we present the threat model and the idea of methods for evaluation of security state. Pattern recognition methods are described in order to gain a useful tool to calculate the threat factors. Direction of future research will be focused on extending and completing the requirements for EWS, verification of methods for pattern recognition, simulation tool, predictive analysis on the basis of obtained real data from security services resources.

BIBLIOGRAPHY

[1] A. Najgebauer – "The Interactive Simulation Method of Decision Support in Combat Actions". Conference Proceedings of European Simulation Multiconference 97, Istanbul, Turkey, pp. 755-758, SCS Publication ISBN 1-56555-115-X.

[2] A. Najgebauer – "Combat Decision Support System". Proceedings of 1st World Congress on Systems Simulation, September 1-3, 1997, Singapore, pp. 204-208, SCS-ISBN 1-56555-114-1.

[3] A. Najgebauer – "Decision Support Systems for Conflict Situations. Models, Methods and the Interactive Simulation Environments" (in Polish, the habilitation theses). Ed. Biuletyn WAT. Warsaw 1999, Poland. (294 p.). ISBN 83-908620-6-9.

[4] Najgebauer, D. Pierzchała, J. Rulka – "The Simulation Researches of Decision Processes in a Conflict Situation with Opposite Objectives". Conference Proceedings of 13th European Simulation Multiconference ESM99, Warsaw, Poland, June 1-4, 1999.

[5] NATO /EAPC/PFP - "Generic Early Warning Handbook", 2001.

[6] Roger Smith – "Counter Terrorism Simulation: A New Breed of Federation", SIW, 2002.

[7] Ripley B. D. – "Pattern Recognition and Neural Networks", Cambridge University Press, Cambridge 1997.