



UNIVERSITY OF NATIONAL AND WORLD ECONOMY
Department “National and Regional Security”

Business and Science for Security and Defence Industrial R&D

The International Conference was organised
under the patronage of
Prof. Dr. Borislav Borisov,
Rector of the University of National and World Economy, Sofia

14-15 May 2009, Sofia

AVANGARD PRIMA
Sofia, 2009



The International Conference “Business and Science for Security and Defence Industrial R&D” was held on 14-15th May 2009 in Sofia under the patronage of Prof. Dr. Borislav Borisov, Rector of the University of National and World Economy. It is the sixth international conference organized in the framework of the project SfP-982063 “Management of Security Related R&D in Support of Defence Industrial Transformation”, funded by NATO Science for Peace and Security Programme. The conference was organised by Department “National and Regional Security” at University of National and World Economy (UNWE), Sofia in cooperation with Institute for Techniques of Intelligent Systems, Federal Armed Forces University, Munich, Germany, Bulgarian Academy of Sciences – Institute for Parallel Processing, The National Defence College, Bucharest, Romania and European University, Skopje, Macedonia. During the conference Centre of Excellence at UNWE was established under the framework of project. The organisers would like to thank for the support of Bulgarian Ministry of Defence and Bulgarian Defence Industrial Association.

BUSINESS AND SCIENCE FOR SECURITY AND DEFENCE INDUSTRIAL R&D

Tilcho Ivanov and contributors

**Editors: Prof. Tilcho Ivanov, PhD
Assoc. Prof. Dimitar Dimitrov, PhD
Assist. Prof. Konstantin Poudin, PhD**

**AVANGARD PRIMA
ISBN 978-954-323-579-7**

Sofia, 2009

TABLE OF CONTENTS

FOREWORD	7
GREETINGS TO THE CONFERENCE.....	9
STRATEGIC BUSINESS ALLIANCES AND BULGARIAN DEFENCE INDUSTRY	17
Prof. Tilcho Ivanov, PhD Partner country Project Director Department “National and World Security” University of National and World Economy, Sofia	
CURRENT ECONOMIC CRISES AND CHALLENGES FOR DEFENCE BUDGETS	29
Prof. Zoran Ivanovski, PhD Rector of the European University, Skopje Assist. Elena Stoichkova, BSc Assistant at Faculty of Economics, European University	
SECURITY AND DEFENCE R&D POLICY FRAMEWORK - OPTIONS AND ALTERNATIVES FOR BULGARIA	41
Assoc. Prof. Dimitar Dimitrov, PhD Head of Department “National and Regional Security”, University of National and World Economy, Sofia	
R&D NATIONAL POLICY IN THE REPUBLIC OF MACEDONIA ACCORDING TO THE SECURITY RELATED AND GENERALLY R&D SCENE – CURRENT STATUS AND SHORTFALLS	51
Major Elenior Nikolov, MSc Military academy “General Mihailo Apostolski” - Skopje Mr. Mitko Bogdanoski, MSc Macedonian Army, Land Forces Captain Robertino Chontev, MSc Ministry of Defence, Department of planning and bilateral cooperation Assist. Elena Stoichkova, BSc European University, Skopje Prof. Zoran Ivanovski, PhD Rector of the European University, Skopje	

ROLE OF THE CENTRE OF OPERATIONAL ANALYSIS IN INTEGRATION OF SCIENCE..... 76

Dr. Velizar Shalamanov

Senior Research Fellow

Institute for Parallel Processing – Bulgarian Academy of Sciences 76

Dr. Georgi Penchev

Senior Assistant Professor

Department “National and Regional Security”

University of National and World Economy - Sofia 76

Mrs. Irena Nikolova

Research Fellow

Space Research Institute – Bulgarian Academy of Sciences

COMPETENCES AND COMPETITIVE ADVANTAGES OF A DEFENCE INDUSTRIAL ENTERPRISE 96

Assoc. Prof. Tsvetan Tsvetkov, PhD

Department “National and Regional security”

University of National and World Economy, Sofia, Bulgaria

CORPORATE LEADERSHIP IN TIME OF CRISIS..... 106

Professor Stefan Hristov, PhD

Department “National and Regional Security”

University of National and World Economy, Sofia, Bulgaria

CONCEPTUAL MODELING IN THE DEFENSE ACQUISITION PROCESS. 117

Captain Marius MĂRMUREANU, Eng, MSc, PhD Candidate

Armaments Test&Evaluation and Scientific Research Center

Military Equipment and Technologies Research Agency

Ministry of National Defense, Romania

FIFTH GENERATION WARFARE – A POSSIBILITY FOR THE FUTURE.... 126

Captain Liviu MATACHE, Eng, MSc, PhD Candidate

Armaments Test&Evaluation and Scientific Research Center

Military Equipment and Technologies Research Agency

Ministry of National Defense, Romania

PLANNING, PROGRAMING, BUGETARY SYSTEM – AN EFFICIENT, MODERN AND..... 137

Lt. Col. Doina Mureșan, PhD

Associate Professor, Deputy Director

National Defence College Bucharest, Romania

SOCIAL SECURITY IN THE CONTEXT OF EUROPEAN SECURITY STRATEGY (CHALLENGES AND RESPONSIBILITIES OF BUSINESS).....	152
Assoc. Prof. Stefka Dacheva, PhD Department of Information Technologies and Communications, University of National and World Economy	
DEFENCE R&D POTENTIAL IN BULGARIA AFTER 1989	165
Assist. Prof. Konstantin Poudin, PhD Department “National and Regional Security” University of National and World Security	
ABOUT SOME PROBLEMS AND OPPORTUNITIES TO INNOVATIONS	176
Lt. Col. Nikolay Atanasov, PhD BGR AF HQ, A3 Department “National and Regional Security”, University of National and World Economy, Sofia	
USER INTERFACE FEATURES OF THE MOBILE WEB ACCESS.....	185
Assoc. Prof. Alexandar Kolev, PhD “G.S.Rakovski” National Defence Academy, Sofia	
SOME METHODS FOR RISK ASSESSMENT OF CRITICAL INFRASTRUCTURE ELEMENTS	191
Assoc. Prof. Plamena Zlateva, PhD Institute of Control and System Research – BAS	
CLOUD COMPUTING SECURITY RISKS AND BEST PRACTICES	197
Assoc. Prof. Dimiter Velev, PhD Department of Information Technologies and Communications, University of National and World Economy	
СЪОТНАСЯНЕ НА НАУКА, ТЕОРИЯ И ЗНАНИЕ В КОНТЕКСТА НА СИГУРНОСТТА	205
проф. д.ик.н. Димитър Й. Димитров Президент на Българската асоциация на конфликтолозите	
MAJOR PROBLEMS IN THE DATABASE SECURITY	213
Dr. Violeta Bogdanova, PhD Senior Researcher Institute for Parallel Processing, Bulgarian Academy of Sciences	

RESEARCHING OF THE INDIVIDUAL MANAGERIAL DECISIONS MAKING IN THE CONFLICT CRISES SITUATIONS IN SUPPORT OF SECURITY AND DEFENCE R&D MANAGEMENT	217
Mr. Ivan Tsanov, PhD Bulgarian Association of the conflictologists	
RISK MANAGEMENT IN DEFENCE ACQUISITION – BEST PRACTICES ..	219
Mr. Yuri Tsenkov, PhD Student Department “National and Regional Security” University of National and World Economy	
R&D AND CRITICAL INFRASTRUCTURE PROTECTION (CANADA’S EXPERIENCE)	229
Ms. Teodora Gechkova, PhD Student Department “National and Regional Security” University of National and World Economy	
INFORMATION SECURITY POLICIES IN R&D PROCESS	242
Mr. Nedko Tagarev, PhD Student Department “National and Regional Security” University of National and World Economy	
AN APPROACH FOR CLASSIFIED INFORMATION LOCAL AREA NETWORK	251
Mrs. Darinka Nickolova, Mrs. Maya Bojilova “G.S.Rakovski” National Defence Academy Defence Advanced Research Institute (DARI)	
HIGH-TECH OUTSOURCING SERVICES IN BULGARIA: SURVEY RESULTS.....	259
Assoc. Prof. Matilda Alexandrova, PhD Chief Assist. Prof. Svetla Boneva, PhD	
A CRITICAL REALIST APPROACH TO SECURITY AND DEFENSE R&D POLICY IN BULGARIA	275
Mr. Nikolay Pavlov Centre for National Security and Defense Research - Bulgarian Academy of Sciences	
PRESENTATION OF GAMA PROEKT 99 LTD.....	280
Mr. Hristo Georgiev Mr. Dobromir Georgiev	





FOREWORD

This paper is a collection of reports, presented to the 6th International Conference “Business and science for defence industrial R&D” held in Sofia at University of National and World Economy on 14-15 May 2009. The conference was organised under the patronage of the Rector of University of National and World Economy Prof. Dr. Borislav Borisov. The international event is one of the activities within the framework of NATO funded three-year project “Management of Security Related R&D in Support of Defence industrial Transformation (NATO Science for Peace and Security Programme SfP – 982063). The conference is the final academic event of the project, where final results and conclusions were presented. Young researchers, academics, students, defence producers, representatives of state administration and NGOs from 4 countries and almost 15 different institutions, Universities and research centres had the opportunity to present and to discuss their findings during the research project. According to the project objectives, the main research results were directed to the national management models and R&D policies of the countries, presented in the project. The participants agreed that the basic elements of NATO compatible R&D policy and models exist in project countries, but this is not enough. There is a need of national coordination of the efforts in defence and defence industrial R&D, improvements of the financing of R&D, real steps for EU and NATO defence industrial cooperation, with the active support and involvement of the state institutions. Efforts should be sustainable and comprehensive, expressed in policies and procedures.

The conference was organised by Department “National and Regional Security” at University of National and World Economy (UNWE), Sofia in cooperation with Institute for Techniques of Intelli-

gent Systems, Federal Armed Forces University, Munich, Germany, Bulgarian Academy of Sciences – Institute for Parallel Processing, The National Defence College, Bucharest, Romania and European University, Skopje, Macedonia. During the conference Centre of Excellence at UNWE was established under the framework of project. The organisers would like to thank for the support of Bulgarian Ministry of Defence and Bulgarian Defence Industrial Association.

GREETINGS TO THE CONFERENCE

Dear Ladies and Gentlemen,

Dear guests,

Dear colleagues,

It is my pleasure to open this respectable international conference. As you know, as a Rector of University of National and World Economy I agreed to be a patron of this conference, thus to underline the importance and significance of the scientific efforts of this research project. I follow the results and the activities of the project and actively support our University Department “National and Regional Security” in their research and administrative work. This support is not occasional. I consider the project and the expected research results as important challenge for our colleagues and for our University. The fact that NATO through its Programme “Science for Peace and Security” funded this project is a real proof that our University as leading Bulgarian university, with cooperation with our respected partners from Bulgarian Academy of Sciences, Germany, Romania and Macedonia, are able to elaborate, coordinate and execute such kind of international projects. And as I see, today's conference is a response to these high expectations. Here in the conference room I see many well known faces of our University colleagues, of our partners from Bulgaria and abroad and this is another merit of the conference and the department “National and Regional Security” - to bring all of these people, all of these professionals together and to have the opportunity to discuss important problems of security and defence. You know that I am not far away of these problems and I am able to evaluate properly the project and the main idea behind this project. Very often in our country we lack of strategic thinking and I see this project as facilitator of this type of thinking. And I am glad to see how our col-

leagues, especially our young colleagues and students from University, from our Department “National and Regional Security” build step-by-step this abilities for strategic thinking, for strategic management, which is implicit characteristics of such organizations as NATO and EU.

I wish you fruitful discussions and research work here in our University. Especially I would like to thank to Dr. Buch and our guests from Germany, Romania and Macedonia and to assure them that co-operation will continue in the future.

Thank you for your attention.

Prof. Dr. Borislav Borisov

Rector of the University of National and World Economy, Sofia

Advisor on Education, Science and Economic Development

to the President of the Republic of Bulgaria Mr. Georgi Parvanov

*Mr. Rector,
Dear Guests,
Dear Colleagues,
Dear Ladies and Gentlemen,*

It is great pleasure for me to be here and to have all of you at this international conference “Business and science for defence industrial R&D”. The conference is under the patronage of our Rector of University of National and World Economy Prof. Dr. Borislav Borisov. The event is part of NATO funded three-year project “Management of Security Related R&D in Support of Defence industrial Transformation (NATO Science for Peace and Security Programme SfP – 982063).

We are almost at the end of the project but I do not like to make full summary of activities and results. Looking from broader perspective, we have to mention several important developments, outside of the pure scientific results. I will start with the students, because the involvement of young scientists, researchers and students is one of the main aims of our project, another proof of strategic thinking, mentioned by Prof. Borisov. Students, who took part in the project, already became Bachelors, Masters or PhD Students. Former PhD students became Doctors – at this moment we have at least 5 defended PhD theses only from Bulgaria. Some of our colleagues, involved in the project, became Assistant Professors, Associated Professors or full Professors. From our project participants we have appointed adviser to the Bulgarian Minister of Defence, country project director from Romania Mr. Fota became presidential advisor on national security, Dr. Shalamanov is going to have high level position in NATO structures and so on and so on. I agree that all of these achievements are not direct results only because of their participation in the project, but at least it shows that we found and use the right people for our objectives and NATO funded project helped to all of us to develop further.

At the end I would like to thank to my colleagues form the Organisational committee and to our students for their support and effective

involvement. Special thanks to Prof. Dr. Borisov for his continuous support and opportunities to use these wonderful conference facilities of UNWE.

I wish you successful work during the conference

Thank you for your attention.

Assoc. Prof. Dimitar Dimitrov, PhD

Head of Department “National and Regional Security”,
University of National and World Economy, Sofia

*Mr. Chairman,
Dear Prof. Borisov,
Dear Guest and Participants,*

I would like to welcome the participants in the international conference “BUSINESS AND SCIENCE FOR SECURITY AND DEFENCE INDUSTRIAL R&D”.

Research and Development are probably the most important factor for the development of the Armed Forces and the security system in national and international aspect. That is why the R&D policy is one of the most important policies for development of national security.

In that respect the Ministry of Defence is probably the bigger end user of this policy and for that reason it is highly interested in development of adequate economic and educational system. Something more, for the development of Armed Forces and system of national security, adequate to the current threats and challenges, it is necessary to implement not only new technologies, but to develop human resources, to prepare new generation of cadres, which have to be included in the system of defence and to work for the solution of their new challenging problems.

Cooperation between the state institutions and especially the educational institutions and the universities, from one side, and from the other side the business is very important not only for the development of the national economy, but also for the development of the national security in the presence of the globalisation of the threats and participation in the system of collective security and defence.

I wish success to the participants in the conference

Greeting Address on behalf of

Dr. Nickolay Tsonev

Minister of Defence of Republic of Bulgaria,
presented by his adviser Mr. Kalin Tomov.

Dear Prof. Borisov,
Dear Friends,
Dear Colleagues,

First of all I would like to thank you to the Rector of University of National and World Economy Prof. Borisov for the warm welcome and the good words about our project. As a NATO country Project director it is my pleasure to meet you at our conference and to wish you successful work. I have to admit that we all together have passed a long way, starting with the preparation of the project even in 2005 and going through all of our joint activities. The most important achievement of our project is our team spirit, our common attitude to the research problems and the friendly atmosphere between us, wherever we are – in Sofia, Skopje or in Bucharest. And I think that it is contributed in big degree to our research results - R&D model, case studies on policies, functional database and website of the project. Today we are going to open our project Centre of Excellence – one of the final elements of our activities, but the element which will be able to sustain current efforts in the future. We have tested several times our videoconferencing facilities, computer rooms and other equipment, which will permit to us and to our colleagues from UNWE to use these facilities long time in the future.

At the end of my opening speech I have to mention the involvement of young people in the project, the next research generation, fact which is highly evaluated in NATO Programme “Science for Peace and Security”. This is invaluable investment in our future.

Thank you again, Mr. Rector, for the wonderful conditions for work of our conference and I wish you again success.

Dr. Heinrich Buch

NATO country Project Director, ITIS,
Universitaet der Bundeswehr, Muenchen

*Prof. Borisov,
Mr. Chairman,
Dear Ladies and Gentlemen,*

Thank you for the participation in our conference, which is number sixth of project international conferences and seminars. As Dr.Buch already stated, we did a lot of work for these almost 4 years, starting with the preparation of our project plan (short and long version), customization and execution. We passed through long learning process, which gave us additional qualifications and confidence, that we also are NATO compatible (if I use the expressions from our project). These new abilities, combined with partners' efforts, lead us (in my opinion) to the successful end of our project. Most of our objectives are almost fulfilled and we are close to the quantitative dimensions of project's criteria for success. But I would like to concentrate your attention to the immediate steps, which are ahead. As you know, today we will open our project's Centre of Excellence, and having this facility, very soon after that follows first training of young researchers, key personnel and end-users, using videoconferencing methods, which is very new for us. We are almost ready with the final design of project database, although the database is already functional. We spent lot of efforts to keep our project website working and we will continue to do this in the future, thus providing more conditions for creation of network of researchers on defence industrial R&D. In this task we rely very much on our partners from defence industry, Ministry of Defence and related research organisations. In short – we did a lot but the project is not yet finished. We have to keep the momentum in order to fulfil all our tasks and aims, which will be reported at the end of the project this autumn on special event in Sofia.

I wish you fruitful work and enjoy your stay in Bulgaria.

Prof. Dr. Tilcho Ivanov

Partner country Project Director,

Department “National and Regional Security”,

University of National and World Economy, Sofia

STRATEGIC BUSINESS ALLIANCES AND BULGARIAN DEFENCE INDUSTRY

Prof. Tilcho Ivanov, PhD

Partner country Project Director

Department “National and World Security”

University of National and World Economy, Sofia

Introduction

It is obvious that politically, business and military alliances influenced to the participating countries policies in a different manner. It is important to see how these alliances defer between themselves. It could help to clarify the answer - what are the key factors for their interaction especially in respect to the defence technological and industrial base of the allied countries? The experience and some publication on the topic will help to found some levers, which could help for rational changes in this sensitive sector of economy. For to make the result of this task more easy, we will focus our attention to the R&D and R&T policies for to clarify what is their current status, and how do they could help a single country, like Bulgaria, to overcome the existing problems in carrying out its ally military missions, supported by its defence production capability.

1. Increasing economic relations among military allies and local problems

It is clear that states create military alliances when they do not possess sufficient power to maintain their national security on their own¹. It is a common appropriate that their output – deterrence is a pure public good, which races the number of issues. Defence burden sharing between the countries, free-riding as an unequal sharing, the

¹ Sandler, T., T., K. Hartley, *The Economics of Defence*, Cambridge University Press, 1995.

limits of the alliance size, and others are the key topics. The important issue for the small and transitional countries is the question of their defence technological and industrial bases. There are two controversial approaches that the countries could follow. First and easier one is to close their specialized defence companies relying on the import from their allies. Converting the defence industry to the competitive civil business countries could save and reallocate their limited resources for more effective civil use. This approach is supported by Prof. Keith Hartley, from the University of York, United Kingdom, which asserted that “if nations do not have a defence industrial base in a particular sector, they should not start one”. This conclusion is rationally based on the admission that is far less expensive to by someone else’s research results and establish procurement partnership with others, and this way to “tap into their learning curves”. It is most probable that some of the countries will accept this liberal approach, but some of them will act with some mercantilism. As the Report of Conference on Defence Economics: Reform, Restructuring, Realignment² declares, separate countries will follows different strategies. For example, Estonia had no plans to establish defence industries; although it does wish to be engaged in research. Lithuania would like to conduct defence research, and to produce food, uniforms, camouflage and small arms. Uzbekistan has no stand-alone defence industry and considers it too expensive to start now. Moldova is focused on completely converting its defence industry to commercial production in cooperation with foreign investors. Experts from Czech Republic accepted that small and smart states will choose production of defence hardware. From this point offensive weapons are for the big ones. For all these we could add that although Bulgaria has not official strategy, the position of the Association of Bulgarian Defence Industry claim for development of existing two dozens of industrial enterprises through regulated state offers. Romania’s approach is not different. Macedonia will rely on the donated or leased equipment to

² Defence Economics: Reform, Restructuring, Realignment, A Report of the George C. Marshall European Center for Security Studies Conference, prepared by Mr. Alan Smith and Prof. Michael Meese, December 6-9,1999.

meet all needs above the level of small arms.

For some of these countries the German four-phased model of development new defence industry since World War II might be symptomatic. It starts with building and preserving a set of companies supplying the Bundeswehr, promotion of foreign cooperation for obtaining technology, and sustaining a minimum level of employment in key skill areas. The country began with licensed production of equipment (F-104 Starfighter). Then moved to collaborative projects as a junior partner (for example Sidewinder air-to-air missiles). Later it began indigenous production of rifles and the Leopard tank and evolved to equal partnership for production of weapons such as "Tornado", "Alpha jet" and "Meko" frigate which facilitated exports. Now most major projects are in collaboration with foreign companies (Eurofighter). Although his attraction, it has to be admitted that this model is premised by the high developed industrial base of the country. Indicative for the model is the collaboration with the allied companies, after the Germany acceptance in NATO in 1955. This case confirms the practical validity of Article 2 of the North Atlantic Treaty³ which states that "The Parties will contribute toward the further development of peaceful and friendly international relations by strengthening their free institutions, by bringing about a better understanding of the principles upon which these institutions are founded, and by promoting conditions of stability, and well-being. They will seek to eliminate conflict in their international economic policies and will encourage economic collaboration between any or all of them." Although the inherence of the WW II Alliance helps and not only Germany but also number of other European countries to restore their defence industrial capability.

On the other hand transitional countries and Bulgaria suffer from underdeveloped defence technological and industrial bases (DTIB). With some differences common findings and gaps are:

- Inherited state centralized R&D management, and even partially state owned companies.
- Underdevelopment and limited government R&D expenditures – for Bulgaria around 0.51% GDP.

³ The North Atlantic Treaty, Washington D.C., April 4, 1949.

- Low innovative private defence companies without government contracts, which explains the existing 7-8 times output decrease and export orientation.
- Strong State Production and Export Controls.
- Decrease in R&T, financed by companies.
- Limited R&D capabilities in academy and universities, financed by government.
- Product and technology gap and decrease.
- Isolation from leading R&D and R&T centers.

Current R&D Policy for DTIB in Bulgaria is characterized by:

- Not clear government policy, and strategy (goals and priorities).
- Not initiated from government Security and Defence (S&D) Sector R&D, and R&T Programs.
- Lack of corporate strategic vision, R&D and R&T budget and limited private resources.
- Social constraints for increase of S&D resources.
- Lack or limited number of innovative local companies.
- Low salaries, brain drain and shortage of researchers and infrastructure.
- Not efficient measurement of R&D and R&T output.

