Monitoring of Terrorist's Treats: a Theoretical Approach

*Vasily POPOVICH, Alexander PROKAEV, Manfred SCHRENK, Filipp GALIANO,
Mareng VORONIN, Angelina SMIRNOVA*

1 ABSTRACT

The paper considers a problem of terrorists' threat control from theoretical point of view. Handling a problem of effective monitoring systems development is suggested from a point of view of monitoring suspicious persons – a key factor of this problem. Meanwhile, the main idea is that persons don't act alone but as members of certain terrorists groups.

In order to develop theoretical fundamentals, basic concepts were defined and subject area was formalized. Mathematic methods for supporting a wide spectrum of decision-making are proposed and briefly considered: from identification of individuals being linked to terrorists group, till terrorists situations' analysis, assessment and control.

2 INTRODUCTION

The project is focused upon the theory, principles and methods of constructing and operating monitoring systems that function at various levels and scales as elements of global, national and international systems for monitoring hazardous materials emplacements.

The core of proposed research is investigating the human aspect of organizations or Terrorists Groups (TG) that can potentially be organizers of executors for the assembly, transportation, emplacement and use of hazardous materials (Explosives, parts of Weapon of Mass Destruction etc.).

The main subjects of the proposed research are the ontology of TG emergence and development, to identify individuals linked to hazardous materials (HM) as members of a TG, and the development of distributed real time intelligent monitoring systems for the detection of TGs.

3 RESEARCH METHODS

1. Formal description of TGs and TG ontology development.
2. Development of mathematical techniques to assess terrorists' situations awareness (TSA).
3. Global monitoring of links or associations between potential terrorists or individuals with special Profiles and/or Tracks within, near or outside a risk zone.
4. Solving direct and inverse problems of TG analysis:
   - defining a potential TG based on terrorists' "profiles" and/or "routes" and association analysis;
   - defining a certain "profile" and/or "route" that is relevant to one or several TG.
5. Developing intelligent TG detection methods.

4 RESEARCH MATHEMATIC STATEMENT

A single individual can hardly arrange for HM development, transportation and implementation. This process is organized by a group of people, with specific skill sets integrated by some organizational structure and personal interrelations.

A formal description of a TG is developed in the first part of the project, which will give formal descriptions for a "profile" and the "track" of a terrorist identified as the HM related individual. For this type of research, an Immunocomputing and Bayesian approach will be used. Analysis of the TG problem indicates that unlike a simple input parameters' vector, some vectors will be parameters, including terrorists' "profiles" and "tracks". In the case study, this problem will make the mathematical solution much complicated. It is evident that Immunocomputing techniques coupled with a Bayesian approach can be extended and adapted to solve these complex discrimination problems.

Solving the problem of ontology development as a mega ontology, based on the results received in the project to identify the "profile" and "track" ontology, is of principal importance.

In the context of present paper ontology is understood as a formal description of concepts (classes) being related to subject area, of slots (that is to say, characteristics describing different features and attributes of each concept) and facets (restrictions on slot values)

Ontology development includes two stages as follows:

1. Forming a list of subject area basic concepts and their definition. For terrorists' threats monitoring such concepts are:
    1. Monitoring object.
    2. Monitoring subject.
    3. Monitoring system.
    4. Information source.
    5. Environment.
    6. Terrorists' situation (TS).
2. Defining interrelations between basic concepts and their characteristics specification; forming system of classes.

Another critical mathematical problem is detecting the links and relations between potential terrorists and suspicious persons, as well as incorporating other suspects, who were not initially identified as potentially dangerous. Due to its high dimensionality, the given problem can hardly be subjected to a global solution beyond a limited defined context such as a certain risk zone or object. Theoretically speaking such a global solution would have required an almost complete analysis (profiling) of the World's population that is neither technologically nor objectively possible yet.

Practically, analysis of information sources is of great importance to solving the given problem. All information arriving from sources can be conditionally divided into two types: statistic and operational ones.

Statistical information is commonly offered by civil services as well as by organizations related to antiterrorist activities. It serves to initial characteristics forming (standard TP and TS) of an individual being involved in terrorist activities and to TS' class defining. Statistic information is a result of realized terrorist acts analysis.

Operational information is dynamically changeable data arriving from primary and secondary sources when system monitoring terrorist's threats (SMTT) is operating. Main sources of dynamically changeable information are: cellular communication systems, Internet (attended sites, e-mail intensity and addressees and others), registration data from information services in hotels, airports, railway stations, intensity and purposes of credit cards using etc.)

