# Problem 6. Cyber Intelligence Decision Support in the Era of Big Data

STEMO Ltd., `http://www.stemo.bg/`

Georgi Dukov, `Georgi_Dukov@stemo.bg`

**Company's overview.** In 2016 STEMO Ltd. is going to celebrate 25 years anniversary with confirmed leading role in the field of information technologies. The company is providing a broad portfolio of IT products, solutions and services to our customers for building and enhancing the efficiency, productivity, security and reliability of their IT infrastructure.

Our versatile professional experience and expertise allow successful implementation of complex projects covering the complete life-cycle of each information system: **consultations, research, analysis, design, planning, implementation, training, operation, optimization, maintenance and upgrade.**

The company has 15 own commercial offices, service and retail centers, warehouses, a training center, equipped with modern information, technological and transport facilities. The branches of the company are situated in the largest cities of Bulgaria.

We employ 260 highly-qualified specialists: sales and technical consultants, service engineers, designers, programmers, economists, etc. with over 600 technical and sales certificates which cover the certification programs of leading world manufacturers.

Our main activities are encompassing almost all services, products and solutions in the field of information technologies, including:
- design, building and maintenance of complex information and communication systems
- delivery and installation of computer and office equipment, software and consumables
- specialized, professional IT services
- warranty and post-warranty support of computer equipment
- software development
- training and certification services

The quality management system of the company was implemented in 2000. It is certified in compliance with the requirements of international standards ISO 9001:2008 and AQAP 2110 NATO standards and covers all branches and activities of the company. The system ensures a high level of customer satisfaction, contributing to the stable development of the company and the fulfillment of corporate objectives. In 2010 the company certified the IT service and information security management according to ISO 20000 and ISO 27000 standards. In 2012 acquired certificates for environmental management ISO 14001 and health and safety management ISO 18001.

The company is a certified direct partner of leading world manufacturers: HP, Microsoft, Cisco Systems, SAP, Oracle, Fujitsu, DELL, Canon, Toshiba, Xerox, Epson, NetApp, VMware, Citrix, D-Link, EATON, APC, Samsung, LG, BenQ, 3M, ESET, Novell, Autodesk, AMP, R&M, Kerpen, Panduit, ITNI, OSPL, Crypto, Systematic, Imanami, Lieberman Softwar, NetSurity, Rola Security Solutions and others.

Our services help customers to achieve maximum return of investments in IT, enhancing the efficiency, productivity, security and reliability of their IT infrastructure. Our customers save time and resources and are able to concentrate on their main activity and priorities.

Over the years, the company financial results have shown a solid development and strengthened our role as an undisputed business leader in the IT market.

The biggest corporate organizations in Bulgaria, state and local administrations, industry and energy enterprises, telecommunication companies, banks, schools and medical centers, NGOs, thousands of SMEs and individuals are among our customers. We stand their success for our own priority.

Every year more than 10 000 organizations and individuals rely on our company as a correct, dedicated and reliable partner.

**Problem description.** Modern technologies in the digital society are constantly enlarging the cyber space scale, services and capabilities. This opens the necessity for proper understanding the behavior of todays' Internet users for assuring a more secure and predictable world. Understanding these evidently requires big data processing and relevant generalization for adequate decision support. STEMO Ltd. is a leading national security systems integrator working in this field since 2009 with multiple successful business partnerships.

Following our practical experience, one of the key problems in the field is to produce a useful aggregation and trends forecasting, in a suitable middleware, concerning the enormous direct and indirect Internet objects relations.

As these generate a number of hybrid threats for the users, critical infrastructure, e-services, AI evolution, M2M autonomous interaction and human-in-the-loop dynamic role, the resulting preventive measures, are quite demanding by means of computational resources and multiple decision makers adequate support.

Being rather comprehensive, the problem requires experts' data combination with big data statistical observations for practical achieving adequate cyber intelligence and countering cybercrimes and terrorist events.

**Five key steps for solving the problem could be implemented:**

1. Defining multiple cyber risks dynamic database.

2. Formulation of aggregation models, concerning data extraction and visualization.

3. Formulation of discrete optimization problems, taking into account the particular forecasting period, regarding expected critical events.

4. Choosing a software environment for solving the formulated problems.

5. Numerical experiments and discussion of results.