All these conditions and factors are result of historical development and acceptance of liberal economic approach to national DTIB. That is a normal economic logic in the case of needed economic stabilization of the country. The DTIB policy has been not a priority of the state in transitional period to market economy. On the practice the yearly income of this sector is not more than 0.06%, while defence expenditures are 1.8% of GDP of the country. The question now is will the alliance policy could change this tendency.

2. Two strategies for defence technological and industrial base development

The alliances could accept at least two pure and number of mixed strategies for development of the countries defence industrial bases. The older one, used by the Soviet Union and Warsaw Pact includes states owned companies, weapon procurement only from the allies,

and cooperative production based on the preliminary negotiated specialization and standardization of production between the partners. This strategy is directed to the centralized cost-effective approach to resource allocation. The alliance used to operates with cheap, universal, and uniformed (single types) weapons and equipment. The high technological types have been produced by Soviet Union. The low technological types have been transferred to the supporting allies on the political base mainly through gifting or symbolic payment of know-how and documentation, without strong safeguards for intellectual property. On practice this approach permitted East European countries to restore and develop their defence industrial bases after the Second World War, and to afford them to participate into Cold War arms race.

On the other side the strategy used by United States is based on the competition of high-tech capable national private companies. The defence industrial base of the country is “capability-driven” with an internal source of development. The Federal Government is allocating for R&D around \$ 30 000 per every soldier, which is equal to the all expenditures for every separate soldier in South East Europe. The difference is so big that it is eliminating the practical possibilities cooperation between two sides. The probable cooperation could have only political, but not business and technological nature.

Historically, the emphasis on innovation as a source of industrial competitiveness became noticeable in the Europe in early 1990s. An Integrated Approach to European Innovation and technology Diffusion Policy had been accepted in 1993. It stated that “Innovation and technology policy has an important role to play in developing the competitiveness of industry in the face of global competition and in improving the quality of life. Later, this causes an essential need to guide the technical change toward important public goals such as environmentally sustainable development” (European Commission, 1993). Further, The European Commission’s 1995 Green Paper on Innovation and the subsequent First Action Plan for innovation in Europe were launched and provided an additional momentum (European Commission, 1995).

Nowadays, in area of defence EU through European Defence Agency developed the Framework and a European Defence R&T Strategy⁴. The Agency selected 12 R&T Capability priorities. It started the process of building a new European Defence Equipment Market and creating new Intergovernmental Regime to encourage transparency and competition in defence procurement practices of the EDA's Member States. The Regime is including the set of agreements. The key point of initiative, according to Javier Solana is that "For the first time ever, European countries have committed to procure defence equipment from each other if the offer is the best available."⁵ The Article 296 of the Roma Treaty give the countries right to take decision about their defence production. The EU defence market has been long fragmented into protected national markets despite the existence of European Community procurement rules. The new principles are directed to guarantee economy of scale and new level of efficiency for the Member States. The Intergovernmental Regime in defence procurement and associated Code of Conduct require transparency and equal treatment of suppliers in national tendering. It should increase fair competition among the companies. On 1 July 2006, a new "Electronic Bulletin Board" was launched on the Agency's website, providing an opportunity to bid for defence contracts in all the other Member States of the EU. Additionally the "Framework Agreement for Security of Supply between Subscribing Member States in Circumstances of Operational Urgency", agreement for "Security of Information Between Subscribing member States", and "Code of Best practice in the Supply Chain" marked the obligations for providing a supply of defence equipment and services in times of need or emergency. On 1 July 2009 EDA launched a new Code of Conduct on Offsets (adopted on 24 Oct 2008, and entering into force on 1 July 2009). The Code introduces publishing of information on national offset policies and practices, and is directing to gradually reducing reliance on offsets, increasing transparency, and evolving

⁴ EDTIB, A Strategy for the European Defence Technological and Industrial Base, EDA, <<http://www.eda.europa.eu/>,

⁵ A guide to the EDA's new European Defence Equipment Market, EDA, <<http://www.eda.europa.eu/>, 2006.

towards use of offsets that help shape the European Defence Technological and Industrial Base (EDTIB).

Although all these initiatives the real support for competent and competitive development of defence technological and industrial base of the transitional countries (including Bulgaria) until now has been often lacking. All these countries are on the Electronic Bulletin Board as buyers but not as sellers. Existing EDTIB Strategy, EDA Armament Cooperation Projects, Defence R&T Joint Investment Programs on Force Protection and Innovative Concepts and Emerging Technologies are faced with a strong challenge of needed capabilities, common enterprise and co-operative EDTIB dilemma.

3. What is and why to establish Strategic Business Alliances (SBA)?

The valuable alternative for to increase the effectiveness of centralized initiatives for defence technological and industrial base development gives the idea for company's strategic alliances.

Parkhe stated that⁶ "...SA are relatively permanent inter company agreement for collaboration, including streams and relations, which there use resources and/or managerial structures from independent organizations for joint achievement of individual goals, related to the corporative mission of every participating companies"

Different types of alliances are in use:

- According to relations - Horizontal, Vertical and diversifying (conglomerates).
- According to partner contribution – Shared supply, Quasi-concentration, Supplementary.
- According to capital involvement – not capital (Subcontracting, Piggyback, Licensing, Franchising, Consortium, Joint agreement); capital (Joint ventures, Minor participation).
- According chain of value – For tech development, for logistics and operations, for marketing and others.

There are a lot of data, which clarify why a company needs to en-

⁶ Marangozov, Y., Strategic Alliances, "Avangard Prima", Sofia, 2009.

ter into Strategic Alliances?

- 60 thousand SA has been established into 179 states for the period 1990-2000 (Moskalev & Swenson, 2006).
- Every big corporation in 2002 is taking part into around 30 SA (Ring & Lorenzoni, 2002).
- 26% of the “Fortune 500” company’s income comes from SA (Spekman, 2000).
- SA in all the branches, including partnership with present or future competitors.
- Increasing competitiveness and lack of company’s investment.
- Reducing the transaction costs.

Summarizing the existing NATO and EU policies toward the transparency, competence and competitiveness of the defence and technological industrial base we could admit the lack of relevant initiative for promotion of strategic business alliances between the transitional countries companies and advanced technological companies in leading NATO and EU countries. We could argue that deficiency is valid not only for the separate local and international companies, states, but also for allied organizations.

A number of factors are complicating the co-operative agenda

- Global financial crises are limiting the willingness for entering into SBA.
- East European Countries, incl. Bulgaria are far from the very centers of economic power and are in an area of economic instability, which is deviating the attention of biggest international companies from these countries. There are not even examples for such co-operation.
- The competence and the defence technological and industrial capabilities of the mentioned countries are on the crucial level for co-operative production. That is underling more political than economic character of the co-operation and the role of the Member States governments than the companies.
- Declaims of production and reduction of personnel also is limiting the adjustment for cooperation
- Strong allies and national political support and company insis-

tence is needed for promotion and development of the SBA.

It is clear that the co-operation in the defence technological and industrial base is not easy and fast process. Some authors stress on the difference of the military and economic strategy. Robert Cooper⁷ compares the military strategies and economic logic and underlines that:

- Military transactions are almost inevitable part of negative sum game. Opposite of that economic transactions are part of a positive sum game.
- Military activity is essentially coercive, economic activity is contractual.
- Military structures are centralized and hierarchical, economic structures are decentralized and competitive.

Sometimes these two opposite approaches are not compatible. If we apply strong economic criteria, co-operation between hilly competitive and back warding companies has no sense. On the other hand enlargement and development of ally's DTIB from military point of view could have an important effect for the common capability. In this case the state or alliance has to have the levers for to promote this process, and also the available resources to take the burden of that.

Acceleration and successful development will need systematic, profound and coordinated effort of all participants. The key points for success are:

- Mutually confidence for observing contracts.
- Guarantees for corporate security.
- Bilateral transfer of knowledge, which mean sufficient R&D capability into companies.
- Proactive state policy and economic guarantees.
- Close contacts with NATO and EU R&D and R&T organizations.
- Active engagement of University and Academia R&D organizations.

This factorial picture and future development is not optimistic, but although it is possible for some of the countries.

⁷ Global Security, North American, European and Japanese Interdependence in the 1990, Edited by Eric Grove, BRASSEY'S ATLANTIC COMENTARIES No. 5, BRASSEY'S, 1991.

4. Role of SPS Programme for promotion of SBA

The 2008 was a 50th anniversary of science co-operation at NATO⁸. The NATO Science for Peace and Security (SPS) Programme is dated to 1956, when a report by Foreign Ministers Halvard Lange of Norway, Gaetano Martino of Italy and Lester B. Pearson of Canada emphasized the importance of political, economic and scientific consultation for Allied security. With the report recommendations the North Atlantic Council (NAC) established the NATO Science Committee (CCMS), which had its first meeting in March 1958. Later the NAC created the Committee of the Challenges of Modern Society (CCMS) in 1969. In 2006 SCOM and CCMS have been combined to form the Science for Peace and Security Committee, in parallel with the formation of a new, comprehensive SPS Programme. The new committee focuses its activity and projects in civil science to scan the emerging threats, and encouraging innovation in security, stability and solidarity among allied nations. This way the SPS Programme play a central role in NATO R&T community, including the NATO Undersea Research Centre (NURC), Allied Command Transformation (ACT), NATO's Main Armament Groups (MAGs), the NATO Industrial Advisory Group (NIAG), and the NATO Consultation, Command and Control Organization (NC3O), established in March 2008 Defence and Environment Expert Group (DEEG) and national experts from NATO and Partner countries.

Although the SPS Programme focuses in support of civil science co-operations between NATO and its Partner and Mediterranean Dialog countries in the area of Defence against Terrorism and Countering other threats to security the development of the technological and industrial co-operations between the Partner Countries is not far from its mission. In Prague, eight specific fields were identified as being the arias where shortfalls needed the most urgently to be addressed: strategic air and sea lift; chemical, biological, radiological and nuclear defence; and air-to-ground surveillance. These are the priority areas for

⁸ SPSC NEWS, 50 Years, www.nato.int/science, 2008; Report of the "Three Wise Men": 50 years on, NATO Review, NATO's past, present and future, www.nato.int/review, 2006.

modernizing military capabilities, and the key topics for R&D and R&T activities for companies. These topics are the key directions for co-operations between RTO, NC3I, other NATO R&D, R&T organizations, and Partner Countries:

- Sponsors practical cooperation between scientists from NATO members and Partners in civil science, environment and technology.
- Facilitating collaboration, networking, capacity-building and promoting the application of the best technical expertise to problem solving.

These directions are promising to prepare the transitional countries to adapt their R&D and R&T policies for co-operative work. Although the promotion of establishment and development a new, even smaller strategic business alliances between the leading companies and smaller ones from the South East Europe and Bulgaria is a future priority.

Conclusions

SBA in defence technological and industrial base is a key factor for integrating of national bases to the Alliance base, which is a vital for the sharing and management of the risks for alliance goals and objectives.

The real problem of Defence co-operation between the Member States comes from the specifics of decisions for that. These decisions involve a number of players. The company has to be ready for that, and to have relevant competence and effectiveness. It has to have an exact estimation about its own competitiveness, the strong and weak points, existing treats and real opportunities. The basic condition is to have a sufficient R&D and R&T potential, which is capable to transfer and to develop the accepted technologies and products.

Government is also responsible for initiating cooperative efforts with clear requirements about the defence industrial output, which has to be well fitted to national capability plans. It is critically important to have a close relation to the companies, and large and efficient national representations into allied R&T organizations for to transfer

the existing opportunities for co-operative activities. Traditional bureaucratic weakness of the national contacts point has to be overcome by promotion and appointment of well prepared and hilly motivated experts. Governments have to stress more on the allied objective than the national interest. They have to rely more on the competitive force than the national offset programs, which benefits separate than the national and ally's interest. Not last but also important is to accept the strategic and program approach for management of co-operative policy.

The allied organizations have to promote relevant to all the countries R&D and industrial co-operative policies, including support of establishing a SBA between the companies. The existing Codes of Conduct for procurement an Offset have to be complement of a new Code for Co-operation between ally's companies.

CURRENT ECONOMIC CRISES AND CHALLENGES FOR DEFENCE BUDGETS

Prof. Zoran Ivanovski, PhD

Rector of the European University, Skopje

Assist. Elena Stoichkova, BSc

Assistant at Faculty of Economics, European University

Abstract

Current economic crises ask prudent and strong actions from the governments in order to prevent hard consequences that challenge their national economic systems. They usually make massive budget interventions in financial and real sector in order to generate additional demand in the economy as well as to stimulate economy.

Budget distribution allocates financial resources for wages (public administration), current expenditures and capital expenditures.

Budget has to provide additional demand and spending in national economy in order to prevent appearance of recession and to compensate lost foreign direct investments (FDI). It is especially necessary for small economies where budget spending affects the rate of economic rise.

It is obvious that because of current economic crises governments have problems to realize planned fiscal revenues and budget expenditures. Many governments already announce budget cuts. The question of scope of military expenditures is already raised through public and academic debate. The range of the debate oscillate between defence spending as a great stimulus and doubts and concerns about it.

Key words: crises, economy, stimulus, defence budget, expenditures, PPP

Introduction

World faces great challenge in terms of economic crises. At the same time, governments create budgets in order to reply to the strategic challenges facing the economy, making massive intervention in finance and real sector of economy.

Beside this new war against crises, governments have to provide public services and rate of economic rise promised to the people dur-

ing their election champagne. It is also necessary highlighting the importance of infrastructure in delivering not only public services that meet people's needs and expectations, but also economic prosperity and growth.

This paper analyses in broad terms the changing investment needs and challenges for the Government of the Republic of Macedonia in terms of economic crises; sets out a range of approaches that have been developed to address complex procurement issues; outlines the role of private finance and the important contribution it can make; illustrates the key principles and drivers of value for money that public sector procurers need to use to evaluate a broad range of procurement approaches; and sets out how the Government is developing a more risk-based, systematic approach to the scrutiny of major projects, while providing support to them and further enhancing the skills of the public sector.

This study outlines the Government's approach both in order to assist public sector procurers and to act as a basis for further dialogue between the public and private sector on how the Government can best meet its investment needs and help drive value for money solutions in complex procurement.

However, because of economic crises, many governments already announce budget cuts. This study will highlight part of debate about role of defence expenditures as a great stimulus and doubts and concerns about it.

1. New role and organization of public services

The basic task or ambition of each government is to provide high quality of public services that can respond to people's need. Governments develop new strategies in order to transform public services and to provide value for money.

World faces great challenge in terms of economic crises. In the same time, governments create budgets in order to reply to the strategic challenges facing the economy, highlighting the importance of infrastructure in delivering not only public services that meet people's needs and expectations, but also economic prosperity and growth.

Governments are trying to secure value for money in its procurement of significant assets, infrastructure and long-term service provision. In doing so, it recognizes the continually evolving needs of the public sector, and the changing approaches to complex procurement that have been developed over the past 15 years, and that will continue to develop. Governments have obligation always to consider possibilities of using PPP (Private-Public Partnership) as well as Private Finance Initiative (PFI) when plan procurement or capital budgeting. It outlines a framework for infrastructure procurement that is designed to drive value for money across the full range of procurement approaches and ensure the effective scrutiny of key projects, while continuing to improve public sector procurement and commercial skills. Through this, governments have to build the techniques and processes for PFI and apply them across a wider procurement spectrum.

Considering ideas and practices about full implementation of PPP and PFI as a strategic decision and vision of the Government of the Republic of Macedonia, it is hard to say that Government move step forward from declarative ideas for their implementation. It dues on hard public perception that such arrangements are causes for frauds, corruption and still communist legacy that somebody can make profit using public assets. However, it is crucial, especially in terms when budget constraints are obvious and expected that Government have to implement PPP and PFI in order to finance and fulfil planned capital investments. There is no alternative, especially when becomes obvious that FDI will miss.

Starting from basic trade off in economy, risk-return, Government has to provide fair return for investors risk and it can attract not only domestic but also foreign investors.

2. The infrastructure challenge- infrastructure procurement: delivering long-term value

The Government has an objective to deliver high-quality public services. To achieve this, sustained increases in investment and new approaches are needed to meet the new challenges especially in terms of crises. Strong and dependable public services also lay the founda-

tions for a flexible and productive economy.

This chapter briefly analyses Government's investment plans to deliver public services, in terms of the direction (sectors) of the Government's investment plans for the future and how the Government intends to reform its framework for the most complex procurement projects to harness the full range of procurement approaches and drive value for money.

The environment in which public services operate has been transformed by far-reaching social, economic and technological developments over the past decade. Changing demographics and patterns of work and life, the impact of globalization, new technologies such as the internet and other developments, including in relation to the environment, are creating new and rising demands on public services and substantial changes in public attitudes and expectations.

Budget of the Republic of Macedonia 2009 sets out the strategic challenges facing the economy and confirms the importance of infrastructure investment in driving economic prosperity and growth. The Government also needs to meet new environmental and security challenges. This requires further progress and investment in associated assets and supporting infrastructure. Government action to meet these challenges includes:

- Education – capital investment in building and maintained of schools. Government started from 2008/2009 with two new important programs - for compulsory high school and establishment of new public universities in order to increase level of education in the country.
- Health – hospital building program and improvement of the quality of health care.
- Transport – capital investments in new highways and finishing railroad to Bulgaria. The basic idea is to stimulate economy development (direct and indirect effects).
- Housing – investment program as a long-term commitment to increase the availability of social housing
- Defence – This commitment provides capital investment in the armed forces. This investment will help to ensure that our armed

forces have the right balance of capabilities, both equipment and infrastructure, in order to meet a range of challenges.

- Waste Management – the Government is increasing investment in more sustainable waste management options as an addition to, and roughly matches, investment by local authorities themselves.

Good procurement is central to the start of the asset life cycle and it is crucial that procuring authorities use a whole-life costing approach rather than the cheapest or easiest option. Major infrastructure projects require detailed and careful planning and it is important that a robust, value for money assessment be made when choosing the procurement option.

There is no doubt about proper identification of the need to invest in above mentioned crucial sectors, but also Government need to have a more strategic approach to asset management, driving better value for money and encouraging efficient management of the government's existing asset base. This includes:

- with the agreement of the Treasury, departments being able to reinvest proceeds from the sale of surplus fixed assets in capital investment in addition to their existing capital budget;
- departments producing asset management strategies to set out their plans for actively managing their existing assets and to provide the strategic context for future investments;
- retention by departments of proceeds from more efficient use of assets arising from engagement in the Wider Markets Initiative;
- initiative to deliver increased efficiencies in the management of the Government's property assets, especially through PPP; and
- the National Asset Register to help ensure that Government retains only those assets required for public service delivery.

Budget constraints as well as inappropriate and unsatisfactory use of public owned assets raised the question of PPP as additional opportunity to realize planned capital investments. PPPs are arrangements typified by joint working between the public and private sectors. In their broadest sense they can cover all types of collaboration across the private-public sector interface involving collaborative working together and risk sharing to deliver policies, services and in-

frastructure. PPP exhibits the following key features:⁹

- a joint working arrangement between the public and private sector, which may be by contract or through a joint venture company, to deliver infrastructure assets and usually, but not always, the ongoing maintenance and operation of the infrastructure assets and the delivery of associated services;
- risks are allocated between the parties based on which party is best placed to manage and bear the risk. Typically design, construction and operational risks are expected to be borne by the private sector; other risks which are shared are allocated in the way that best incentives both parties to manage the risks;
- generally a PPP is a long-term (25-30 years) arrangement between the parties but can be shorter term, for example where ongoing maintenance of the infrastructure assets and associated services are excluded;
- where ongoing operation and maintenance of the infrastructure assets and delivery of associated services are included, the public sector may pay the private sector for all or part of the use of the infrastructure over the life of the arrangement;
- payment to the private sector is structured in such a way as to ensure the private sector is incentives to deliver the required services or obligations under the arrangement;
- payments are usually made by the authority but can be made by the end user, for example for the use of a toll road;
- the public sector is seeking to access private sector management and expertise to drive value for money; and
- the project is often financed either in part or in whole through private finance.

Government has to proceed with continued assessments of the ownership and management of the governments corporate and financial assets, these initiatives have also ensured good progress against the asset disposals target.

⁹ *Infrastructure Procurement: Delivering Long Term Value*, HM Treasury, March 12, 2008, page 18

3. Better asset management, PFI and its place in public expenditure

The vast majority of investment in the Macedonia's public services has been, and will continue to be, procured through conventional means. However, other innovative procurement approaches, and PFI in particular, has to be used to deliver some of the government's most complex and significant public sector infrastructure projects and programs. It becomes more and more necessary especially in terms when Government faces with budget constraints and limited resources for capital investment to start with PFI. PFI is an arrangement whereby the public sector contracts to purchase services, usually derived from an investment in assets, from the private sector on a long-term basis, often between 15 to 30 years.

It is necessary for Government to stimulate innovative procurement approaches that may in some circumstances provide better value for money for the public sector in addressing the complex infrastructure investment challenges ahead. It does, however, also announce a number of specific measures. To improve the procurement process, applicable to any delivery model, for large, complex infrastructure projects and programs, the Government (Treasury) has to:¹⁰

- issue guidance on conducting tenders for complex projects under Competitive Dialogue procedures;
- issue guidance on project maturity – the state of development in infrastructure investment plans should have before the public sector formally engages with potential private sector contractors;
- move to a risk-based approach to scrutiny, with scrutiny taking place earlier in the procurement cycle and with increasing focus on the delivery model and the procurement process; and
- continue to support a wide-ranging program aimed at enhancing public sector procurement and intelligent client skills.

Government has to make clear guidance on joint ventures, to consider changes in credit terms through banking institutions where

¹⁰ *Infrastructure Procurement: Delivering Long Term Value*, HM Treasury, March 12, 2008, page 11

Government is part of ownership, has to issue guidance on specific PFI financing issues (related to refinancing, primary equity returns, underpinned debt and public sector capital contributions).

4. Defence spending as “stimulus”

The current world economic crisis torn defence and policy planners worldwide between two seemingly contradictory urges: reducing defence expenditure to help restrain spending, and increasing defence expenditures to help restrain growing global instability and shifting balance of power. Balancing or keeping at one side of this urge is something governments are facing while preparing 2010, or rebalancing 2009 budgets.

It is quite a challenge to cut defence budgets now, after military budgeters over the last decade went on expenditure binge. But the question is why or where to cut, or if there is a possibility that defence spending could be a stimulus for world economies that face economic downturn. In United States the question of scope of defence expenditures is already raised through public and academic debate.