Operational information differs from statistic one by the fact that data constituent operational information is generated in dynamics of SMTT operating and relates to a concrete monitoring object.

The problem of TG analysis can be reduced to direct and inverse problems: i) defining potential TGs based on terrorists' "profiles" and/or "routes" ensembles' analysis; and ii) defining a certain "profile" and/or "route" relevant to one or several TGs.

Theoretical solution of the given problems can be achieved by using recognition theory and cluster analysis, using Immunocomputing techniques and Bayesian approach as the core methods. The combination of the above proposed methods demonstrates significant advantages over methods using genetic algorithms and algorithms based on neural nets.

The development of TG detection is the most important part of the project. The method incorporates the development of the three most important constituent techniques as follows: 1) potential TG detection and tracking, 2) TG detection as a result of HM detection, 3) TG detection arising from HM use.

Potential TG detection and tracking is based on the learning and self-training capacities of Immunicomputing. The problem can also be solved by engaging experts using Immunocomputing or similar recognition system. Hypothetical threats and related TGs can be generated based on previous experience.

Because of a great number of characteristics being taken into account and variety of their types, information integration of separate characteristics values and their significance for building aggregate characteristic (such as TS' class or terrorists' activity index) becomes a nontrivial problem. In order to get such an aggregate evaluation the following parameters should be defined [1]:

1. Relevant features.
2. Scales for representing selected features.
3. Grouping method for selected features.
4. Significance (importance) of selected features.

Aggregate Indices Method (AIM) can be used for solving the above mentioned problems. AIM allows to assess not only terrorists but also monitoring objects.

- For the present instance two basic situations are possible:
- Learning sample is sufficient. Immunocomputing is used for accurate recognition, and monitoring system is learned on the basis of learning sample.
- Learning sample size is insufficient for accurate recognition. In this case AIM is applied, and system learning is based on expert opinion.

The above two methods can be used simultaneously for mutual checking and improving terrorists' threat recognition reliability.

TG detection as a result of HM detection can be achieved by analyzing a set of potential or known TGs as well as assessing the possibility of a new TG appearing. This is achieved by defining the potential "profiles" and "tracks" involved in HM detection.

TG detection following the use of an HM in the second case differs in the precise localization of the HM incident and correspondingly, in a sharp decrease in the number of TGs that could possibly be involved. In those circumstances, the requirement to respond quickly is critical, and the algorithm requires a real time realization.

To prove the above theoretical concepts, a computer prototype will be developed to demonstrate the operational integrity of the proposed approach, while using information on terrorist activity and occurrences of HM use.

5 CONCLUSION

Thus, monitoring of terrorist's threats requires solving of multifaceted problems that can be usually divided into two groups:

1. Subject area formalization, determining structure of incoming information and heterogeneous information fusion. This group of problems is solved by developing ontology and mathematical formulation of basic concepts.
2. Developing mathematical methods for integral characterization of information arriving from monitoring object, for both cases of sufficient and insufficient size of a learning sample (in our case – Immunocomputing and AIM respectively).

Moreover, as far as a great part of incoming or resulting information has geospatial gridding, appropriate operating of similar system requires involving of state-of-the-art intellectual GIS technologies.

6 REFERENCES

V.V. Popovich, A.V. Pankin, M.N. Voronin, L.A. Sokolova. Intelligent Situation Awareness on a GIS Basis. //Proceedings of MILCOM 06, October 24-26, Washington, USA.

Popovich, V.; Prokaev, A.; Sorokin, R.; Doldo, M. Intelligent Situation Awareness.//Proceedings of MilTech2, October 25-26, 2005, Stockholm.

Popovich, V. , Voronin, M. Data Harmonization, Integration and Fusion: three sources and three major components of Geoinformation Technologies.//Proceedings of IF&GIS, September 25-27, 2005, St. Petersburg.

Tarakanov, A.O., Skormin, V.A., Sokolova, S.P. Immunocomputing: Principles and Applications. Springer, New York, 2003.

Н.В. Хованов. ОЦЕНКА СЛОЖНЫХ ЭКОНОМИЧЕСКИХ ОБЪЕКТОВ И ПРОЦЕССОВ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ. К 95-летию метода сводных показателей А.Н. Крылова . Вестник СПбГУ. Сер. 5. 2005. Вып. 1.