U.S. Defence Department's budget, excluding funds for nuclear weapons, rose by nearly 70% between 2001 and 2009. The bullish economic climate, globalization, global war on terror and the rapid ascend of India and China provided all the excuses and resources to both politicians and military professionals. But now, with the global economic crisis they are forced to take a hard look at future military expenditures. At the end of 2008, after America got its new president Barak Obama, and the crisis became deep economic recession, it was clear that changes are needed to be made. Many expected immediate budget cuts in response to the decline in national income, but also many argued for increased government spending as a way to offset the sharp decline in consumer outlays and business investment.

Economies with the most developed defence industries are ones that can use their defence expenditures for moving and stimulating the whole economy. But it is obvious that such measures can only bring benefits to countries that implement them, and the recession is a global issue. Conservative economist and one of U.S. President

Obama's advisors on the President's Economic Recovery Advisory Board, Martin Feldstein made waves last year when he declared his support for a fiscal stimulus bill to combat the recession. Last December, Feldstein wrote in the *Wall Street Journal* that "a temporary rise in DoD spending on supplies, equipment and manpower should be a significant part of that increase in overall government outlays." Thus the idea of defence stimulus was born.

This idea has its bases in the Feldstein's arguments that if Washington adds 10 percent to its overall investments in defence, 5 percent to the Pentagon's operations spending, and recruits another 30,000 soldiers (a total increase of \$30 billion), it will help make the economy well again. Even Defence critics such as Lawrence Korb have called for more defence dollars in the stimulus package.

The Obama administration's \$787 billion stimulus package was headline news for weeks, bitterly argued over, hailed and derided in equal measure. At the end of February, another huge "stimulus" package was announced but generated almost no comment, controversy, or argument. The defence industry received its own special stimulus package – news of the dollars available for the Pentagon budget in 2010; and at nearly \$700 billion (when all the bits and pieces are added in), it's almost as big as the Obama economic package and sure to be a lot less effective.

But why less effective, what are the arguments against using defence expenditures as an economy stimulus? What are the facts that crucified the idea of using defence expenditures as a way out of world economic crisis? The world remembers how World War II and the production stimulus it offered lifted the United States out of the Great Depression.

Today, the opposite seems to be the case. There are many arguments behind this statement.

First, there isn't a policy reason to increase the defence budget. The bulk of the spending for Iraq and Afghanistan has already happened. Currently Defence's resources are at historically unprecedented levels, as U.S. defence spending dwarfs any previous level in constant dollar since World War II. U.S. spends more on defence than

every other country in the world combined and all of this has led to an almost unprecedented fiscal boon to the manufacturers of military equipment and out-of-control defence budget. Even the defence increase from 3.4 percent of GDP in 2002 to a 4.2 percent in 2008 did little to stimulate economic growth and did nothing to contain the current economic crises – making Feldstein’s proposal to add \$30 billion in defence spending to the stimulus package to boost the economy, sounds like a joke.

Second, it is very important to allocate defence expenditures that can bring benefit to the economy in short terms. Even if Obama stimulus package includes more than \$10 billion for defence expenditures, it is a must-to-know their exact allocation in order to anticipate short and long term impact on the economy. In other words, the stimulus package does contain some spending for defence – new construction, building repairs and maintenance, greening the military infrastructure, etc., but that money is in fast-spending dollars, the construction projects are already designed, the repairs can happen quickly, and the green infrastructure can move just as fast. And when it comes to the equipment that has been degraded by operations in Iraq and Afghanistan, the funds that are needed to repair and replace it have already been heavily front-loaded in the last three “emergency” supplemental budgets, each of which contained \$20 billion to \$30 billion to repair, upgrade, and buy new military equipment. This shows that some kind of stimulus package in the defence industry of U.S. has been under way for a while, yet the economy has sharply tanked. Feldstein argues that defence expenditures have near-time stimulative effect on the economy.

There are also opposite opinions. Economists have also weighed in on why “war for jobs” as a way out of recession or depression has entered the world of mythology. An analysis from the University of Massachusetts’s Political Economy Research Institute, for instance, finds that, for every one billion dollars invested in defence, 8,555 jobs are created. By contrast, the same billion invested in health care would create 12,883 jobs, and in education, 17,687 jobs or more than

double the defence stimulus payoff.¹¹ Reallocation and rationalization of defence expenditures is what U.S. is doing now. U.S. President Barack Obama and Defence Secretary Robert Gates decided rather to rationalize than to cut defence expenditures so successively defence budget signals changes in goals and in weapons. Mr. Gates's proposed baseline 2010 Defence Department budget of \$534 billion is up 4% from last year.¹² But it signals a major departure from business as usual at the Pentagon, with a heavy emphasis on overhauling a procurement process that he and congressional leaders have decried as being too heavily influenced by powerful contractors.

However, small economies have also to consider necessity of investment in defence sector as economy stimulus. Considering Republic of Macedonia, country with still fragile security, it is question without alternative. Security is precedent for the people, so defence budget will escape from current budget rebalance.

Conclusion

Responding to global economic crises requires governments to have innovative approaches in solving current issues, sometimes to make tough decisions and to apply them in order to realize what is decided and planned. Global changes arises the need for changes not only for the private, but also for the public sector of the economies. Problems need to be solved with synchronized action between governments and their agencies on one side and private sector on the other side. It is obvious now, months after appearance of crisis, that both sectors need coordinated actions. So why not to take advantage of that connection and use it in a way that brings benefit to the whole economy?

Recession means less or even no FDI, less budget revenues and more cuts of budget expenditures and this is where Governments face a problem. They must find a way to compensate what is lost and to stimulate economic growth. A way of doing this, is through Private-

¹¹ Berrigan, Frida, *"Is the Next Defence Budget a Stimulus Package"*, March 12, 2009

¹² The 513 billion dollar budget for 2009 is a final budget, and the proposed 2010 budget of 534 billion dollars hasn't had any supplements yet.

Public Partnership and Private Finance Initiative and these innovative approaches are ensuring better assets management and good procurement. There are also many other ways of stimulating economies that have problems connected with the crisis, as it is defence expenditures or cutting, rationalizing and reallocating different parts of the budget. Still, what will prove to be the best solution is something that first needs to be done.

References

1. *Infrastructure Procurement: Delivering Long Term Value*, HM Treasury, March 12, 2008 [http://www.hm-treasury.gov.uk/d/bud08_procurement_533.pdf]
2. Feldstein, Martin, “*Defence Spending as Stimulus*”, The Wall Street Journal, 24 December, 2008. [<http://online.wsj.com/article/SB123008280526532053.html>, retrieved April 24, 2009]
3. Leo Shane III, “*Crisis Could Affect Defence Budget*”, Stars and Stripes, European edition, February 08, 2009. [<http://www.military.com/features/0,15240,184538,00.html>, retrieved April 22, 2009]
4. Lubold, Gordon, “*Defence Spending As ‘Stimulus’*”, The Christian Science Monitor, January 08, 2009. [<http://www.csmonitor.com/2009/0108/p01s03-usmi.html> , retrieved April 22, 2009]
5. Adams, Gordon, “*Increasing the U.S. Defence Budget Won’t Stimulate the Economy*”, Bulletin of the Atomic Scientists, February 10, 2009. [<http://www.csmonitor.com/2009/0108/p01s03-usmi.html> , retrieved May 02, 2009]
6. Berrigan, Frida, “*Is the Next Defence Budget a Stimulus Package*”, March 12, 2009. [http://www.newamerica.net/publications/articles/2009/next_defence_budget_stimulus_package_11761 , retrieved May 02, 2009]

SECURITY AND DEFENCE R&D POLICY FRAMEWORK - OPTIONS AND ALTERNATIVES FOR BULGARIA

Assoc. Prof. Dimitar Dimitrov, PhD

Head of Department “National and Regional Security”,
University of National and World Economy, Sofia

Dear participants,

Since our project is approaching to the end, I would like to outline some of our project results, according to the Project Plan – Objective 2. The topic of my report is directly connected with these results. For almost 3 years our project teams from Bulgaria, Romania and Macedonia prepared Research methodology, several case studies, 3 national draft policy frameworks, teaching materials, at least 25 publications devoted to the research problems. Some other project results with contribution to Objective 2 - Problem identification, Developed NATO integrated R&D Concept and Model, Database, Expert network and relevant publications as well as involvement of young people in the project activities. I am stressing on the way, through which we reached our final task – elaboration of national policy framework.

In my presentation I will use examples and ideas from and for Bulgaria, although the problems are common in all project participants, but they need national solutions.

Why elaboration of policy framework

In my previous project reports and presentations I already mentioned this issue. Our objective is not to produce one of the numerous written documents on policy, but to look on the problems more broadly. Just preparing a formal written document is not a solution of the problems in defence R&D. Our goals were related with definition of the main problem areas, policy analysis, analyzes of the main policy elements and then proposing ideas and alternatives for change. It is hardly to improve

something which almost does not exist. In our research we met many obstacles, related with the lack of main strategic documents in security and defence (long existing problem for Bulgaria), lack of National R&D Policy, lack of sectoral policy(ies) in security and defence industry and other obstacles as access to information and transparency. Without these very important elements and characteristics of the policy framework, it is very difficult to improve or to propose new defence R&D policy for Bulgaria. But looking from other perspective, it is narrow approach, too focused on Bulgarian problems and specificities. That is why we tried to use another modification of this top-down approach, based on our European and Euroatlantic integration. Anyway, the need of elaboration of security and defence related R&D Policy for Bulgaria exists. Also the policy framework for Bulgaria exists on European and NATO level, where (I have to mention this) fast processes of transformation are underway. Now Europe or more punctually European Union is moving to achieve consolidation on the demand side of the market, and to facilitate further progress towards supply side consolidation. The need, in short, is to accept that the DTIB in Europe can only survive as one European whole, not as a sum of different national capacities. The European DTIB's survival also depends on exploiting all the resources available in the enlarged Union, part of which is Bulgaria as well.

So, having in mind the main parameters, we tried to found the main policy common denominators, which in our opinion are European Integration, Euroatlantic Integration (NATO), National Coordination, and, Integration of National Efforts and Resources in Security and Defence related R&D.

Policy and policy framework

A policy is typically described as a deliberate plan of action to guide decisions and achieve rational outcome(s). However, the term may also be used to denote what is actually done, even though it is unplanned. The term may apply to government, private sector organizations and groups, and individuals. (Wikipedia)

In general good effective policy could exist only in relation with similar environment. We consider policy framework as set of princi-

ples and long-term goals that form the basis of making rules and guidelines and gives the overall direction to planning and development. The framework is very important and deficiencies in the framework explain many of the problems with real or written policies in Bulgaria.

The main elements of policy framework are Dialog; Political debates; Policy research; Setting goals; Setting priorities; Setting criteria; Setting rules of the game; Policy implementation; Accountability; Publicity; Transparency, Dissemination of information and knowledge; Access to information in regard of: projects, people, potential; Evaluation of results. Of course, there is and should be some overlapping with the policy itself, but it is understandable. When general rules are established, then they could be developed in more details in the policy. Also we have to take in account policy hierarchy. In our case it is National policy; National security policy; National defence policy; National R&D policy; National defence industrial policy and finally within this policy is the place of National Defence industrial R&D policy. The experts in this conference room know very well that many of these documents do not exist or are not updated accordingly. For example there is a draft Defence industry strategy, but the fact that it is put for consideration and discussion at the very end of the mandate of the government shows that for the long period it will continue to be only draft. There are many other examples. Even in one of his speeches President Parvanov stated jokingly and seriously that we have the most strategies per capita but unfortunately most of them are not working. When we have lack of debate, policy research and consensus on some basic societal developments, then it is difficult to elaborate good working policy. Government has a very special relationship with the defence industry – as customer, regulator, and principal source of research and development funding. But less and less does it remain owner; and, as defence companies move progressively from government to private ownership, and as shareholder funds become increasingly prominent in the control of companies, so one may expect the normal laws of a globalised economy to apply; capital will migrate to optimise returns.

Further my presentation is structured around the main elements

of the policy content, and comments and ideas for change are relevant for Defence R&D.

Policy overview

It will be much easier to comment if there was existing national and defence R&D policy. That is why within the project we carefully studied NATO R&D policy, EDA R&D policy, EU R&D policy and written materials are available, result of our project case studies. According to our research methodology, the case studies at least have similar structure and easily could be compared. In parallel with this we have studied national practices, starting with problem identification. Defence R&D is not isolated from the overall environment. Again, looking broader on policy framework, we studied the whole system of research in Bulgaria. Starting point was the new draft National Strategy for R&D development. (In the context of the report, we have to mention that for several years Bulgaria had similar document and again it was only draft. Now we have another draft document, which is still not accepted by the Parliament).

This document is not a pure strategy, it is more related with problem identification and of course, at the moment this draft is put for public discussion. Anyway, according to this material several main problem areas were identified, which are relevant for defence R&D as well. There is a short list with some comments.

1. Internationalization of the science – very limited number of international defence R&D projects with Bulgarian participants; it is especially true for the defence business R&D.

2. Lack of clear defined priorities. It is well recognized problem, but without solution until now. It is not clear who have to be the leading actor in the process of priorities' definition – the state, the science, the business or something else. In interviews Prof. Anastas Gerdzikov, Chairman of the National Research Fund, admitted that there is no clear process of identification and setting priorities for the national science. This problem was recognised also by the President of The Republic, Mr. Parvanov, who stated that it is not possible to concentrate our limited resources without priorities, defined according to

our national needs.

3. Lacking and ineffective financing – Bulgarian funding for R&D is well below the European level, and it is for many years.

4. Fragmented research and research organizations. - It is related with priorities again, but also depends on the state policies in Science and R&D.

5. Lack of modern R&D infrastructure. - Natural result of Under-investment in R&D.

6. Ineffective policy in regard of research personnel - with 2 tendencies – average number of Bulgarian scientists again is well below the European level, and the second tendency is related with aging of the research personnel.

There is no need to invent something totally different for defence R&D policy overview. Putting these problems in the future defence R&D policy will be the initiation of their solution. Then, further having the other policy instruments as size of resources, priorities, structures, etc, the defence producer will be acquainted with the actual intentions of the state in the field of defence R&D. Of course, it should be put in broader context of overall defence policy.

Defence R&D Policy Goals and Priorities

In our opinion these priorities should be in the direction of our EU and NATO integration and effective coalition participation, Current National Achievements (related with our current and potential markets and leading positions in defence R&D), Missions abroad, National Armaments Modernization Projects, and ‘Production’ of Scientists. Of course these are principal directions and they could be changed. The most important is the approach, the process and instrumentalisation how these goals and priorities will be elaborated. This is the problem of the policy framework.

When studying foreign experience, we found several interesting practice. For example, US DoD establish a Centre for Strategic Industrial Base Evaluation at the Industrial College of the Armed Forces (at the National Defence University) to continuously evaluate the health of the US defence industrial base in real time as well as strategically

and longer term, and to develop strategies for mitigating these risks in critical areas. This centre should analyze and build on the information in the extended production model, specifically regarding the global defence supply chain, and recommend key actions to ensure that the US military remains exemplary.

And this is not isolated act. As it is stated, all measures (including creation of this Centre) are results of the recommendation from the recent US National Innovation Initiative (again policy framework element). Such kind of debates, research, initiatives and other arrangements of the state institutions permit them to look more strategically in the future. These efforts must be coordinated with the DOD “priority critical technologies” identified in the defence industrial base capability assessment studies (DIBCS) being completed at DOD. Military excellence can only be achieved by preserving cutting edge technologies and the abilities to produce on demand (it is relevant for US).

In critical defence industry and technology sectors, US DOD supports roadmapping exercises, cost shared with industry, to help assure a strong industrial base in such sectors. DOD should also use these roadmaps to design its defence R&D initiatives, cost shared with industry, to assure ongoing technology advances in critical and promising defence technology areas. These roadmapping efforts could include technologies identified on the “watch list” being created by the Deputy Under Secretary of Defence for Industrial Policy’s office. This practice could be used by Bulgaria as well. Initial policy analyzes, policy research are the missing elements of Bulgarian defence R&D policy framework. It should, in the interest of enhanced interoperability, embrace pursuit of mutually-advantageous opportunities for pooled purchase of off-the-shelf equipment; or taking shares in a jointly-owned capability; or moving towards role specialisation or integration in a coherent and complementary fashion.

Actors and Coordination

There is a gradual transformation of Bulgarian defence R&D sector. As Prof. Nachev, director of DARI (Defence Advanced Research Institute to Bulgarian MoD) stated in his interview, during the transi-

tion period there was a significant downsizing of the military science and defence R&D organisations. The military educational institutions were excluded from the research activities, combined with the problems of the system for reproduction of scientists.

The situation in the defence business was the same -the R&D structures were the first victims of the enterprise downsizing. In absence of state policy toward defence industry, the state was disengaged from the defence industry. We see that American example is different. The creation of adequate structure is an essential element of creation and implementation of any policy. The structures with attitude to defence R&D in Bulgaria are very few, with very limited resources and opportunities. From one side, in Bulgaria we have DoD Program №10 (not transparent departmental programme), and from the other side we have powerful structures of EDA, NATO RTO and RTA, Framework programs, many councils, etc. with many responsibilities, documents, directives and priorities. It should be clearly stated -it is not problem of Ministry of Defence or the Education, it is national problem. In our studies we identified that there is a need of national coordination unit or contact point, with little bit higher level – at Council of Ministers. There is a need of integration of all efforts at national level – in regard of resources, personnel and information. And it should be done also in regard to homeland security, because there is a dividing line between defence and internal security.

Otherwise principal actors in defence R&D are Civilian R&D structures; Military /Defence ; Security structures; Defence industry; International actors, National representatives to different councils and bodies; Embassies; NATO and EU Committees and Councils participation; R&D personnel; Scientists; Administration; Students (incl. PhD); Politicians. Nowadays distinctions between defence and civil R&T will become increasingly blurred; that the latter will become increasingly important for satisfying defence needs; and that the pace of civil technological advance is constantly increasing. In this respect our Project Model for R&D management and according database could be useful for national coordination and management of R&D projects in security and defence.

Policy Guidelines

Warfare itself has become scientific, particularly in the twentieth century. After all, so notable an astronomer as George Ellery Hale said quite explicitly in his advocacy for the establishment of the National Research Council, “War should mean research,” and the First World War became known as “The Chemists’ War” and the Second, “The Physicists War.” In this century, with the advent of electronics, computers, and the Military-Industrial Complex (for all its effects), military hardware have become more and more scientific. Finally, the rhetoric of conflict at the twenty-first century repeatedly emphasizes the scientific, precision nature of warfare. Laser-guided bombs, GPS enabled troops, and night-vision IR goggles all take combat to the enemy with precision, power and progress. There are two additional areas that also call for a government role: R&D aimed at protecting from non-conventional terrorists threats, and R&D for improved cyber security. The former differs from a conventional terrorist threat obviously in the scope of the potential damage, making them a “macro” threat and thus turning the provision of security against them into a classic public good, with the usual implications.

Recognition of the importance of the science is not enough. We also need to establish clear Procedures and Rules for R&D funding and R&D activities in security and defence, Clear rules of Evaluation and Reporting, Diversity of forms and types of funding integration of national efforts.

Results and Beneficiaries

Principal beneficiaries of R&D policy are citizens, researchers, SME and Industry. The crucial role of the universities should be recognised. The expected results in general are growth and jobs, but also competitiveness, Labour productivity growth and effective coalition participation, enhanced security. Defence R&D is very likely to have **immediate, direct** spillovers to civilian uses. Presumably, there have been spillovers from “traditional” defence R&D all along (even if these are hard to quantify). The difference is that in this case the

technological frontier that defence (for example antiterror) R&D is supposed to push is the same as that required for progress in civilian uses. That is not the case with improvements in nuclear weapons or in stealth technology: in those cases the gradient of technological advance in military R&D has no direct relevance for civilian purposes, and the spillovers, if at all, are only indirect. Another area that calls for increased R&D resources is fast analysis of vast amounts of information, or data mining technologies, that has become an increasingly important activity in a wide range of sectors. R&D programs designed so as to preserve this diversity and to encourage further competition may prove highly beneficial both for the required defence R&D and for the advanced sectors of the economy themselves, thus fostering economic growth.

Research and Development (R&D) may produce technology which reduces operating costs of a system. When is such R&D economically justifiable? On economic grounds, the operating savings should exceed the R&D costs. For defence industry the main benefits are Competitive R&D potential, Spin-off effects on economy, Real integration in EU and NATO.

Resources

This is traditional problem – lack of sufficient defence R&D resource. Bulgarian R&D budget in defence is 3-4 Million Levs (it is not a percentage- it is around 2 Mln Euro). It is clear that there is a need of sharp increase, but also we need stable and sustainable growth of defence R&D.

Transparency and accountability

At first place political will is necessary, because the defence producers and related R&D are not nor acquainted with actual framework, they do not know the priorities, the rate of sustainability of efforts, size of resources and so on. More information, debates and transparency will permit to them to use more effectively European and NATO opportunities. Here many instruments could be used -

Websites, Reports, Analyses; Conferences, Foreign experience; Opportunities for cooperation and funding; Visibility of R&D Coordination Structures; and transparent and accountable regulations and procedures (not classified).

References

- 1 http://www.amtonline.org/amt_items/Bonvillian%20Paper.pdf
- 2 AN INITIAL LONG-TERM VISION FOR EUROPEAN DEFENCE CAPABILITY AND CAPACITY NEEDS
www.eda.europa.eu/webutils/downloadfile.aspx?fileid=105
- 3 <http://mediapool.bg/show/?storyid=152717&srcpos=1>
- 4 www.bgarmy.eu/?action=news&id=1373
- 5 www.minedu.government.bg/.../proekt_strategia_nauka-2008-2.pdf
- 6 www.president.bg/news.php?id=3209
- 7 www.nber.org/papers/W9725.pdf
- 8 www.pueron.org/pueron/news/.../Anastas_Gerdjikov.doc
- 9 <http://sfp.e-dnrs.org/>

**R&D NATIONAL POLICY IN THE REPUBLIC
OF MACEDONIA ACCORDING TO THE SECURITY
RELATED AND GENERALLY R&D SCENE –
CURRENT STATUS AND SHORTFALLS**

Major Elenior Nikolov, MSc

Military academy “General Mihailo Apostolski” - Skopje

Mr. Mitko Bogdanoski, MSc

Macedonian Army, Land Forces

Captain Robertino Chontev, MSc

Ministry of Defence, Department of planning
and bilateral cooperation

Assist. Elena Stoichkova, BSc

European University, Skopje

Prof. Zoran Ivanovski, PhD

Rector of the European University, Skopje

Abstract

Willing to use a more general, comprehensive, methodical and thorough approach based on a deductive analyze as well, striving to contribute on a pragmatic way in the area of interest - Security and military R&D policy in Republic of Macedonia, below is offered (by the authors) a ***problem-available means-possible solutions model*** based on the analyzing the current status, comparative examples, national and international environment, problems and shortfalls and consequently optimal possible solutions, future steps needed to be done.

1. Policy Framework

1.1. Governmental Bodies

According to the Constitution, the state has an obligation to encourage and support the technological development of the world. The governmental body in charge of R&D policy in the Republic of Macedonia is the Ministry of Education and Science, which is organised and executed by the Department of Science and Technology and advised by the Council for Science and Research. The Ministry of Education and Science is responsible for organisation, financing, developing and promotion of scientific research, technological development, technical culture, information technology and information systems as well as the international cooperation related to these issues. The responsibilities of the Ministry also include issues related to level of education.

Scientific activities in the Republic of Macedonia are performed and organised by a network of scientific institution comprising 6 universities (3 public and 3 private), several research institutes active in various fields units in industry. An important scientific organisation is the Macedonian Academy of Science and Arts, the goal of which is to stimulate development of the science and arts.

Within the governmental sector, we should also mention the activities of other ministries: the Ministry of Agriculture, Forestry and Water Supply; the Ministry of Economy, Health and Ecology; and especially the Sector of European Integration of the Government. According to their strategies, all these bodies act as important subjects related to the research achievement of the scientific community.

1.2. Legal Framework of the R&D Sector

Issues related to R&D are regulated by the following laws:

- Law on the Macedonian Academy of Science and Arts;
- Law on Science and Research Activities;
 - **Internal documents for:**
 - **Supporting of young scientists**
 - **Financing of scientific projects**
 - **Supporting of publishing**
- Law on Encouraging and Supporting Technology Development;

- Law on Higher Education;
- Law on Industrial and Intellectual Property Protection;
- Several regulations and instructions.

The Laws related to research arrange the system, principles, public interest, forms of organizations and management of these kind of activities as well as the ways of stimulating and supporting their development, scientific personnel and other issues related to them. The system of scientific activities involves scientific research, qualification and training of personnel for research work and research infrastructure.

The basic principles of performing scientific activities are inviolability and protection of human personality and dignity, and they are also based on the following: freedom of scientific creativity; autonomy and ethics of researchers during their scientific work and use and application of the results; diversity of scientific ideas and methods; and international cooperation.

These laws also define the public interest in scientific research in the field of national and cultural identity of the Macedonian people and others living in the Republic of Macedonia. It also determines research as a general condition for the economic, social, cultural and environmental development of the country. Research that serves the function of increasing the scientific level and transfer of knowledge as well as that in the field of defence and security is also defined in this law. Improvement in the human resources and research infrastructure are also in the public interest. A five-year programme for development of these activities is being prepared.

The law related to technology development stimulates and supports this kind of development in the country as well as the programming of this activity and its financing. This law defines technology development as:

- Development of own technologies;
- Progress of the country upon independent economic base;
- Modernization of existing production capacities;
- Building of necessary technological infrastructure and transfer of knowledge thorough a continuous superstructure of skills.

1.3. Role of the industrial sector in R&D

Considering overall political, social and economic conditions the country has faced during the past years, while additionally burdened by instability, the role and position of industry has significantly decreased in the domain of research and development.

As a result of restructuring and privatisation processes, many R&D units within enterprises have vanished. Present inconvenient financial circumstances do not allow larger investments in research and development.

1.4. Macedonian Research Infrastructure

Macedonian institutional infrastructure is as follows:

- Macedonian Academy of Science and Arts, comprising five departments and five research centres;
- Six universities (three public and three private);
- Thirty-four faculties;
- Thirteen public scientific institutes;
- Twenty R&D units within industry;
- Six scientific regional associations;
- Consulting agencies and offices.

In the following table can be seen scientific human resources in Macedonia until 2004.

Table 1

Scientific Human Resources in Macedonia

YEAR	1998	1999	2000	2001	2002	2003	2004
Total	3275	3168	3094	2909	2869	2589	2552
FTE	1892	1838	1786	1630	1519	1464	1447
FTE per 1000 LF	2.4	2.3	2.2	1.9	1.8	1.7	1.7

1.5. Financial aspects of science and technology in R. Macedonia

Considering the overall political, social, and economic conditions the country has faced during the past years, the funding of scientific research has been very limited. This has also been followed by a continuous decrease in the number of active researchers in the country. However, the Ministry has promoted and stimulated activities aimed at an integrated approach in research activities and especially for regional and international cooperation.

In 2002, the gross HE (Higher Education) expenditure on R&D - ratio of the GDP was 0.11. Out of 100% gross expenditure for R&D, 40.9% goes to research conducted in the HE sector. Support from the National Budget: national and international research projects, grants for postgraduate and doctoral studies in the country and abroad, R&D meetings, participation of academics in the international meetings, study visits abroad, programs of the public research institutes, equipment, R&D literature etc

The Higher Education Development and Financing Council (HEDFC) was established by the Government in October 2003. The Council is responsible for development and implementation of measures and criteria for financing of HE (institutions, investments in HE, student grants and loans etc.). It prepares programs for development of HE to be submitted to the Government for adoption.

In accordance with sources for financing, R&D can be financed through:

- own resources of institutions,
- companies resources,
- state budget,
- international financed projects.

Budget contribution to R&D is limited (scarce resources) and in 2002 it was 0,44% from governmental budget. In accordance with EU suggestion and directives from Barcelona it has to be from GDP, and in case of the Republic of Macedonia it actually means only 0,11 % from GDP. On the other side funds coming from business community are 0,02%, while EU directives are 2%. It means that in the Republic of Macedonia *business sector provides 100 times less than countries*

from EU. We can conclude that if continues in that way, we could not expect faster development of R&D in Macedonia. *Having not enough established R&D innovation system in the private sector and low interest in the private sector for R&D it couldn't be possible to provide faster development of science.*

The number of researchers in 2002 was 1519. For their activities in last five years were spent 0.2% of GDP per year. Considering the fact that level of budget expenditures for R&D is still not sufficient, we can identify the need for changes and searching new sources as urgent.

Public-Private partnership should be seriously considered as a additional element of R&D Concept and Policy, that can provide funding and development of necessary capacities and support of R&D Projects in the Republic of Macedonia.

Government still shows low level of trust to private companies' capacities for R&D in security sector as well as their bigger involvement and functions in security area. Full implementation of the Concept of Logistic Support for the Republic of Macedonia and ARM can provide progress in that way. It will help not only to improve the situation in security sector, but also will bring additional influence to economic development of the country.

2. The goals of R&D Policy in the Republic of Macedonia

Republic of Macedonia has managed to achieve significant results in certain scientific areas. There are several distinguished high-level institutes and centres recognized throughout the international scientific community. There are also other research units moving rapidly toward achieving international standards and criteria, which can be competitive and desirable partners in research activities.

The goals of R&D policy are to:

- Increase the use and transfer of knowledge for economic, social, cultural and environmental development of Republic of Macedonia;
- Encourage and promote international cooperation and transfer of knowledge and technology from abroad;
- Introduce a monitoring and evaluation system of scientific and technological quality and output of research groups using inter-

- nationally accepted standards and criteria;
- Increase investments in S&R activities;
 - Increase the use of international funds, technical assistance, etc;
 - Define and establish interdisciplinary programmes for target research;
 - Set internationally recognized measures for evaluation and assessment of the economic value of research results as criteria for future policy definition;
 - Support enterprises in establishing R&D units for effective transfer and use of new technologies;
 - Reduce the technological gap in order to reach the level of development of more highly developed countries;
 - Create conditions to raise the quality of knowledge and innovation;
 - Create a system of technology information as part of a community information system according to the criteria of relevant databases, services and networks;
 - Establish a unique infrastructure model to support and develop science and technology;
 - Heal and improve domestic industry and companies, and especially support SMEs in order to achieve better performance of their products and make them competitive worldwide;
 - Establish a system of priorities that will be supported by economic policy tools.

3. Measures Taken by the Government to Develop the R&D Sector and Encourage R&D

The ministry of Education and Science strives toward the successful transformation of higher education with regard to better transfer of knowledge within the scientific and business sectors.

The Governmental measures for improvement of the R&D sector are defined in several programmes, which encompass programmes for improvement of R&D and programmes for enhanced technological development. The Ministry of Education and Science has seriously considered the problem of the technological development of the country,

and in that regard, measures have been taken in order to stimulate and support cooperation between the universities and industry, improve and intensify the use of scientific research results in industry, and promote the technological development of enterprises aimed at stimulating their competitiveness.

→ Programs for improvement of R&D

- for encouraging and supporting national R&D projects,
- for granting fellowships for post-graduate and doctoral studies both in the country and abroad,
- for supporting researchers for participation at international meetings,
- target research program for coordination of the R&D activities within the governmental bodies,
- for encouraging and supporting technological development for the period 2006-2010,
- for development of R&D infrastructure

→ For enhanced technological development, measures are taken in order to:

- stimulate and support the cooperation between the universities and the industry;
- improve and intensify the use of the scientific research results in the industry;
- promote the technological development of the enterprises aimed at stimulation of their competitiveness.

During 2004 and 2005, for the first time, a complete database with publications in scientific journals with impact factors (journals referred to in SCI and citations of institutions and researchers) was created in the country. A database of all patent activities was compiled as well.

In 2005, the new Council for Scientific research was introduced. Furthermore, a completely new system of project evaluation was established with assigned national coordinators for each scientific discipline who manage the evaluation process of scientific projects in the respective fields.

In 2006, the Ministry of Education and Science signed an agree-

ment for national access to the electronic scientific database Scopus, which is available for all faculties and institutes at the state universities in the country. Also in 2006, the Government accepted a “Programme for development of scientific research activities in the Republic of Macedonia for the period of 2006-2010”. The Programme was prepared in one year by experts and officials from all fields of science and future activities are set out in the Action Plan of this Programme. The new strategy for improvement of R&D defined in this document suggests an integrated approach to research activities characterized by necessity and quality. Increasing funding for R&D projects and for fellowships for young researchers is one of the priorities together with increased regional and international cooperation. Additionally, a definition of the national priorities in the R&D sector as well as an improved intergovernmental coordination between the ministries is emphasized as main concerns for the future development of the country. This strategy for the future science policy also includes a definition of criteria for supporting R&D, establishing a new peer evaluation procedure.

As one of the strategic objectives, five potential centres of excellence have been identified in the country based on their scientific results: Institute of Chemistry at the Faculty of Natural Sciences and Mathematics; Research Centre for Genetic Engineering and Biotechnology at the Macedonian Academy of Sciences and Arts; Nephrology Clinic at the Faculty of Medicine; Research Centre for Energy, Informatics and Material Science at the Macedonian Academy of Sciences and Arts and the Institute for Earthquake Engineering and Engineering Seismology. They are recognized not only in the country, but also internationally due to their publications, citations and international cooperation.

During the 2006, the Ministry has promoted and stimulated international cooperation in all fields of scientific research and technological development. This strategy has produced a substantial increase in international scientific cooperation with many countries, especially with the European Union Member States. The scientific cooperation has been realized through the Framework Programmes for RTD, COST, NATO, UNESCO, IAEA and JICA. The increased participation

of the Macedonian scientists in the 6th Framework Programme should be especially highlighted. According to our data, more than 50 projects with our scientists have been approved, which is 4 times more than in the 5th Framework Programme. The Macedonian Government officially stated the willingness and readiness for improvement of science and research in the country and a full participation in the 7th Framework Programme. The Department of Science at the Ministry of Education and Science is an active participant in two large and important multilateral projects in the 6th Framework Programme (SEE-ERA.NET and ERA-WEST-BALKAN+), which enables a wider incorporation of Macedonia in European S&T activities. The participation of our scientists in the COST Program also significantly increased from 5 Actions in 2003 to 25 Actions in 2006.

The Department of Science creates European oriented science policy and, in every way, promotes, stimulates and assists in establishing international cooperation. Three years ago, there was bilateral project cooperation with Slovenia and Germany only. Then, this kind of cooperation was for the first time established with Bulgaria, Serbia, Croatia, France, Albania, the Russian Federation, Japan and China with more than a hundred bilateral projects. In the near future, cooperation with the USA, Israel, Austria and Spain will begin as well. Furthermore, there is an open call for joint project proposals with institutions from countries with which Macedonia has not signed agreements for scientific cooperation yet.

All these activities are intended to facilitate the incorporation of Macedonia in the European activities in the scientific research area, which has been recognized in the opinion of the European Commission for the status of this sector in the country, stating that in the fields of Science and Research the country should not have major difficulties in applying the *acquis* in the medium term.

Finally, the necessity of full understanding, coordination and support between the science policy makers and other decision makers should be emphasized because it is the only way for efficient and productive improvement of the scientific research and technological development of the country.

3.1. National Research Priorities

The Ministry of Education and Science has defined and set the following R&D priorities:

- Sustainable development;
- Water resources and management;
- Energy;
- New materials;
- Environment;
- Information and communication technologies;
- Health;
- Biotechnology;
- Nanotechnology
- High-quality food production;
- Earth science and engineering.

Special attention will be paid to overcoming problems concerning modernization of the existing R&D infrastructure as well as building a new one.

3.2. Development of the strategy for industrial policy in the Republic of Macedonia

Key drivers of Macedonian industry development are the following:

- Future of Macedonian industry will depend on enhanced collaboration between business and academia/research for knowledge creation and innovation.
- Macedonian industry will need better technology and will have to adopt high-quality standards in order to create high-value added products and services. Strategic industries will have to be defined.
- SME development and entrepreneurship will depend upon concrete governmental measures for elimination of administrative barriers.
- Relevance of education and importance of knowledge for industry development should be intensively promoted.
- Macedonia should strive for regulation compatible with EU (especially in the area of technology imports, quality, prices and other terms of trade).

- Exploitation and financing of new technologies should be stimulated (also by establishment of coordinative body for new technologies support).
- Public-Private Partnership (PPP) should be enhanced (learning PPP from experiences in other countries).
- Renewable energy production will have to be stimulated by supportive regulation and proactive policy measures.
- Better financing for SMEs (loans, venture capital etc.) is a prerequisite for SME development.
- Innovation support institutions will have to be developed and they will have an important role for innovation development.

Investment enhancement will have to be based on equal treatment between domestic and foreign investors. The Inter-ministerial working group, business sector representatives and academia members have created a **shared vision** of industry development. It has been jointly agreed that the **vision of Macedonian industry will be based on high value added products and the development of new capacities in research and production of sustainable, organic and specialized high-tech products and services** (i.e. organic wine and foods, eco-steel, specialized electronic parts, renewable energy production, construction, medical equipment, authentic tourism etc.).

The pro-active industrial policy as a set of governmental measures will support Macedonian industry in such way that it will be able to **grow traditional (niche oriented) as well as new high tech sustainable industries around the renewable energy field, and combining information technology and other advanced services – building on knowledge networks established through the world.**

Macedonian industrial policy will strive to enhance new, applicable research and innovation methods in education and industry. Business and research will be stimulated for interaction and collaboration (clustering). Knowledge for development will be possible due to the **increased public and private investment in research and development and engagement of talented people** (approaching towards Lisbon Strategy goals).

The Macedonian new industry potential will be possible due to the

ability of key development stakeholders (political, business and research/academia leaders) to reach consensus and decide for value-added, internationally oriented industry based on dynamic mix of sustainable and authentic industries, “clean-tech” manufacturing, and innovative service industries that create jobs and a rising standard of living for all its people.

4. Republic of Macedonian security related R&D scene

Macedonia’s accession to the North Atlantic Treaty Organization (NATO) requires restructuring as well as modernization of the Macedonian Armed Forces in compliance with the NATO standards. Along with the outlined plan for the modernization of the Armed Forces within a timeframe that spans from 2004-2013 there is also a separate Strategic Defence Review (SDR). Its main task is to perform a thorough reassessment of the state of the armed forces and to outline the guidelines for their long-term development in conformity with the new security environment and the available defence resources.

The ***upgrading of the communication/information systems will be one of the main focuses*** of the campaign, as well as ***strengthening the operative capabilities of the deployable forces***. The modernization of the armament/equipment of the Army, and Aviation WING, Development of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance Systems (C4ISR) is another priority.

For the sake of development of the structure and capabilities, defence assumptions should be adopted most urgently, which relate to operational capability, readiness, scale of effort and concurrency for operations. The development of the structure of forces and capabilities should be in accordance with the requirements and structure of forces and capabilities established in this political framework, especially the priorities, missions of defence and tasks of Macedonian army.

The ***Strategy is adopted*** for the management of defence at all levels of decision making, as well as in the areas that relate to personnel (including also education of civilian experts), its professionalisation, qualifications, career with equal opportunities for all, as well as adequate ethnic representation in the Macedonian army, training and

education, including the civilian personnel in the ministry of defence, interoperability, modernization and procurement, logistics, standardization, as well as development of strategies for improvement and interoperability of the intelligence capabilities and crisis management.

The current Strategic Defence Review works on the basis not of a nonexistent conventional threat, but of a **considerable internal terrorist and insurgent threat**. Cross-border criminal activity should figure prominently in these calculations, as should plans to stop trafficking and **organized crime** networks from further eroding the authority of the Macedonian state. The lingering **ethnic tension** signals to NATO that Republic of Macedonia still requires significant external assistance, from both Europe and the United States, in order to embrace its original reform policies and goals and that continued international engagement and the bi-ethnic composition of the ruling coalition in Republic of Macedonia will help to reduce the threat of a return to the open conflict experienced in 2001. However, the acknowledgment of the achieved results accomplishing all NATO membership criteria (including political stability and contribution to regional and worldwide stability) given to Republic of Macedonia during NATO Summit in Bucharest 2008 presents Republic of Macedonia in an another light - as more contributing country than an user of foreign assistance.

Achieving NATO interoperability and contributing to the organization's future operations are priority goals for Republic of Macedonia, even though currently the ARM's capability is limited in both of these areas. Still, Republic of Macedonia now contribute a motorized infantry company, a medical squad, an aviation detachment with two utility helicopters, and an engineering platoon for Multinational Peace Force South-East Europe (MPFSEE)/ Southeast European Brigade (SEEBRIG).

The Republic of Macedonia is not "giant" manufacturer of armament and military equipment and therefore the Republic of Macedonia is not a big exporter of defence technologies. There are only two factories producing some military equipment and armament ("Suvenir" – producing munitions and repair of small weapons and "Euro-composit"- producing equipment for personal protection as helmets and bulletproof personal equipment) and one factory for repairing and

maintenance of the military equipment and armament factory - “MZT Specijalni vozila” (factory that repairs the artillery armament and light combat vehicles). At the beginning of 2005 the factory “Suvenir” was bought by “Olympicos Industry”. The restarting of the production is expected followed by extending of the small ammunition production program- appropriate to NATO standards. In the next period the factory “Eurocomposit” should be sold and its privatization is to be expected in the near future. According the factual situation there is no strict and designed concept for defence industry transformation.

According to the Production and Turnover of Armament and Military Equipment Law (published on 15 July, 2002), articles 9 and 10, D & R of new armament and military equipment technologies is committed under the base of a D & R program which is adopted by the Government of the R Macedonia on the proposal by the Ministry of Economy in cooperation with the Ministries of Defence and Interior. The D & R of the new armament and military equipment can be committed by public science institutions, enterprises producing armament and military equipment and other science institutions that are dealing with science – research activities, in accordance to the existing laws. The program is financed from the budget of the Republic of Macedonia. The Ministry of Defence doesn’t possess science – research and producing capacities. Therefore the Ministry of Defence for its own needs is contracting products and services with the factories that are part of the Economy system, eligible and verified for this purpose. Within the Ministry of Economy exists a Sector for Special Production that is the pillar body for coordination of R & D activities. In the budget of MoD/Sector for Logistic – Section for R & D of the weapons and military equipment is planned an amount of 50 000 Euros per year for R & D. The R & D issue is only generally considered within the 5th part of the SDR – Equipment and Modernization Plan.

5. Actors and coordination of security related R&D

Ministry of Defence R&D capacities- The function of the Section for R&D (3 persons manned only) of the production of weapons and military equipment in the frame of the Sector for Logistic in the MoD is: informa-

tive support to the leading authorities in the MoD in the creating of the policy for equipping of the MoD by weapon and military equipment from the domestic industrial resources, cooperation with the Sector for Special Production in the Ministry of Economy by overseeing the situation of the domestic industrial capacities and preparation of the relevant legal documents, preparing the regular analyses for technical – technological capacities and regular analyses for the personal management capacities of the production subjects that are dealing with R&D of the production of weapons and military equipment.

The Commission for Special Production oversees the situation and the development of the production of weapons and military equipment in peace; development and preparation of the basic and additional capacities intended for production of weapons and military equipment, as well as production of medical materials and other products, equipment and services for the needs of the defence.

Within the Ministry of Economy - Sector for Special Production is the focal point dealing with special production and plays the coordination role for other institutions and agencies (Ministries).

The main own innovation potential of military science development and R&D policy of the MoD and General Staff are the Military academy, the Military Hospital and other institutions in the Army. Material and financial support is from the MoD budget funds. Responsible institution in MoD (Department for training and education and R&D policy) should make plans and programs and should held A Law for R&D policy within the Army.

The Military Academy of the Republic of Macedonia was established by Law which is in accordance with the Law on Higher Education and the Law on Research Work in the Republic of Macedonia.

The Military Academy was verified by the Ministry of Education and Science as tertiary level educational and research institution, which gives it the same status as other faculties and makes it part of the educational system of the Republic of Macedonia. The degrees issued by the Military Academy are valid in the country and they give officers an equal education status as other graduates from civilian universities. The Military Academy is the only tertiary-level military educational institution in the

Republic of Macedonia. Its main task is to educate, train and provide further development for officer personnel for ARM, and to engage them in research in the field of defence in accordance with the law.

Section for R&D of the production of weapons and military equipment, in the frame of the Sector for Logistic in the MoD, provides: informative support to the leading authorities in the MoD in the creating of the policy for equipping of the MoD by weapon and military equipment from the domestic industrial resources, cooperation with the Sector for Special Production in the Ministry of Economy by overseeing the situation of the domestic industrial capacities and preparation of the relevant legal documents, preparing the regular analyses for technical – technological capacities and regular analyses for the personal management capacities of the production subjects that are dealing with R&D of the production of weapons and military equipment.

On the 1st of July 2003 the Law on **the Police Academy** came into effect. This law provides the Police Academy with a leading role concerning research and education in the field of policing and other areas of security.

Police academy (now is transformed as faculty of security from St. Klement Ohridski University - Bitola) want to enhance its educational role by delivering basic and further education of national and international acknowledged quality and by the evaluation, dissemination, production and application of scientific knowledge in the field of policing and other areas of security. Police academy want to become a **centre of excellence** in our part of the world as well as belonging to the top five Police Academies in Europe. It considers itself responsible for remaining up-to-date in the field of research and education. Its police education is recognized on national and international level. This means that it will meet national and international quality standards. Its diplomas will be recognized all over Europe and they will facilitate participation in studies abroad. Being a centre of excellence will provide the Macedonian police and the other agencies in the field of security with state-of-the-art expertise. In this way we can serve the police and the other agencies in our field of security of our country in the best way.

6. Future steps – by priorities

6.1 Investments against possible security threats

Having in mind the national and international defence missions, tasks, strategic goals and functions, the asymmetric character of most possible security threats (facing with terrorist groups attacks) especially viewed through the light of casualties analyze from the conflict 2001 in Macedonian, where more than 80% were spawned by anti transport vehicles mine attacks, it is obvious that first priority of the security and military R&D should be obtaining **highest level of combat/transport vehicles mine attacks protection**. Other priorities in this area should be T72 tanks modernization and supplying of transport aircrafts.

6.1.1 In pursuit of mission 1.1.1 subtask B.4- -defence and protection of the territorial integrity and independence of the Republic of Macedonia versus Control of the Macedonia Airspace, creating the **optimal development antiaircraft protection programs** would be second priority. In this regard a suitable regional ASOC system development program will be much appreciated.

6.1.2. Concerning the counterterrorism the development **upgrading programs for the communication/information systems should be one of the main focuses**, especially in correlation to the Development of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance Systems (C4ISR) is another priority. Taking into consideration that the current Strategic Defence Review works on the basis of a **considerable internal terrorist and insurgent threat** and that cross-border criminal activity should figure prominently in these calculations, development of appropriate **engineer equipment and special vehicles upgrading programs** are welcomed as well as programs for soldier personal higher protection (for example within a cooperation with EUROINVEST company)

6.1.3. Having in mind that in the long term we are not expecting any conventional one, in addition to the above said, the visions, plans, force structures and manner of their functioning should incorporate elements and contents of what is today called crises management and early warn-

ing on potential threats. To that end, we particularly have to improve the intelligence capabilities and possibilities of compatible and efficient information sharing and coordination of the activities with the all other subsystems of the R. Macedonia, as well as with our neighbours, countries in the region, NATO and the international community.

The Republic of Macedonia continues the development of the national capabilities for the fight against terrorism and capacities for support of and participation in the joint activities of NATO and its Partners, as well as with the other international organizations. The security agencies in the country (the Directorate for Security and Counterintelligence at the Ministry of the Interior, the Military Service for Security and Intelligence at the Ministry of the Defence and the Intelligence Agency) maintain mutual coordination and cooperation at an exceptionally high level. Prime minister and the president of Republic of Macedonia are regularly inform on the security situation in the country and in the region through joint intelligence information from the security services.

Security agencies of the Republic of Macedonia maintain continues and good cooperation with NOS (NATO Office for Security), ILU (Intelligence Liaison Units) and TTIU (Terrorist Threat Intelligence Unit). On several occasions in course of 2007 direct communications has been established and Joint meetings have been held.

Aiming at creating a single and integrated national security system, upon the initiative of the Ministry of the Interior, and an inter-department Working Group, compose of representatives of the competent ministries, agencies and services for intelligence and counterintelligence, for reform of the security system was establish.

In capability category of intelligence collection and reconnaissance, procurement of the Long range Surveillance Vehicles, Hide performance Radar Equipments, Unmanned Aerial Vehicles and specific Warfare Equipment will be made and they are to be organically combined in the mix ISR Units of the Army intelligence branch.

6.2. Cooperation with EU and NATO R&D institutions

Having in mind the Macedonian aspiration to be full-fledged member of NATO and EU and to promote collective approach to the security and stability as comparatively considered superior and more

appropriate versus clear national approach, especially seen in the light of coping with asymmetric threats - such as international terrorism, for Republic of Macedonia would be very beneficial to continue with following and incorporating its own R&D capacities within NATO and EU R&D structure, programs and organization (NATO Program for Security Through Science, NATO Research and Technology Organization, EDA and EU R&D area with EU Framework Programs)

6.3. Education system improving

Concerning the threats coming from structural violence especially potential internal ***ethnic tension*** and low level of R&D oriented education it is more than needed to strengthen the governmental coordination with relevant IO's (OSCE, EU, NATO, US resident missions) through development of common (governmental and IO supported) confidence building focused programs¹³.

6.3.1. Development of programs for better and more qualitative R&D oriented ***education*** comprising as much as possible of the school population.

6.3.1.1. Increasing the awareness and relevance of education and importance of knowledge for industry development should be intensively promoted.

6.3.1.2. Improving the education and science system in order to tackle shortage in the supply of qualified labour, to improve the firms' access to high qualified personnel, including vocational and on-the-job training and to provide a public research base as a partner in innovation projects.

6.3.2. The lack of enough traditional produced energy is more and more obvious and in the future this lack can spawn instability and security threats. In order timely to take relevant and appropriate measures it is necessary a development of renewable and alternative energy production programs - to be stimulated by supportive regulation and proactive policy measures.

¹³ For example OSCE Spill-over mission (in Skopje) budget for 2007 was around 10 Mil EURO. One of five sections within structure of this mission is focused on confidence building.

6.4. *Government (state) institutions versus privates companies*

- Improving framework conditions for innovation, notably through simplifying the tax system and reducing the tax burden for firms, and by diminishing bureaucratic procedures that may inhibit innovation and the start-up of new enterprises.
- Promoting innovation activities in firms through financial aid. Subsidies can be delivered via four channels: R&D grants for research in high-tech areas, R&D grants for co-operative research, financial support for innovation projects in technology-oriented R&D provided either through loans or venture capital and technology consulting services and the provision of a techno-scientific and informational infrastructure for innovative enterprises.
- Establishment of Inter-ministerial and private companies working groups,
- Establishment of new technology transfer centres in a view of more efficient integration of research and business entities,
- Providing favourable working conditions for the research entities with unacceptable conditions.
- Stimulation of the promoting new research and development units within the economy,
- Recommendations for increasing knowledge transfer between universities and industries,
- In pursuit of aspects of security and industrial policy - the preservation of core capabilities, the problems relating to military equipment and dual use equipment, the preservation of technology and jobs must hereby all be taken into account

6.4.1. The ***research work conducted by government-funded institutes*** is of particular importance. In addition to the available civilian research and its results that are to be used for defence technology these institutes have to accomplish the following central tasks:

- to provide the scientific and technological know-how for intelligent and economical equipment decisions;
- to offer new technological solutions and to realize the relevance of new technologies for the armed forces' capabilities;

- to develop new generic (sub-)system concepts;
- to work out contributions for a national- relevant international NATO/EU research and technology basis and for the ability for cooperation;
- to participate in maintaining a defence-related competence;
- to research in the area of the *Catalisators and electrode structure for ecological clean electromechanical energy sources with hard polimery electrolite*, bilateral project funded by the Ministry of Science of the RM and The institute for electrochemistry at the Bulgarian Academy of Science, continuing with work during 2008;
- to research in the area of the *Unstability and nature law at the rising up of the morfology forms at the electrochemical systems which are far from stability*, bilateral project funded by the Ministry of Science of the RM and The institute for phisical chemistry at the Bulgarian Academy of Science, continuing with work during 2008;
- to study *the morphology of the metal deposits with electrorafining in modiflicated conditions*, project funded by the Ministry of Science of the RM, 2003-2006
- to provide the system for researching and following the chemical stability of pressured explosive materia – fusses, project funded by the Ministry of Defence of the RM, from 2006 and during 2008.

6.5. Funds

As it is elaborated above, concerned by the growing capabilities gap between Europe and the United States, the 2002 Barcelona European Council set the goal of raising overall research investment in the **EU** from 1.9% of GDP to **around 3%** by 2010. Nearly all Member States have set targets, which – if met – would bring research investment in the EU to 2.6% by 2010. The same trend exists in **NATO** frame where many European leaders have already taken steps to increase their defence budgets. France, Norway, Portugal, and the United Kingdom have submitted budgets with **a boost in defence spending**, ranging from 1.2 percent in the United Kingdom to 8.2 percent in France (here especially increasing the level of funds dedicated to R&D - near **to 2%**)

From the another side a short overview given above within item 1.5

depicts the low level of financial support (**0.44%** from the GDP) as well as even low level of consideration of using developed R&D capacities advantages within the industrial process (military/civilian) in Macedonia. A proper way ahead could be increasing of national (governmental) funds dedicated on R&D capacities, especially in the industrial process, based on the priorities mentioned in this item or a consolidated version of these main priorities appropriate to national industry (state or private sector), but not limited only on the relying on these funds. It will be great advantage to use also the IO, NGO, multilateral cooperation projects and bilateral cooperation programs funds for this purpose i.e. supporting the industrial R&D projects as it is case with some agricultural projects, electrical power and water supply projects, clean environment (ecological) and communities confidence building projects etc. It is to convince the projects allocation funds decision makers on the benefit of some industrial R&D and technological development projects.

7. Perspectives and ideas for change of the R&D National policies for the Republic Macedonia

In the field of R&D in the Republic of Macedonia, the *main priorities* are as follows:

- Further development of the academic research network,
- Renovation of the research equipment,
- Stimulation of the promoting new research and development units within the economy,
- Systematic and continuous supply of foreign reference literature and providing access to electronic scientific data bases,
- Upgrading the library information system,
- Strengthening the present technology development capacities,
- Establishment of new technology transfer centres in a view of more efficient integration of research and business entities,
- Providing favourable working conditions for the research entities with unacceptable conditions.
- Improving framework conditions for innovation, notably through simplifying the tax system and reducing the tax burden for firms, and by diminishing bureaucratic procedures that

- may inhibit innovation and the start-up of new enterprises.
- Improving the education and science system in order to tackle shortage in the supply of qualified labour, to improve the firms' access to high qualified personnel, including vocational and on-the-job training and to provide a public research base as a partner in innovation projects.
 - Promoting innovation activities in firms through financial aid. Subsidies are delivered via four channels: i. R&D grants for research in high-tech areas (esp. through the thematic programs of the Science institutions in the Republic of Macedonia); ii. R&D grants for co-operative research by SMEs; iii. financial support for innovation projects in technology-oriented SMEs provided either through loans or venture capital; iv. technology consulting services and the provision of a techno-scientific and informational infrastructure for innovative enterprises.
 - Aspects of security and industrial policy, the preservation of core Macedonian capabilities, the problems relating to SMEs and dual use, the preservation of technology and jobs in Macedonia must hereby all be taken into account

Macedonia aims at the participation of the institutes, where it is possible and useful, for they can act as competent and integrative links between the civilian and military levels of security research, even more so as this subject will become increasingly important in the Commission's future framework programs for research.

A short overview given above within item 4.3 depicts the low level of financial support as well as even low level of consideration of using developed R&D capacities advantages within the industrial process (military/civilian). A proper way ahead could be increasing of national (governmental) funds dedicated on R&D capacities, especially in the industrial process, based on the priorities mentioned in item 8 or a consolidated version of these main priorities appropriate to national industry (state or private sector), but not limited only on the relying on these funds. It will be great advantage to use also the IO, NGO, multilateral cooperation projects and bilateral cooperation programs funds for this purpose i.e. supporting the industrial R&D projects as it is case with some agricultural projects,

electrical power and water supply projects, clean environment (ecological) and communities confidence building projects. etc. It is to convince the projects allocation funds decision makers on the benefit of some industrial R&D and technological development projects.

7.1. Perspectives

The DG will continue to manage the Framework Programmes, which will remain a central policy tool. But while these programmes have to date mainly sought to bring about synergies in European science by sponsoring trans-national collaboration and mobility, we will need to add new activities. We envisage competition-based European funding for fundamental research, European decision-making about the development of major facilities, and large-scale technological research projects undertaken through public-private partnership.

The overall results of the consultation reveal a strong stakeholder support for the ERA vision, and the six specific ERA dimensions. Knowledge sharing is coming out on top and it is the area in which actions is most required at regional level. It appeared that forthcoming action at EU level will have to aim at the realisation of a single labour market for researchers. Correspondingly, five key communications have been planned (in the following chronological order):

1. Joint Programming of Research for more strategic and ***better-structured joint programmes*** and common calls for projects as of ***2010***.
2. A communication on measures ***to increase researcher mobility***, e.g. by a ‘European Researchers’ passport’;
3. A legal framework for pan-European research (based on ***art. 171 EU Treaty***) to facilitate the construction and operation of new consortia;
4. A European strategy for enhanced and coherent international science and technology cooperation;
5. ***Recommendations for increasing knowledge transfer between universities and industries.***

**ROLE OF THE CENTER OF OPERATIONAL ANALYSIS
IN INTEGRATION OF SCIENCE, INDUSTRY,
GOVERNMENT CAPACITY TO SUPPORT
INTEGRATED SECURITY SECTOR IN BULGARIA**

Dr. Velizar Shalamanov

Senior Research Fellow

Institute for Parallel Processing – Bulgarian Academy of Sciences

Dr. Georgi Penchev

Senior Assistant Professor

Department “National and Regional Security”

University of National and World Economy - Sofia

Mrs. Irena Nikolova

Research Fellow

Space Research Institute – Bulgarian Academy of Sciences

Introduction

For about 60 years NATO was and is still the cornerstone of the European Security. At the same time with the New Security Concept of 1999 NATO and EU countries accepted that there will be ESDI within NATO. Currently after more than 10 years NATO launched very transparent and inclusive process of consultation for the Security Concept to embrace new challenges as climate change, energy security, cyber security, dealing with piracy, etc. – all the areas where more cooperation with the EU is expected. After political framework cooperation will be possible on the level of involved agencies on both sides to mention NC3A and EDA for example.

The adoption of EU Common Foreign and Security Policy (CFSP) and European Defence and Security Policy (ESDP) resulted from a long lasting debate on dimensions and role of European security. The roots of these policies can be found even in 1948 and Treaty of Brussels. The idea of self-defence treaty passes through steps as Plan Fouchet (1959-1962), European Political Cooperation (1970), European Defence Cooperation and was subject of many discussions. After 1999 the development of new security and defence policy was fostered by many activities among them Petersberg Task, Councils in St. Malo and Cologne, Helsinki Headline Goal and adoption of the European Capability Plan (2001). Some adopted objectives and policies were proven too ambitious from political, military and economic point of view. Many researchers and politicians were concerned with the solution of imminence issues which would appear in relation between national and supranational (EU) level. A lot of these issues already are less or more resolved by adoption of the EU Security Strategy "A New Europe in the Better World" and the Lisbon Treaty.

The implementation of Security Strategy after 2004 and recent organisational developments on EU level impose need of certain action on national level and Bulgarian scientific organisations can play significant role in such activities helping to the administration and to the business in integration of security sector both to national and EU structures.

Especially in the case of Bulgaria there are additional dimensions of change – first is the long and very slow emancipation of Bulgarian defence industry from the dominance of non-existent former Soviet Union and respective influence on defence modernization on one side and at the same time greater influence of US in the region, to mention only FMF and joint military facilities.

The aim of this article is to present both the challenges of Integrated Security Sector as result of EU Comprehensive Approach to Security / NATO comprehensive Approach to Crisis Management (Bucharest Summit) and Bulgarian academic community answer. The community builds capacity for integrated approach to R&D and E&T in security through organisational set-up of two Centres of Excellence

in NATO Projects SfP-981149 “Operations Research for Transformation” and SfP-982063 “Management of Security Related R&D in Support of Defence Industrial Transformation”. The analysis will be focused on main developments in EU, NATO and Bulgaria, as well as the scientific, R&D and design projects supporting the processes of the transformation. On this ground the conclusions will be drawn for the role of the CoEs and the academia as a whole in the development and implementation of the Integrated Security Sector concept. The future actions will be purposed for better and closer participation of Bulgarian institutions in EU and NATO structures related to security/defence research and development/education and training.

Security sector transformation

In the last few years the political-military situation in the world has changed dramatically. The confrontation between the East and the West has given way to partnership. The idea for the creation of a common security and defence policy has become an important positive tendency.

Security Sector Reform (SSR) – or security system reform as it is often referred to by developmental actors – is a concept that has gained increasing recognition from the international community. In assisting countries make the transition from conflict to sustainable development the United Nations (UN) engages in a wide range of SSR activities. Although the UN is only one of a number of international actors involved in this effort, by virtue of its mandate, legitimacy, early presence on the ground and experience, the UN has a crucial role to play in supporting SSR across the whole peace building spectrum. This is particularly true in cases where UN peacekeeping operations are deployed as part of a comprehensive, multidimensional assistance effort that includes political, security, humanitarian, development, rule of law and human rights components and which seeks to bring together all UN actors on the ground within a common approach.

Security sector reform is driven by the understanding that an affordable, effective and efficient security apparatus (i.e., one that is able to provide security and justice to the state and its people within a

framework of civilian oversight and democratic accountability) is needed to ensure sustainable development, democracy, peace and security. There is, however, no generally accepted definition of the security sector or what SSR entails, with different actors embracing broader or narrower understandings of this relatively new concept.¹⁴

Broader and more comprehensive approaches to post-conflict interventions have been developed by both the security and development communities. Such comprehensive and ‘joined-up’ approaches have enjoyed huge gains at the policy and planning levels, particularly in wider security policy areas such as Security Sector Reform (SSR). Integrated planning cells, joint assessment teams and missions, joint doctrine and cross-Government steering committees all represent mechanisms which have facilitated the broader approach to security and development work and between two fields which – in the past – rarely interacted at both the strategic planning and operational levels.

Despite the gains felt at the policy and programming levels, the way in which such programmes are managed on the ground – and evolved, monitored and measured – still requires much work. Due to the multi-faceted nature of SSR with complex challenges associated, there still exists a significant research gap exploring the broader management with issues related to inter-dependencies, sequencing, change, cross-impacts and contingent challenges of SSR interventions. Because the mainstay of research supporting SSR is undertaken primarily by specialists in the fields of conflict, development, political and global security studies, such management-related dilemmas for SSR specialists have not enjoyed deep investigation.

The sphere of security is difficult to assess, quickly changeable and with a high level of uncertainty. Addressing the risks, threats, but also, the opportunities forming this sphere of security requires a much higher level of coordination in the security sector, extremely accurate civic-military relations and integration of the different elements of a diversified sector of security into task forces for different types of operations.

Up to the beginning of the 90-s “security” was a synonym of “defence”. While today in most European countries security is firstly as-

¹⁴ The OECD DAC Handbook on Security System Reform (2007), <http://www.oecd.org/>

sociated to risks like: illegal migration, ethnic and religious conflicts, the proliferation of weapons of mass destruction and, of course, terrorism. These may also include effective prevention, mitigation and management of the consequences of natural disasters and industrial accidents. That is why security is no longer a purely military concern. Today it is also connected to the social-economic development. It is important that all elements of society become involved. In accordance to this the new demands towards security impose fundamental reforms of the national structures, investment models, systems for management, adoption and mass application of contemporary methods of operations research, system analysis and risk management. Without such an approach the conclusions and decisions based on them cannot be fully substantiated.

Security and defence, which are natural bases of the economy and social development, depend, and will more and more do so, on the creation, acquisition and use of knowledge in all its different forms. The new organisational models are born as the result of the new systems for education and the central role reserved for information.

An extremely important characteristic of the transformation of the security sector is the level of introduction of new technologies allowing joint actions concerning the concept for results-based operations. In order to deal with this question there must be tight cooperation in the sphere of scientific studies between the Ministry of Defence and the other departments from the security sector, the Bulgarian Academy of Science, the universities and the defence industry on national and international level (NATO, EU, USA etc.)

International cooperation in the sphere of science and technology helps to broaden the horizons for research in connection to the new requirements, for exchange of scientific practises and assists the international connection of the Bulgarian universities and institutes.

The transformation of the security sector is based on three main ideas:

- Orientation towards capability and results in operations;
- Improvement of the cooperation between all participants in the security sector;

- Connection to third parties to offer the service “security” to citizens.

The Integrated Security Sector

The integrated model of security is a relatively new concept after the terrorist attacks of September 11, 2001 in New York.

Current structure of the security sector to include different institutions with monopoly over use of force or information operations in support of use of force is mirroring the structure of well defined and separate operations of use of force / information support to use of force. At the same time nowadays security environment defines the need for complex crisis management operations where interagency, international, joint, private-public cooperation is essential. This reason drive integration in the security sector, where different institution keep their identity together with the opportunity to form combined interagency joint forces for specific complex operation with change of the mix of forces in different stage of operation or when moving from one to another operation in the same region.

Integrated security sector is not an organization, but concept for organization of institutions participating in this network in order to be able to work together; to support each other, reinforce each other when for every certain operation one institution has a lead according to the legal status of the operation. Integrated security sector requires an integrated management system and maintenance of individual elements.

The management of a complex system like the security sector is practically impossible without using modern information technology. Effective management requires access to information in the process of decision making on the part of those who need it (or have the right to do so). The existence of integrated and secure database is one of the most important conditions for effective management and control of the security sector

Still, the most important condition for good governance of the security sector is the presence of integrity in the sector. In this connection, 01 July 2008, NATO created a trust fund for good governance in

the institutions of defence, by agreement between Poland, Switzerland and Britain, signed by Deputy Secretary General of NATO. Therefore, change in the security sector at a cost, but intelligent and transparent governance model and will be grounds for the use of these good practices in other spheres of public power and to switch to small, wise and competent government. In this sense, the reforms in the security sector far exceed the importance in managing this area, as always so far from the changes in the security sector are influenced changes in the public sector.

The new technologies and tasks necessitate using new terms and technologies in the sphere of management, for example: structural change; change management; organizational development; reengineering of organisations and processes; portfolio management etc. This demands the construction of an effective model for the change management in the security sector, supported by the appropriate scientific research, which should in their turn be managed in a way that achieves results.

Every single change is an extremely complex process. There is no special pattern for making this change and there is no ready solution to the problem. The change in the strategies, processes, structure and culture can be achieved gradually, in the form of steps or radically, under the form of big jumps (transformations). In this respect we talk about evolutionary and revolutionary (transformational) models of change.

In contrast to the evolutionary models reengineering is based on the fundamental rethinking and the radical restructuring of the systems and processes and the use of the new informational technologies.

The change management in the security sector is a joint work between the different units of the security sector in direct cooperation with the scientific organisations and the business sector on a national and international level. It encompasses the organisation, methods and means, education for the support of the process of building a system of civil security as a core of an integrated security sector.

By using scientific-based methods and models for the management of processes and measuring results in the development of an in-

egrated security sector we can guarantee transparency, effectiveness and activities focusing on results.

Connecting element between the scientific sphere, the public sector and industry is creating a network of inter-disciplinary units, object-oriented, such as established under the project, financed by NATO "Security through Science" program, Centre of excellence in IPP-BAS and UNWE Sofia. These units are designed to build capacity of highly qualified people in various fields to work in the use of modeling, simulation and operational analysis in the security sector, combining the scientific and civil side of this issue, security sector reform. One practical test for capacity of these two centres was joint participation in EU TACOM SEE-2006 full-scale exercises with participation of 7 countries plus EU (MIC) and NATO (EADRCC) and UN (OCHA) as well as more than 10 ministries and agencies from Bulgaria.

EU, NATO, National Experience and Scientific Programmes for Security Sector Transformation

The process of adoption of the ESDP and afterwards organisational developments and set-up is not a single process of political-administration debate and efforts. The scientific support to the political and organisational processes is obvious. The discussions started after 1999 about EU Security Sector was supported by projects in Framework Programme (FP), oriented toward resolving the national-supranational level contradictions. As example the project in FP5 Bridging the Accountability Gap in European Security and Defence Policy, ESDP Democracy, started in 2000 was aimed in "in measuring, interpreting and enhancing democratic accountability across the EU policy area of security and defence"¹⁵.

The political-organisational developments started with Petersberg tasks (1992) continues through WEU-NATO European Security and Defence Identity, the Berlin plus agreement (1996), incorporation of WEU and Petersberg tasks into Amsterdam Treaty (1998), Cologne European Council and St. Malo meeting resulted in appointment of

¹⁵http://www.ulb.ac.be/iee/esdpdemocracy/2_theproject.htm

High Representative of the CFSP responsible for further progress on EU's CFSP and ESDP.

The political goals and activities on ESDP were supported by set-up of Helsinki Headline Goal and Helsinki Force Catalogue. The long-term nature of Helsinki Headline Goal forced EU to launch European Capabilities Action Plan (ECAP) at the Laeken Summit (2001) and to extend the Helsinki Goal in Headline Goal 2010 in 2004. The intentions to create integrative approach to defence capabilities creation, new competitive, transparent and integrated European defence market, cooperative armament acquisition and defence R&D, as well as emergency planning and crisis management resulted in set-up in 2004 of the European Defence Agency (EDA).

The above mentioned activities were supported by the R&D programmes and projects. The Group of Personalities in the field of Security Research was created. On 15 March 2004, The Group of Personalities (GOP) for Security Research presented its Report 'Research for a Secure Europe' describes the need for increased coordination in security research, outlining 12 recommendations for the future, establishment of a European Security Research Programme (ESRP) and formation of European Security Research Advisory Board (ESRAB). The new Preparatory Action on the enhancement of the European industrial potential in the field of Security Research (PASR) was established within the FP6 and new Security theme was introduced within FP7 (2007-2013).

The one of the most important results into the area of the security related research is the formation on 11 September 2007 of the European Security Research and Innovation Forum (ESRIF). The main objective of ESRIF is the development of a mid and long term Joint Security Research and Innovation Agenda that will link security research with security policy making and its implementation¹⁶.

Transformation and integration of the Security Sector were also amongst one of the most important themes in NATO after the 2001. The agenda of the Science Committee was changed according to the new trends and global security issues. The supporting scientific activi-

¹⁶<http://www.esrif.eu/objectives.html>

ties were focused mainly on SfP projects through “Security Through Science” Program. The capabilities development and R&D and E&T activities were supported by respective projects and researches through Research Technology Organisations (RTO) panels and working groups. The role of the Centres of Excellence set-up by NATO Allied Command Transformation and working into the network TRANS-NET is also significant in research and training activities.

The one of the biggest agencies in NATO – NC3A is a good example with its specific experience as a customer funded, strategy focused organization for transformation through C3 technologies. The NC3A's Sponsor Account Segment is serving as interface to the Agency shareholders and sponsors organisations. This interface is used both for set-up goals for the NC3A programmes and projects and for allocation of the resources which NC3A shares with other NATO agencies and organisations.

The Bulgarian experience in supporting Security Sector transformation and implementing the comprehensive security approach is not such coherent as in EU and NATO, but there are events and activities that should be mentioned as follows:

- In 1999 Interoperability Centre was established at Defense Staff College and later Advanced Defence Research Institute was created.
- During the 2002 Intergovernmental Expert Consultative Council was established between MoD, Bulgarian Academy of Sciences (BAS), University of National and World Economy (UNWE) and other universities, ministries and NGOs.
- The Centre for National Security and Defence Research was established in BAS in 2002.
- The Scientific Coordination Centre to General Service – Civil Protection was found in 2003.
- The Centre of excellence in Operational analyses (COA) was found in Institute for Parallel Processing, BAS (IPP-BAS) in 2004 within the framework of NATO project SfP-981149 Operations Research for Transformation.
- JTSAC-CS in IPP-BAS was established in 2005. The Centre is integrating case by case the activities of academia, industry and government.

- The CoE in Defence R&D Management was established in UNWE-Sofia within framework of the NATO project SfP-982063 Management of Security Related R&D in Support of Defence Industrial Transformation.
- National Military Simulation Centre “Charalitsa” was found in 2006 in order to provide modelling and simulation capabilities both to the planning and training processes in Bulgarian Armed Forces.

After the period of quantitative development of capabilities derived by projects, funded by NATO, EU, US and some non-coordinated national bodies it is time for review and consolidation of R&D, E&T, test, validation and verification facilities in Bulgaria, alongside new security strategy to be approved to the end of 2009 as the new reformists government committed itself. This process of consolidation could be based on National research program in security and defence, fully coordinated with EU and NATO programs in the area.

Expectations, the Future of EU Research and Innovation Agenda

Since EDA establishment in 2004 there are intentions to set-up the Comprehensive Capability Development Process, which has to systematically translate the EU security goals into programmes of the member-states. The ESRIF's WG 10 'Governance and coordination' supports ESRIF's opinion that Europe will need over the coming years to develop a Common Capability-Based Planning Process and possibly, ultimately a Joint Security Capability Plan. The Common Capability-Based Planning Process will be prepared by an “Independent Adequate Structure” populated by experts from agencies/institutions dealing with operational issues even through a constructive dialogue between that structure, public laboratories and industry, such as to translate capabilities in technologies and to facilitate prioritisation of the efforts. The JSCP has to get a political approval at the right level and a permanent organisational structure to update and maintain JSCP.

The proposed Governance structure by ESRIF WG 10 should act in accordance with the following principles:

- Central role for EU High Representative for European Security

- and Defence Policy and Common Foreign and Security Policy.
- Permanent structure should keep in close loop representatives of each stakeholder.
 - For each of the four missions, the coherence should be monitored between all actors of security research following ESRIA.
 - Stay in close contact with Technological and Industrial Base in a structured dialogue.
 - Use/take into account existing co-ordinations (regional, national or inter governmental) in some fields (as an example – in crisis management).
 - Separate operational co-ordination from governance co-ordination
 - Parallel implementation of capabilities and research and technology work.

In the meanwhile, public and private stakeholders alike, both at EU and national levels will need to proceed to systematic identification of available and required capabilities. In specific sectors, relevant agencies can play an important role.

Still the issue of closer cooperation between EU and NATO is open on the alliances level, but could be strongly motivated and supported by smaller countries in NATO and EU that simply can't allow themselves to have three tracks – one for EU, one for NATO and one for national needs. These countries face a security challenge that requires strong commitment of US as well, so this dimension is as additional motivation to integrate this fourth track as well in one comprehensive approach to security R&D.

Center of excellence in Operational analyses - IPP-BAS

The Centre of Excellence in Operational Analysis (CoE-OA) is founded in 2005 within the frameworks of the SFP 981149 project “Operations Research for Transformation”, Bulgarian Academy of Sciences and George C. Marshall Association - Bulgaria.¹⁷

CoE – OA is focused on development and adaptation of models for

¹⁷ Operations Research Support to Force and Operations Planning in the New Security Environment, SFP 981149, 2005-2007, <http://www.gcmarshall.bg/c4i/>

decision making support and CAX in the area of operations planning, force planning, C4 planning, acquisition planning for the larger security sector.

The main goals of the Centre are:

- To create capabilities for operations research and computer modelling and simulations in Bulgaria.
- To develop and transfer models and software for operational analyses and change management in Bulgaria.

The Software Library is a key component of the Information infrastructure of SfP981149. It is a collection of different types of software which are selected after careful planning and consideration of different alternatives, to create capabilities to perform the project specific tasks.

The software is divided in 3 categories:

System and Support Software

- Operating systems
- Backup and security solutions
- Different administrative tools and utilities

Applications

- Office packets
- Communication and coordination software
- Planning software
- Graphic & pre-publishing software

Project Specific

- Specific programs used to achieve the goals of the project. These include Integrated Development Environments (IDEs), specialized software for mathematical analysis or creation of system architectures, etc.

In CoE was developed the author's methodology for application use of modelling and simulation by computer-assisted exercises in which the application is developed using modelling and simulations, starting from the user's assessment of its requirements and how they

could be used in developing scenarios and simulation of events (war, peacekeeping operations, crisis operations, incidents occurred such as terrorist acts, etc.), documentation, support decision-making and analysis for participants from the computer exercise. Software package BEST (Basic Environment for Simulation and Training) was used in several projects since 2006 and officially presented and awarded in 2008 at BAIT EXPO-08.

Software is being developed in the Centre of excellence of operational analysis under the project EU TACOM SEE-2006¹⁸ which will enable us to plan and report expenses for crises management training (Fig. 1).

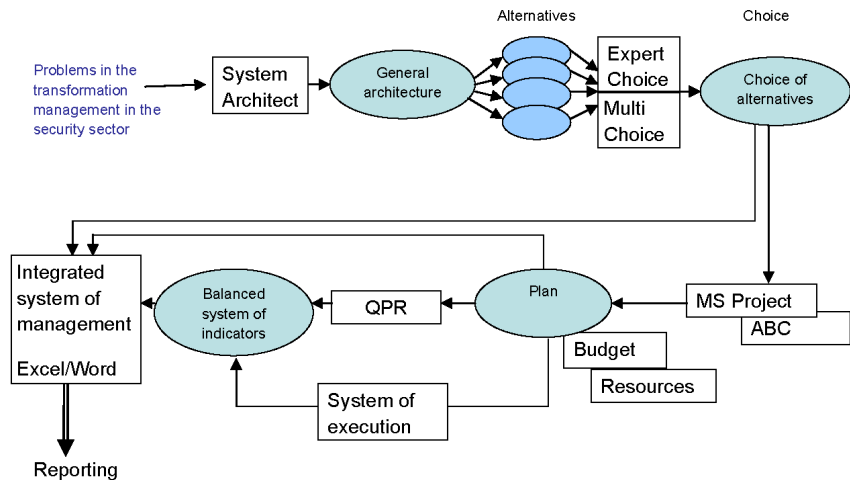


Fig. 1. Elements of the system for planning and reporting expenses for training

The implementation of results from scientific research projects can be achieved by forming an interdisciplinary centre in an academic institution – i.e. CoE.

¹⁸ National Computer Assisted and Field Exercise with International Participation for Large Scale Crises Situations 'European Union – Terrorist Act Consequences Management in South-East Europe (EU TACOM SEE-2006)', (<http://www.cp.government.bg/EU-TACOMSEE2006/EN/>)

Public Private Partnership is characterized by the following:

- Transparency, reporting, efficiency (competitive)
- Clear and accurate specifications, plans for execution, expenses, management
- Well- defined criteria for evaluation
- Coordination with the procedures for budgeting
- Understanding of the requirements by the end-users and organizations that provide financial support.

Under the project SfP 981149 and EU TACOM SEE-2006 a Public-private partnership was formed in the Centre of Excellence with ‘Electron progress’ joint-stock company, ‘Telesys’ Ltd, ‘Smart Media’ Ltd., ‘TV-MET’ Ltd. and other companies in order to achieve better results using the advantages that administration, academic institutes and business give.

Current efforts are aimed at realization of a project that will focus on the building of a business processes model of CoE /JTSAC (“as is” and “to be” status) that incorporates both CAX and OA applicable within NATO standards and Concept Development and Experimentation framework. This will be done through transfer of best practices from the Joint Warfare Centre in Stavanger and through modelling of the JTSAC core processes with the help of ARIS¹⁹. The elaborated model will be transferred to Albania (through the Institute for Democracy and Mediation to the Regional Defence College) and Macedonia (through the Ohrid Institute for Economic Strategies and International Affairs to the Crisis Management Centre). The goal of the transfer will be to support the NATO integration of these two neighbouring countries in order to strengthen the belt from Adriatic to Black Sea and its further extension later to Caspian Sea.

The methodology which will be used in the description of JSCATJTSAC business processes is based on the concept of process-management approach. By the formal description of work processes it is possible to clarify the persons in charge and to standardize the utilized documents and forms. On the basis of the modelled processes, it

¹⁹ ARIS is a business process modeling tool, which is developed by IDS Sheer, Germany.

is possible to automatically generate work procedures and job descriptions. The formal description also allows for the clarification of the interaction among the various organizational units or among different organizations. When the performed activity (process) is separated from the responsible person (organizational unit), it is easy to transfer good practices from one organization into another.

The Centre of Excellence in Defence R&D Management

The changes in political and economical structures and transition process in Bulgaria had almost destructed very close relations between defence industry, administration and science existed before 1990. NATO and EU membership, as well as regional cooperation initiatives within the Balkans require massive modernisation not only of the Armed Forces / security sector at large, but also of the way of doing business. The armament modernisation as well as integration of the security sector is not single-step or single-organisation endeavour. Thus restoration of close, integrated relationships between administration and the business is impossible without scientific expertise and support. In order to provide such kind of support and expertise both to the administration and business the CoE in Defence R&D Management was established in University of National and World Economy (UNWE) within the framework of the NATO SfP-982063 Management of Security Related R&D in Support of Defence Industrial Transformation.

The project SfP-982063 is an international cooperation activity intended to provide knowledge-sharing among the countries from the NATO, EU and Balkan region in the area of the Defence R&D. The project also has goal to foster the relations among administration, defence industry (and business as a whole) and academia on national level in order to support defence industry transformation and its integration to the national economy and to the Security Sector.

According to the SfP-982063 objectives the goals of the CoE were set-up. These goals are as follows:

- To accumulate and disseminate knowledge in the field of economics and management in defence and security, including models for

defence industrial transformation.

- To disseminate the best practices models and to set high standards in management of educational and scientific activities.
- To offer scientific and other information to government institutions and other organizations in Security Sector and to offer alternatives for development of contemporary regulations for R&D management.
- To cooperate in resolving the social issues caused by the defence industrial transformation.
- To develop cooperation with local and foreign partners in the field of economics and management of defence and security.²⁰

The CoE is intended to serve as international organisation body concentrating the expert potential, educational activities and information for technologies and leading management techniques applicable to Defence R&D management and to the defence industrial transformation. For implementation of this role the project teams developed four training packages, the videoconferencing system was installed and Database for the State of Scientific Research (DSSR) was developed.

The CoE has two rooms equipped with videoconferencing capabilities and appropriate hardware/software solution both for educational and research activities. The implemented into CoE EVO videoconferencing system is a world-wide researchers' videokonferencing network, providing both cost-saving solution and on-line space for collaborative research. The EVO was used during the first on-line training in CoE. To the first course participated all SfP-982063 members from Bulgaria, Romania, FYROM and Germany in four sessions, as well as officials and representatives from the defence industry. The training was conducted according to the four main training packages developed in CoE with the project teams from all participants of SfP-982063.

The CoE will keep and update information for research potential, ongoing and finished defence R&D projects through the DSSR, thus providing the background for research project, technology transfer and cooperation.

²⁰ CoE in Defence R&D Management web-site > Management http://coe.e-dnrs.org/?page_id=3

Knowledge Sharing and Management Support

Considering the capabilities of both Centres of Excellence – established in IPP-BAS and in UNWE – IT/knowledge dimensions can be identified as follows:

COA/JTSAC

- Library and documentation centre was established in order to collect the specialized literature and to document all COA's activities;
- Development, installation and support of Knowledge Management Portal²¹
- Development of Advanced Distance Learning courses
- Co-learning in VTC environment
- Computer Assisted eExercise environment
- Advanced Technology Demonstration environment
- After Action Report and Analysis & Lessons Learned (feedback mechanisms).

CoE in Defence R&D Management

- Development of Defence R&D training courses
- Database for Defence R&D potential and possible technology transfer
- Videoconferencing capabilities for distance learning and on-line collaboration through the EVO network

The two centres continue to develop and maintain and capabilities in management analyses and practice in their respective areas, as follows:

- Use of Business Process Modelling and various Capability Maturity Models for continuous improvement;
- Organizational flexibility based on Architectural Approach with Activity Based Costing, Roles Definition / Job Descriptions and Portfolio Project Management;

²¹ COA/JTSAC Knowledge Management Portal <http://www.caxbg.com/>

- Strategic Map and Balanced Score Cards Management.

During the period 2004-2009 at two centres introduced key initiatives for building of knowledge base, development of centres' infrastructure and training of the core staff. On this ground for the next period possible goals can be set-up as follows:

- Sustain and improve Business Process Excellence expertise and capacities;
- BAS level integration for COA/JTSAC and better co-ordination with CoE in Defence R&D Management and other CoEs;
- Set-up a formal interface with ministries and administration related to the security;
- Involvement in FP7 and future FP8, as well as integration in ESRIA implementation network;
- Introduce elements of ACT CoE Military Support to Civil Authorities in training courses;
- Create transferable CoE Model for the Balkan region.

The above mention strategic goals could be implemented during the period 2009-2013.

New wave of strategy focussed reforms announced in MoD and MoI as well as formal acceptance of the concept of integrated security sector by the leadership of new administration is providing very positive environment to exploit the capabilities developed during last 8-10 years under different NATO, EU, US and nationally funded projects in NAS and UNWE. Possible formal cooperation programs with EDA, NC3A and other agencies from EU and NATO with third party – BAS/UNWE, other universities and Bulgarian defense Industry Association could be very instrumental in achieving more with less and transformation of the security sector in knowledge based and integrated organization.

Conclusions

In conclusions taking in account the need for rapid actions for real integration of the Security Sector in Bulgaria the role of the academia and especially the CoEs can be made significant with respective organisational and educational activities.

In order to be more flexible Bulgarian Academy of Sciences has to develop capacity for sponsor account management for integrated security sector, industry, NATO (NC3A, RTO) and EU (EDA) as well as for regional partners (Adriatic – Caspian Seas). Such kind of action can decrease the bureaucracy and the starting time for new project related to security because of streamlined and reliable relations with sponsor organisations.

UNWE and BAS have to develop an education programme in Integrated Security Sector Development for Administration, Industry and partners from NATO, EU and SEE. This programme should create around BAS Security R&D Centre and UNWE Defence R&D Management Centre a network of research and education institutions of MoFA, MoD, MoI, MoES, SA NS, NIS, NPS, SC PCI and other elements of the integrated security sector.

On the national level should be created National security R&D/E&T program with Program Management Office acting as a coordinator and supervisor of the programme. In addition, the Consultative Committee on Science to the Security Council of the Prime Minister with section for technology transfer should be established in order to assure the political support. To assure the participation of the industry, NGOs and other organisation the Integrity Pact between BDIA, administration, BAS Security R&D Centre and UNWE's CoE in Defence Management should be signed with strong emphasis on transparency, accountability and effectiveness in result oriented security R&D and E&T.

Finally, all above mentioned activities should result in consolidated representation in NATO SC, NC3A, NATO RTO, NIAG, EDA, EU JRC and FP on theme “Security” of Bulgarian business, administration and academia.

COMPETENCES AND COMPETITIVE ADVANTAGES OF A DEFENCE INDUSTRIAL ENTERPRISE

Assoc. Prof. Tsvetan Tsvetkov, PhD

Department “National and Regional security”

University of National and World Economy, Sofia, Bulgaria

The main purpose of the operation of a business organization associates with the realization of sufficient profits in the long or short term. To expect that a defence industry enterprise will agree to participate in the R&D, this process must conform to its strategic objectives and in particular – to the goal of providing adequate income and competitiveness in the long term.

The purpose of this report is to present the logic of the relationship between the competencies of the company and its competitiveness and provide a model for competencies management.

Ensuring adequate return for the company can be provided in two ways: entering attractive industry and establishment of competitive advantages. It is believed that the defence industry is a sector with a high rate of profitability. One can identify many cases both all over the world and in the country of companies that realize higher profits. There is a number of reasons, however, why the defence industry as a whole can not be called an attractive industry in this country. Bulgarian defence industries lost a large part of their traditional markets. Existing technology partnership structures were destroyed. Ratings of the companies as excellent producers decreased. In industry there is a high level of competition. The ratio between the competing forces in the sector is not favourable for producers and can not provide them with sufficient market power.²² In this sense, the only way for the defence industrial enterprises to ensure achievement of their objectives

²² Porter, M., *Competitive Advantage. Creating and Sustaining Superior Performance*, New York, The Free Press, 1985, p. 5.

is to reach sufficiently high competitive advantages.

According to widespread ideas of M. Porter on providing competitive advantage is the development of an effective competitive strategy that provides offensive or defensive actions taken to protect the company's position against the five competitive forces. To ensure this, according to Porter are several possible approaches:²³

- Positioning of the company in the place, where its potential will provide the best protection from the existing set of competitive forces;
- Impact on the balance of forces through strategic action to improve the relative position of the company;
- Providing for changes in the factors underlying competitive forces, react to these changes and thus developing a strategy corresponding to the new competitive balance of forces before their competitors found it.

In recent years, significant diffusion gained so called “resource approach” to strategic management. The purpose of this approach is to create competitive advantages by development of strategy for use of unique portfolio of resources and competences of the enterprise. To ensure this, the enterprise must aim: comprehensive and deep understanding of its resources and competences, strategy establishment to use effectively its key strengths, efforts to develop its own resources and competences.

From this perspective, the achievement of sustainable competitive advantage is realized by the company with the following logic: (Fig. 1).

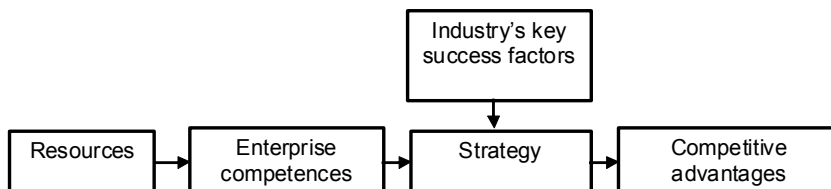


Fig. 1. Factors for achievement of sustainable competitive advantages

²³ Porter, M., *Competitive Strategy, Techniques for Analyzing Industries and Competitors*, quoted by Портер, М., *Конкурентная стратегия. Методика анализа отраслей и конкурентов*, Пер. с англ. М., Альпина Бизнес Букс, 2005, с. 67-68.

As is known, the company's resources can be tangible, intangible and human. For its part, tangible resources can be financial and physical. Intangible resources can be technological (intellectual property, innovation potential, research infrastructure, experts) as well as reputation of the enterprise. Human resources in themselves can have their abilities and competences, which, however, are not subject to review in this report. Here attention is focused on the competence of the organization, which may or may not provide sustainable competitive advantages.

Assessment of existence of resources for companies in the Bulgarian defence industry is not unequivocal. One could say that the availability of physical resources is sufficient. The companies have the necessary buildings, machinery, equipment, tools, appliances, etc. In many cases there are even greater quantities of the required, and capacity utilization rate is very low. Another question, however, is the quality of natural resources. They often have a high degree of physical wear and a low technological level.

Availability of financial resources can be assessed as inadequate. Own funds of companies are not sufficient. This is truth both for already privatized, and those which public participation. There are difficulties in accumulating external financial resources. As the financial and economic crisis in the world, banks are increasingly clamp procedure for granting loans even for current needs, and even more for technology development. Last but not least, this role has a high level of regulation of the banking sector in the country - one of the highest in Europe. Non-traditional sources like venture capital funds, leasing, specialized national and European funds are not sufficiently popular.²⁴

In the possession of intellectual property, Bulgarian industrial enterprises and enterprises of high-tech sectors lagging behind in respect of applications for protection and issued patents to the leading countries and to the average of the European Union. A similar situation is in respect of the industrial design objects.

²⁴ For more information on financial sources for innovations in the Bulgarian enterprises see: Innovation BG, 2008, ARC Fund, p. 80-86, <http://www.arc.online.bg/fileSrc.php?id=2446>

Innovation potential and research infrastructure - the possession of the defence industrial enterprises decreased significantly in recent years. Many companies that used to have their own research potential gradually lost it. Currently, most companies (with few exceptions) rely on external sources of research products that can be implemented.

It is believed that the enterprises of defence industry have highly qualified and experienced staff, compared with other industries. Nowadays, however, the industry is experiencing more and more acute need for qualified personnel. Initially it was felt the lack of skilled workers, but in the last 1 - 2 years it cleared that there is a shortage of senior engineering staff. Expectations are that the shortage of qualified staff will grow in the foreseeable future.

Since the mid 90-ies in the world scientific literature began to develop the idea of competencies and core competencies of the company. According to this idea, the main factor for the competitiveness of a company is the presence or absence of basic competencies. In this sense, sustainable competitiveness is associated not with the quality of the finished product or service that the company offers for sale, but whether it owns competences and core competences.

The substance of a competence is a combination of available resources, available technology and human knowledge and skills. Themselves competencies are unable to provide competitive advantages. Based on its competencies, the company carries out production of one or more products or services. For each product are needed one or more competencies. For this purpose, except the very existence of competencies, there must be a possibility to combine them in an optimal way with other resources of the company. Knowledge, skills and information necessary to optimize the combination of competence are also competence, which may be acquired and developed.

In literature there is no single opinion on which competencies of the company are "basic". In general, opinions were divided into two groups. Some authors believe that basic are those which are most crucial to its competitiveness. Others believe that basic competencies are unique worldwide. Because the companies that claim to uniqueness worldwide are not many in Bulgaria first opinion could be considered

as a working definition.

According to Prahalad and G. C. Hammen (authors who are considered the founders of the concept), the basic competencies are characterized by three features: first - they provide potential wide access to a variety of markets, second - they should be able to provide significant benefit to the consumer of the final product and the third - to be difficult to imitation by competitors.²⁵ These authors regarded the corporation as a set of competencies, products and businesses in the following way: Fig. 2.

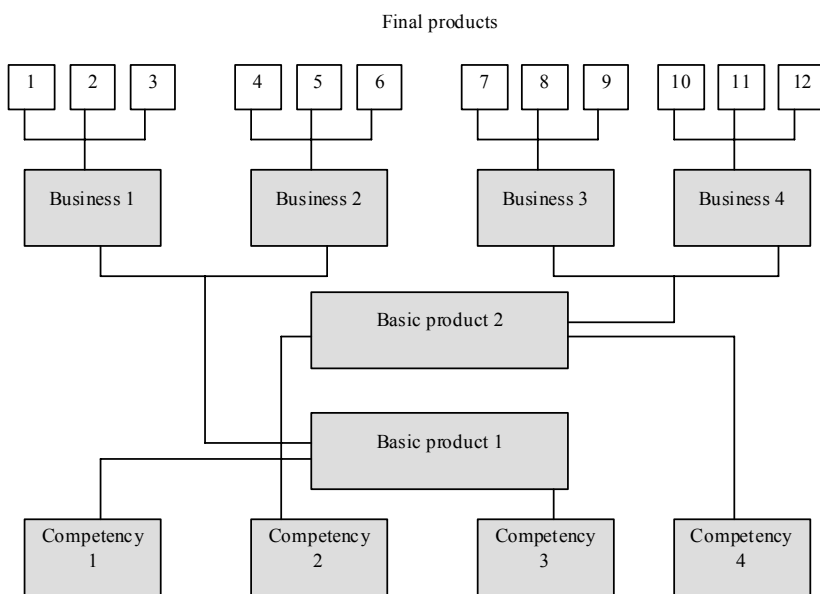


Fig. 2. Competencies, as roots of competitiveness

Source: Prahalad, C.K., G. Hamel, The Core Competence of the Corporation, Harvard Business Review, May-June 1990, p. 81.

²⁵ Prahalad, C.K., G. Hamel, 1990, The Core Competence of the Corporation, Harvard Business Review, May-June 1990, p. 83-84.

Each company has its own unique set of competencies and skills to combine them to achieve competitive advantage. In addition to offering their own products, the companies largely rely to find their place as subcontractors in the production of more complex products which are final for other manufacturers. Such a strategy is appropriate, taking into account the availability and necessity of competencies for successful competitive struggle.

The main purpose of a business organization is to ensure sufficient profitability for a given time horizon. Assessing the potential profitability of certain owned by the company resource can be made based on the following logical scheme: (Fig. 3)

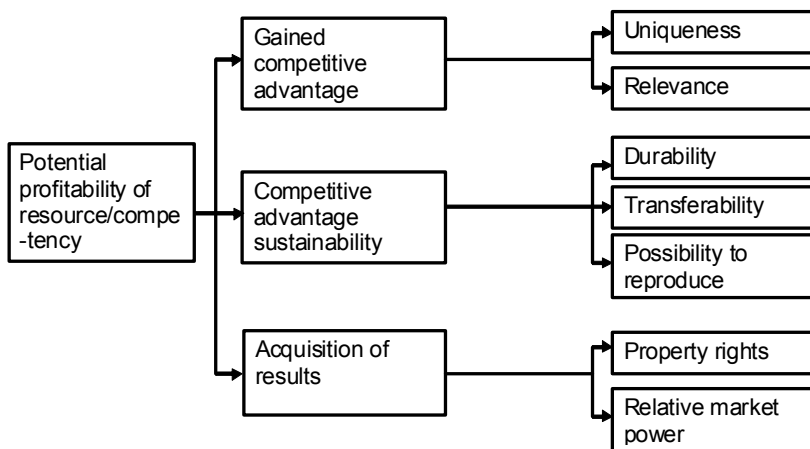


Fig. 3 Resources, competencies and profitability

Source: Grant, R., Contemporary Strategy Analysis, 5-th ed., Blackwell, цит. по Грант, Р., Современный стратегический анализ, 5 изд., Питер, 2008, с. 160.

Possession of a resource or a competence can provide a profitability if it can provide a competitive advantage, if advantage is sufficiently stable over time and if possible beneficial effects of this advantage could be accumulated by the company.

It is possible that a resource or capacity to provide a competitive

advantage only if they are unique in any direction. Much of owned resources and competencies are necessary to carry out business, but may not provide an advantage, because all competitors in the industry have them. At the same time, resources or competencies must be relevant to the particular business.

Sustainability of competitive advantage is result of the predetermined duration of its existence, the possibility of its transmission from one actor to another and the possibility of its reproduction. At the same time, the company may have a certain advantage, which provides beneficial effects for consumers, they are willing to pay a higher price for the product, but it is unable to accumulate the potential beneficial effects generated.

The procedure²⁶ to gain competitive advantages includes the following activities:

1. Main resources and competencies identification.
2. Evaluation of resources and competencies.
3. Drawing strategic conclusions.

There are two approaches to identify the main resources and competencies. The first one concerns identification of the Industry's key success factors and the second - to analyse the Enterprise value chain.

Key success factors for each individual business depend on the interdependence between the competing forces in the industry. Managers with some experience in the industry can easily identify which are the key factors for success in this industry or in the occupied by the company's niche. If we make a summary for the defence industry in Bulgaria, we can consider that essential to the operation of the business are the following factors:

- Financial stability
- Reputation
- Speed of new products development
- High products quality
- Good marketing
- Customers confidence

²⁶ The idea is adopted from: Grant, R. Op.Cit. p. 164-172.

The Enterprise value chain approach is proposed by Michael Porter. It consists briefly in the following. All activities performed by the company in pursuit of a particular business are divided into two groups – primary and support activities. Activities should be subdivided until it is possible to establish how each activity affects the competitiveness and what are the cash flows associated with it. At the same time there must be determined important links between activities. A graphical depiction of the approach is presented in Fig. 4.

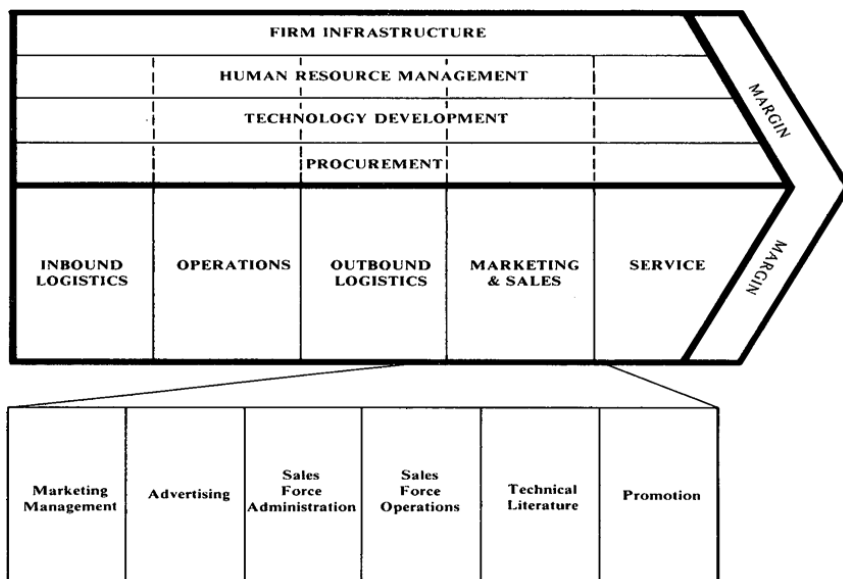


Fig. 4. Value chain approach

Source: Porter, M., *Competitive Advantage. Creating and Sustaining Superior Performance*, New York, The Free Press, 1985, p. 46.

If implemented these two approaches in terms of defence industrial enterprises in Bulgaria can be concluded that the most important competencies for their competitiveness can be:

1. Financial management abilities.
2. New products development ability.

3. Competence to run Quality management system effectively.
4. Competencies to conduct own marketing studies.
5. Ability to keep customers trust / confidence.

Evaluation of resources and competencies can be done from two perspectives: an assessment of their importance and their comparative power. In assessing the importance, the emphasis is not on what will be the choice of the user but on how the factor may affect the long-term maximization of income through the establishment of sustainable competitive advantage. The accent is not on what the consumer will choose, but on whether the item will influence the long term income maximization through sustainable competitive advantages.

The comparative power evaluation is based on objective comparative analyses of strength and weak resources / competences in comparison with competitors.

A subjective assessment of the identified competencies from those two perspectives, using a scale 1 - 10 (1 - very low estimate, 10 - very high estimate) is presented in Table 1.

Table 1.

**Comparative assessment of competencies of Bulgarian
defence industry enterprises**

Competency	Strategic Importance	Comparative power
1. Financial management abilities	4	5
2. New products development ability	10	4
3. Competence to run Quality management system effectively	7	6
4. Competencies to conduct own marketing studies	8	7
5. Ability to keep customers trust/confidence	8	6

A graphical representation of the same information enables the resources and competencies to be divided into four groups, depending on the quadrant in which they fall (Fig. 5).

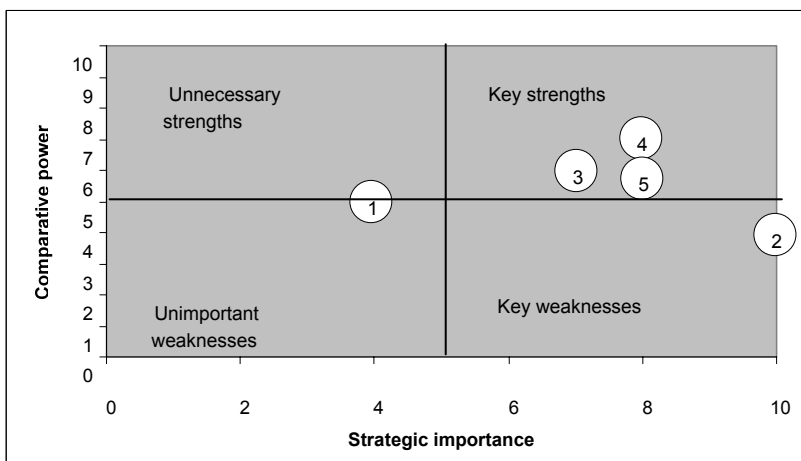


Fig 5. Positioning of competences of the Bulgarian defence industry enterprises

Strategic conclusions which can be made as a result of this analysis will depend on the quadrant, which hit the resources or competences. Depending on that recommendations may be, for example:

Use of key strengths:

- To develop a strategy to use key strengths maximum effectively

Management of key weaknesses:

- Long term efforts and investments to reach competitors.
- Outsourcing.
- Transformation of weaknesses into strengths.
- Development of a strategy/adaptation of active strategy in order to defend enterprise from its weaknesses.

Activities to unnecessary strengths:

- Decrease investments in these resources and competencies
- Innovation strategy to transform unnecessary resources and competencies into valuable resources and competencies.

Concentration on analysis of a specific defence industrial enterprise will enable to carry out in more precise manner the offered procedure, to identify more and more specific competences and formulation of more useful strategic conclusions and recommendations for action.

CORPORATE LEADERSHIP IN TIME OF CRISIS

Professor Stefan Hristov, PhD

Department “National and Regional Security”

University of National and World Economy, Sofia, Bulgaria

Introduction

Global crisis is the centre of attention for state heads of world's leading countries. They try to come up with effective decisions on its restriction and overcoming. Emerged crisis causes significant decrease in demand, market shrinkage, production cut, finance deterioration, credit restriction, investment reduction, rapidly rising of unemployment rate, living standard on decline and other negative phenomena.

Economic challenges facing our country are primarily related to external impact of the fundamental factors of global crisis. They have negative impact on the key branches of the national economy, including defence industry. Corporate leaders of domestic companies are required to perform a sensible decision making and take adequate actions, aimed at preserving the local business.

Theoretical Framework

Leading in times of crisis is not easy work. Famous leaders usually know what to do, why to do, how to do, when to do, where to do and so on. They have the actual vision and the appropriate strategy to achieve desirable goals in complicated environment. Charisma, wisdom, intelligence, vitality, confidence, responsibility and other characteristics are of substantial significance. Special traits to suit the situation are also needed.

The current research uses creative ideas from Leadership Theory and Personality Theory. The first one emphasizes on distinctive attributes for coping with challenges and the second one – on the specific

qualities of corporate leaders. They are of great importance during a crisis having strong impact on organizational performance. Leadership behaviour in times of enormous insecurity and high risk is essential.

Classical models were created in the field of corporate leadership.²⁷ They are generally based on the use of such approaches, as:

- Trait approach;
- Contingency approach;

The first one is focused on general attributes and the second – on common qualities of leaders for problem solving.

Leadership behaviour is formed to a certain extent under the influence of various psychological factors. The Theory of Psychological Types is originally developed by the Swiss psychiatrist Carl Jung²⁸. It's the groundwork for MBTI²⁹ instrument (Myers-Briggs Type Indicator) for personality inventory by Katharine Briggs and Isabel Briggs Myers.

Psychological preferences of corporate leaders can be described in Table 1.

Table 1

Psychological Preferences		Way of deciding	
		Thinking Type (T)	Feeling Type (F)
Way of acting	Judging Type (J)	TJ Type	FJ Type
	Perceptive Type (P)	TP Type	FP Type

Psychological traits reveal distinctive preferences of leaders in problem solving process. Thinking Type is lead by thoughts, while Feeling Type – guided by emotions. Judging Type is known for its planning and organizing, while Perceptive Type – with adaptivity and spontaneous. Combination between particular types allows them to be divided in four clusters with personal specifics. **TJ Type** combines practicality with responsibility, **TP Type** – rationality with flexibility, **FJ Type** – creativity with commitment, **FP Type** – ingenuity with improvising. That determines differences in personalities of corporate leaders.

²⁷ Stogdill, R., Handbook of Leadership, 1999.

²⁸ Jung, C., Psychological Types, 1923.

²⁹ Myers-Briggs Type Indicator, 1962.

Corporate leadership is classified according the level of engagement of the associates of the business organization such as:

- Participative leadership, based on support a great number of contributors in the decision-making process.
- Directive leadership, based mainly on individual decision-making by leader.

Good leaders should be able to demonstrate talent for seeking innovative solutions. They have to think before act in dynamic situations in turbulent time. True leaders always need to be communicative and motivating. Their thinking has to be proactive and positive. They have to correctly outline priorities and directions for improvement of their organizations.

Empirical Investigation

Crisis situation requires leadership attributes, professional qualities, personal abilities, business experience, etc. The primarily focus of empirical investigation is on leadership attributes and professional qualities, determining the way of thinking and way of acting in times of crisis. The key issue in the present research is „Which essential attributes and important qualities have to have corporate leaders of Bulgarian companies in time of economic crisis?“ The right answer has to define the exact combination of leader’s traits for a particular situation. A survey with total of 90 respondents was conducted. The psychological types of all participants were defined using MBTI test. Their distribution is illustrated in Table 2.

Table 2

Type	Number	Percent		Type	Number	Percent
Extraverts E	70	77,8%	vs	Introverts I	20	22,2%
Sensing S	57	63,3%	vs	Intuitive N	33	36,7%
Thinking T	47	52,2%	vs	Feeling F	43	47,8%
Judging J	42	46,7%	vs	Perceptive P	48	53,3%

Processed results show that *Extraverted type (E)* dominated over *Introverted type (I)*, *Sensing type (S)* over *Intuition type (N)*, *Thinking type (T)* over *Feeling type (F)*, *Perceptive type (P)* over *Judging type (J)*.

TJ, TP, FJ and *FP* types are of considerable interest for the current research. Their distribution is illustrated on Figure 1.

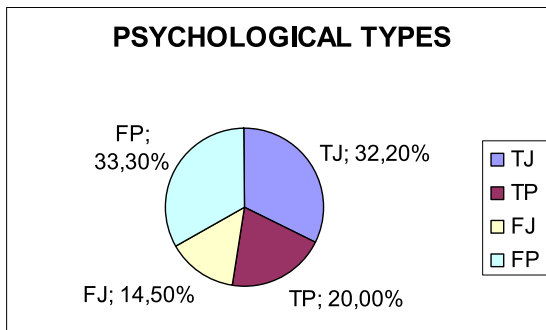


Fig. 1

The results show that the most numerous ones are *FP* and *TJ type*, respectively with 33,3 % and 32,2 % total number of participated people.

The first task of interviewed respondents was to list the leadership attributes of corporate managers of Bulgarian companies in times of crisis according to their importance. Subject assessments were key leadership attributes (LA) such as:

- Decisiveness (LA₁)
- Persistence (LA₂)
- Openess (LA₃)
- Profoundness (LA₄)
- Honesty (LA₅)
- Daring (LA₆)
- Ethics (LA₇)

Summarized results of conducted survey show that there is a complete agreement between all participants - Thinking type (47 people) and Feeling type (43 people) in ranking of leadership attributes.

Decisiveness (LA_1), Persistence (LA_2) and Profoundness (LA_4) of the leaders are considered the most sufficient. Consensus values of the **T type** and **F type** are shown on Figure 2.

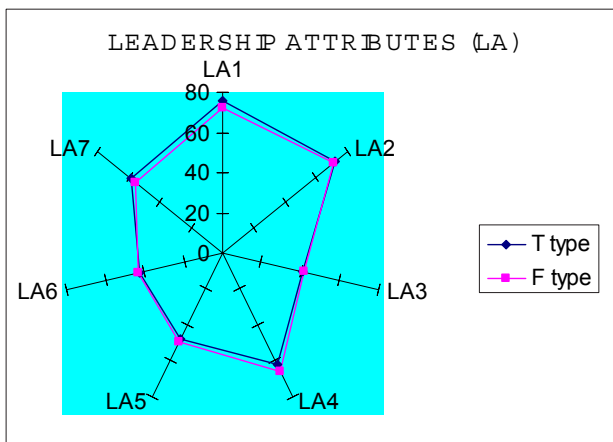


Fig. 2

There are significant differences in ranking of leadership attributes by **Judging type (J)** and **Perceptive type (P)**. Calculated ranking and consensus values are summarized in Table 3.

Table 3

LA	TJ Type		TP Type		FJ Type		FP Type	
	Rank	Cons. %	Rank	Cons. %	Rank	Cons. %	Rank	Cons. %
LA_1	1	84,24	3	62,70	2	73,63	1	71,90
LA_2	2	69,46	1	76,19	1	82,42	3	66,67
LA_3	6	44,83	7	36,51	7	36,26	7	44,76
LA_4	4	53,20	2	75,40	3	61,54	2	67,14
LA_5	5	49,26	5	44,44	5	48,35	5	49,05
LA_6	7	42,36	6	42,86	6	39,56	6	45,71
LA_7	3	56,65	4	61,90	4	58,24	4	54,76

Similarity in ranges obtained from different psychological types can be measured with Spearman's rank correlation coefficient ρ (rho). It serves as non-parametric measure of the relationship between two ratings. **TJ type** respondents give highest rank to Decisiveness (LA_1), Persistence (LA_2) and Ethics (LA_7), while **TP type** – to Persistence (LA_2), Profoundness (LA_4) and Decisiveness (LA_1). The value 0,786 of rho coefficient indicates a close similarity in ranking of leadership attributes among the participants from **TJ type** and **TP type**.

According to **FJ type** respondents the most important attributes are Persistence (LA_2), Decisiveness (LA_1) and Profoundness (LA_4). Inquiry group of the **FP type** ranks Decisiveness (LA_1), Profoundness (LA_4) and Persistence (LA_2). The value 0,893 of Spearman's rho showing very high similarity in ranking of leadership attributes among participants of these types. It's interesting to mention the fact that according rho coefficient 0,964 the closest rankings are among the respondents from **TP type** and **FJ type**.

The second task of contributors was to evaluate the necessary professional qualities of corporate leaders of Bulgarian companies in times of economic crisis. A five-score scale was used; in which 1 is the lowest value and 5 - the highest value. The key Professional Qualities (PQ) illustrate principal approaches used in solving crucial problems such as:

- Competence (PQ_1)
- Innovativity (PQ_2)
- Entrepreneurship (PQ_3)
- Creativity (PQ_4)
- Communicability (PQ_5)
- Constructiveness (PQ_6)
- Encouragement (PQ_7)

Calculated scores of the interviewed in the survey exemplify the manifested preferences of all psychological types regarding professional qualities of corporate leaders. They are described in Figure 3.

Competence (PQ_1) and Entrepreneurship (PQ_3) get the highest score of all respondents. These qualities of corporate leaders are very likely to contribute to the successful crisis management performed by the Bulgarian companies.

**Fig. 3**

Initial values of invited respondents are grouped by means of psychological type. They are used for calculation of average scores and the importance of professional qualities. The raw scores are converted later on to ranks (Table 4).

Table 4

PQ	T Type			F Type		
	Mean score	Importance %	Rank	Mean score	Importance %	Rank
PQ ₁	4,383	15,1%	2	4,581	15,6%	1
PQ ₂	4,277	14,8%	3	3,884	13,3%	5,5
PQ ₃	4,447	15,3%	1	4,419	15,1%	3
PQ ₄	3,681	12,8%	7	3,837	13,0%	7
PQ ₅	4,213	14,5%	4	4,465	15,2%	2
PQ ₆	3,851	13,3%	6	3,884	13,3%	5,5
PQ ₇	4,128	14,2%	5	4,233	14,5%	4

Respondents from **T Type** evaluate with highest score the importance of Entrepreneurship (PQ₃), Competence (PQ₁) and Innovativity (PQ₂) of corporate leaders. **F Type** respondents give credit to such professional qualities such as Competence (PQ₁), Constructiveness (PQ₆) and Entrepreneurship (PQ₃). Similarity in assessment of the two groups, measured with Spearman's rho, estimates 0,649. Think-

ing type favours dynamic persons and Feeling type rather prefers intelligent individuals.

The average score value of Thinking Type (T) and Feeling Type (F) leaders is shown on Figure 4.

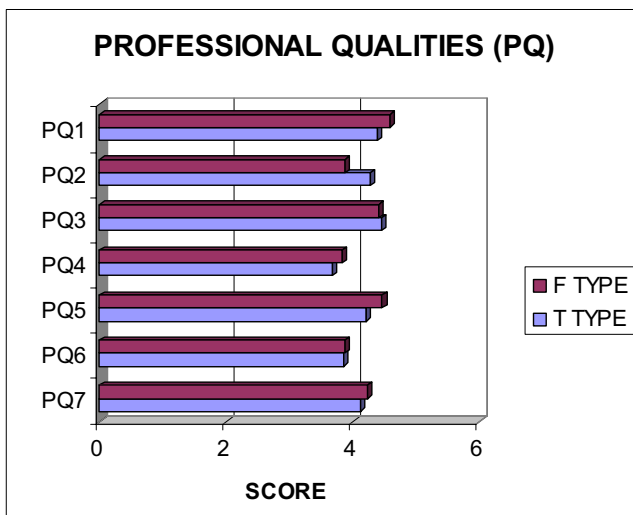


Fig. 4

The biggest difference is outlined in score value of Innovativity, which is among the leading ones for **T Type** and quite far in **F Type** ranking. There is a close difference in mean scores regarding Competence.

Successful leadership requires relevant qualities, which are crucial for difficult and responsible decision making concerning important changes in time of crisis. A good leader of every level should be able to solve practical issues „What if...?“ The list of needed qualities is quite long, because it depends to a certain extent on the essence of each task.

Calculated scores of professional qualities of corporate leaders according **TJ Type** and **TP Type** respondents are shown in Table 5

Table 5

PQ	TJ TYPE			TP TYPE		
	Mean score	Importance %	Rank	Mean score	Importance %	Rank
PQ ₁	4,414	15,4%	2	4,333	14,8%	3,5
PQ ₂	4,138	14,4%	4	4,500	15,6%	1
PQ ₃	4,517	15,7%	1	4,333	14,8%	3,5
PQ ₄	3,724	12,7%	7	3,611	12,1%	7
PQ ₅	4,069	14,1%	5	4,444	15,4%	2
PQ ₆	3,759	13,0%	6	4,056	14,1%	5
PQ ₇	4,241	14,7%	3	3,889	13,2%	6

Contributors from **TJ Type** assess with highest score the importance of Entrepreneurship (PQ₃), Competence (PQ₁) and Encouragement (PQ₇) for corporate leaders. People from **TP Type** evaluate as highest Innovativity (PQ₂) and Communicability (PQ₅). The Spearman's rho is 0,336, showing from weak to moderate range of values of **TJ Type** and **TP Type** in ranking of professional qualities. There is a positive correlation between PQ estimated r coefficients. Analogically with **TJ type** between Entrepreneurship and Competence ($r=0,516$), Encouragement and Creativity ($r=0,481$), Communicability and Constructiveness ($r=0,345$). Analogically, **TP type** shows a moderate relationship between Creativity and Communicability ($r=0,624$), Entrepreneurship and Competence ($r=0,577$), Competence and Communicability ($r=0,519$), Creativity and Competence ($r=0,511$), Creativity and Innovativity ($r=0,463$), Competence and Innovativity ($r=0,462$), Encouragement and Entrepreneurship ($r=0,429$).

Corporate leaders differentiate from the ordinary people in business organizations. They are leading individuals, which respect staff with enhanced skills and turn them into voluntary followers. Their abilities generally stand out in decision making in crisis situations.

Table 6 features data on the significance of professional qualities of corporate leaders according **FJ Type** and **FP Type** respondents.

Table 6

PQ	FJ Type			FP Type		
	Mean score	Importance %	Rank	Mean score	Importance %	Rank
PQ ₁	4,615	16,0%	1	4,567	15,5%	1
PQ ₂	3,846	13,2%	6	3,900	13,2%	5
PQ ₃	4,308	15,0%	3	4,467	15,4%	2,5
PQ ₄	3,769	12,7%	7	3,867	13,1%	6
PQ ₅	4,462	15,3%	2	4,467	15,4%	2,5
PQ ₆	4,077	13,9%	4,5	3,800	12,7%	7
PQ ₇	4,077	13,9%	4,5	4,300	14,7%	4

Interviewed **FJ Type** respondents appraise as the most important professional qualities of corporate leaders - Competence (PQ₁), Communicability (PQ₅) and Entrepreneurship (PQ₃). **FP Type** respondents show similar position, arranging listed qualities in the following sequence: Competence (PQ₁), Entrepreneurship (PQ₃) and Communicability (PQ₅). The Spearman's rho is 0,836, which shows strong similarity in ranking of professional qualities among the participants from **FJ type** and **FP type**. For **FJ type** the r coefficient indicates a moderate correlation between Encouragement and Innovativity ($r=0,564$), Competence and Communicability ($r=0,489$), Encouragement and Innovativity ($r=0,400$). For **FP Type** it shows from weak to moderate relationship between Creativity and Communicability ($r=0,371$), Innovativity and Communicability ($r=0,366$), Encouragement and Creativity ($r=0,317$).

Good leaders should have well-timed reaction to urgent threats in external environment. They should also skillfully use the newly come business opportunities in turbulent times.

Conclusion

Corporate leaders in time of crisis should inspire trust, security, hope and optimism among employees of business organizations. The conducted research shows that in times of economic crisis leadership attributes and professional qualities play significant role. Psychological factors determining leader's behavior show considerable impact on

problem solving. Corporate leaders of the Bulgarian enterprises have to develop an ability to work successfully coping with different circumstances during crisis. Strong influence of national and cultural factors along with psychological factors should be considered in the process of searching for appropriate strategy as response to critical challenges in economy.

Literature

1. Hristov, S., Strategic Management, 2.e., 2009. (In Bulgarian)
2. Sayles, L., Leadership for Turbulent Times, 1995.
3. Stogdill, R., Handbook of Leadership, 1999.

CONCEPTUAL MODELING IN THE DEFENSE ACQUISITION PROCESS

Captain Marius MĂRMUREANU, Eng, MSc, PhD Candidate

Armaments Test&Evaluation and Scientific Research Center

Military Equipment and Technologies Research Agency

Ministry of National Defense, Romania

Abstract

The paper defines conceptual modeling and the necessity to use it in the defense acquisition process. Basic concepts, efforts and current tendencies in the area are presented along with main benefits that conceptual modeling gets in the general framework of systems development.

1. Introduction

Decreasing budgets, coupled with the necessity of being prepared for multi-faceted types of military activities, such as humanitarian interventions, joint peacekeeping efforts, and other "Missions-other-than-War" have created a need to prepare for unforeseen missions. There is also a requirement for the military to attempt to try out unfielded and evolving weapon systems and technologies to see how they might affect their tactics, techniques and procedures. This analysis is being done by means of modeling and simulation, from conventional (live-action) war-gaming to completely virtual simulations. Constructive simulations are being used to determine the effect of new technologies on Command, Control, Communications, Computers and Intelligence (C4I). Capturing high-level, contextual information as well as sharing data object can enhance simulation interoperability.

2. Some basic definitions

A model is a representation of reality, also called an abstraction. By definition the model will only represent some aspects of the problem domain and ignore other issues. This means that models and simulations can never be perfect reproductions of the systems, units or processes that they are meant to represent.

A concept is an abstract idea or a mental symbol, typically associated with a corresponding representation in language or symbology, that denotes all of the objects in a given category or class of entities, interactions, phenomena or relationships between them. Conceptualization is the realization or emergence of concepts.

A conceptual model is defined as an abstract (mental) model of some part of reality. A conceptual model describes the key concepts, and their relationships within this specific part of reality.

The purpose of Modeling & Simulation (M&S) is to represent a real system in order to draw conclusions about the real system by experimentation with a model. Thus, the direct correlation between the model, an intended purpose of model use, and a clearly identified real system are among the key characteristics of simulation. The term "simulation" implies a claim to represent the behavior of a real system as it is or as it could be. The direct association to a real system distinguishes computer-based simulation from, e.g. computer games. As decisions that heavily impact the real world rely increasingly on models or simulation results, the more important their correctness and suitability becomes. Suitability refers to the concepts of capability, fidelity, and accuracy, while correctness refers to consistency and completeness. The growing role of M&S implies that measures must be taken to ensure the correctness and suitability of models and simulation results.

As neither suitability nor correctness can be proven in most cases, the credibility of a model or simulation results is of major importance. The credibility of a model is based on the perceived suitability and the perceived correctness of all intermediate products created during model development.

Advances in computational and networking capabilities during

the past decade brought major increases in M&S capabilities. Significantly increased reliance is placed upon M&S for a wide variety of applications: analysis and planning, system design and engineering, test and evaluation, operational support and execution, as well as training, education and mission rehearsal. This increased reliance upon M&S in so many critical areas in the defense community, government organizations as well as in industry and academy, gives special importance to M&S Verification and Validation (V&V). V&V is the means by which M&S correctness is enhanced and ascertained so that appropriate credibility and confidence may be placed in M&S.

3. Conceptual Models

Conceptual models (CM) are key to the transformation of user needs and requirements to M&S design, and eventually implementation. CM form the bridge of understanding between the users of M&S, the military domain experts that have the necessary knowledge that must be represented in M&S, and the software and simulation engineers that implement simulations.

Without Conceptual Models, history has shown that simulation developers often do not sufficiently understand the military domain to be modeled and implement M&S that do not reflect the intended reality, and thus do not satisfy the user's needs. Further, Conceptual Models form the basis of an important step in Verification and Validation (V&V) activities determining that the application domain has been described sufficiently to meet user's needs while accurately incorporating subject matter expert knowledge.

Modeling is an essential aspect of systems development. For example, an information system can be viewed as a representation, or a model of another system (usually termed the real system). Modeling is especially in the analysis stage of systems development when abstract models of the represented system and its organizational environment are created. Such models are termed conceptual models. A conceptual model should reflect knowledge about the application domain rather than about the implementation of the system.

Once simulation objectives have been established, development of

the simulation conceptual model may begin. Simulation requirements and conceptual model development are a classic "chicken-egg" pair. They each stimulate and derive from the other. Conceptual model development may even begin before completion of the simulation requirements. In some cases, the iterative and interactive formulation of simulation requirements with development of the simulation conceptual model can be beneficial.

There are four basic steps in the development of a simulation conceptual model. The first step is to collect authoritative information about the intended application domain that will comprise the simulation context. Development of the simulation concept and collection of authoritative information for the simulation context are likely to occur iteratively as the entities and processes to be represented in the simulation are more clearly defined.

The second step in conceptual model development is to identify entities and processes that must be represented for the simulation to accomplish its objectives. This enumeration process is fundamental. It is here where basic decisions are made about the level of detail and aggregation that is appropriate to support simulation requirements. These decisions determine whether a system (such as a radar) will be represented as a single entity, as a composite of subsystem entities (such as an antenna or receiver), or as a composite of composites of ever-smaller entities (to whatever level of detail is needed for the purpose of the simulation). Decisions are made at this step about the level of representation of human decisions and actions.

The third step is the development of simulation elements. A simulation element is needed for each entity or process (or composites of such) identified in step two. Here, decisions are made initially about the level of accuracy, precision, resolution, etc., needed in the representation of the entity or process. Simulation elements determine the functional and behavioral capabilities of the simulation. Simulation fidelity is a function of both the scope of representation in a simulation (the entities and processes identified in step two) and the quality of entity and process representation in terms of accuracy, and precision.

The fourth step addresses relationships among simulation elements to ensure that constraints and boundary conditions imposed by the simulation context are accommodated. In addition, it ensures that simulation space issues (e.g., control capabilities that allow the simulation to be stopped, backed up in time, restarted, etc., or that identify data to be collected during the simulation) are addressed appropriately. These four steps will be iterated often in most simulation developments.

Nine items (listed below) are suggested for the description of a portion of the conceptual model (such as a simulation element) or the entire conceptual model in the scientific paper approach to documenting a simulation conceptual model:

1. Conceptual model portion identification
2. Principal simulation developer point(s) of contact for the conceptual model (or part of it)
3. Requirements and purpose
4. Overview
5. General assumptions
6. Identification of possible states, tasks, actions, behaviors, relationships and interactions, events, and parameters and factors for entities and processes being described
7. Identification of algorithms
8. Simulation development plans

4. M&S, CM and Acquisition Processes

Evaluating system performance against stated requirements fosters user confidence in the system produced. In system acquisition, M&S serves as a key tool in reducing time needed to field a system; in reducing resources needed to develop and evaluate that system; and in reducing decision risk.

Risk is the potential realization of undesirable consequences from hazards arising from a possible event. Risk is present in decision making because only imperfect knowledge is available to make the decision. Models and simulations (M&S) have become an integral part of the systems acquisition process, being employed in every phase of sys-

tem development such as requirements development, design, production, and test. As M&S are increasingly used, it becomes increasingly important to accumulate evidence that these tools are performing correctly. Verification, validation, and accreditation (VV&A) of models and simulations are required to reduce the risk of incorrect decisions based on erroneous M&S outputs. The goal, then, of VV&A is to mitigate the risk of poor decisions based on incorrect models and simulations.

M&S also can provide means to evaluate and improve quality, military utility and supportability of fielded systems. In system acquisition's T&E phase, M&S is used to develop parameters for mission rehearsal; to design tests; to analyze data collected during testing; and to evaluate regions of the operational envelope not otherwise testable. While M&S is a useful tool for predicting, training and planning, it is not a substitute for testing. M&S is practical only if it applies to the evaluation of the system being acquired, and only if it is capable of replicating reality to a required level. Evaluating M&S systems against the requirements, both system specific and in terms of real-world representation provides insight into M&S credibility.

5. Overview of Relevant U.S. Defense Acquisition Policy

In 2003, the U.S. Department of Defense (DoD) issued new directives and instructions covering nearly every aspect of system acquisition including modeling and simulation.

DoD Directive 5000.59, DoD Modeling and Simulation Management, states that M&S used to support major DoD decision-making organizations and processes shall be accredited for that purpose.

DoD Instruction 5000.2, Operation of the Defense Acquisition System, states that program managers must plan for modeling and simulation activities throughout the life cycle. The Instruction goes on to say that the "*T&E strategy shall provide information about risk and risk mitigation, provide empirical data to validate models and simulations, evaluate technical performance and system maturity, and determine whether systems are operationally effective, suitable, and survivable against the threat detailed in the System Threat Assessment*". Fur-

thermore, "*appropriate use of accredited models and simulation shall support (T&E)*" with accreditation being defined as the official certification that a model or simulation is acceptable for use for a specific purpose.

DoD Instruction 5000.61, DoD Modeling and Simulation (M&S) Verification, Validation and Accreditation (VV&A), states that it is DoD policy that "*verification and validation (V&V) shall be incorporated into the development and life-cycle management processes of all M&S...commensurate with the relative importance, risk, and life-cycle management phase of the model, simulation, or federation to which they are applied*". Furthermore, it says that the "*M&S Application Sponsor shall document accreditation results, to include... the accreditation methodology, including V&V activities, that support accreditation; data verification and validation; risk assessments; and acceptability criteria*".

The DoD directives and instructions offer guidance on use of VV&A activities to identify and mitigate risk, but no details; these are left to service implementation instructions. Documents implementing DoD Instruction 5000.61 and DoD Directive 5000.59 repeat the requirement that the acquisition process is one means of mitigating risk in planning, developing, testing, and fielding military systems. There are variations in the service policy documentation required for a risk analysis, some being part of the VV&A plan and reports, others the accreditation plan and report. But they all call for a risk analysis and documentation of the results and how the risk analysis results affect planned uses of the M&S.

The Defense Modeling and Simulation Office (DMSO) VV&A Recommended Practices Guide (RPG), available from the DMSO website, contain detailed guidance for VV&A practitioners. The guide provides information on risk assessment. A detailed discussion of risk analysis and its impact on VV&A is provided in a special topic paper in the RPG on the DMSO website.

The T&E process is founded on requirements, including critical technical parameters, operational issues, and measures of performance and effectiveness. Maturity of the T&E process provides an excel-

lent benchmark for the VV&A process to evolve. T&E assesses operational system performance in the same manner that VV&A assesses M&S credibility. The DoD Generic VV&A Process, described in the Recommended Practices Guide, identifies both the problem and the requirements for solving it. The next step calls for determining the problem solving approach. M&S is one problem-solving tool, but other tools also may be employed as well. Given that M&S will guide researchers to find at least part of the solution, the process identifies general requirements for model capabilities. Depending on the nature of these requirements, problem solvers may use an existing model either as is or modified, or they may need to develop a new model. Once researchers decide on an approach, they can establish requirements for the specific model(s) chosen and then prepare the model for use. While the T&E process is rooted in requirements definition, the VV&A process has not yet learned the lesson or importance of requirements. Many programs attempt to avoid requirements definition or to make unfounded assumptions, one of which is that M&S is the correct tool to use when another tool might be more effective. Another example is choosing a specific model without adequate rationale. Choosing an inappropriate model could lead to invalid results. This situation sometimes results from researchers' lack of familiarity with the VV&A process.

However, instances have occurred in which participants intentionally have made suboptimal decisions either to maximize other resources or to placate a decision maker who had already chosen a tool. In some cases, researchers have tailored requirements from the VV&A process. Tailoring, a VV&A term, describes the action of focusing a well-planned VV&A effort on those tasks providing optimal return on investment. In this process, participants select V&V tasks and techniques that will render the most expedient, credible results by which to assess the model. Requirements definition, however, is not open to negotiation or tailoring. Common sense dictates that, to assess a simulation credibly, one must know what the simulation is supposed to accomplish.

References

1. Eugen POPESCU, *Conceptual Modeling Role in the Defense Acquisition Process*, Military Technique, Number 1 (2008), Departments for Armaments, Romania.
2. Dale K. PACE, *Ideas about Simulation Conceptual Model Development*, Johns Hopkins APL Technical Digest, Volume 21, Number 3 (2000).

FIFTH GENERATION WARFARE – A POSSIBILITY FOR THE FUTURE

Captain Liviu MATACHE, Eng, MSc, PhD Candidate
Armaments Test&Evaluation and Scientific Research Center
Military Equipment and Technologies Research Agency
Ministry of National Defense, Romania

1. Fifth Generation Warfare Background

The first generation of war arose from the first generation of the state as the coherent governing entity and describes an arc of regimented, linear combat beginning from the Romans at Cannae and Zama, pausing at the formalizing of the state in the 1648 Treaty of Westphalia, and accelerating the killing up to and through the horrors of the American Civil War.¹

The second, attritionist generation of war, began as man realized what the state, massed and determined, could do—the horrors of World War I trench warfare and a stubborn Prussian insistence on demanding an orderly battlefield imposed on chaos. If battle wasn't organized, armies could be. (See Figure 1.)

The third generation of war began at the point where the British Empire's fall intersected with America's rise from power to empire and corresponds directly with a rise in the mechanization of war. Conflict moved from up-close murder to distant engagements with hardware, and the raw violence of war decreased in direct proportion to the beyond- visual range externalization of violence. With its roots in World War I, this generation carried Western armies through DESERT STORM, emerging from German staff officers' clear-eyed views of the chaotic battlefield and a concomitant willingness to embrace chaos and substitute maneuver for men marching into the bullets. This set of ideas meshed nicely with Huntington's

ideas on the progression of war—from an emperor’s acting to expand kingdoms to states’ acting in raw national interest. As the state grew more nimble, so did its backbone of military leadership.

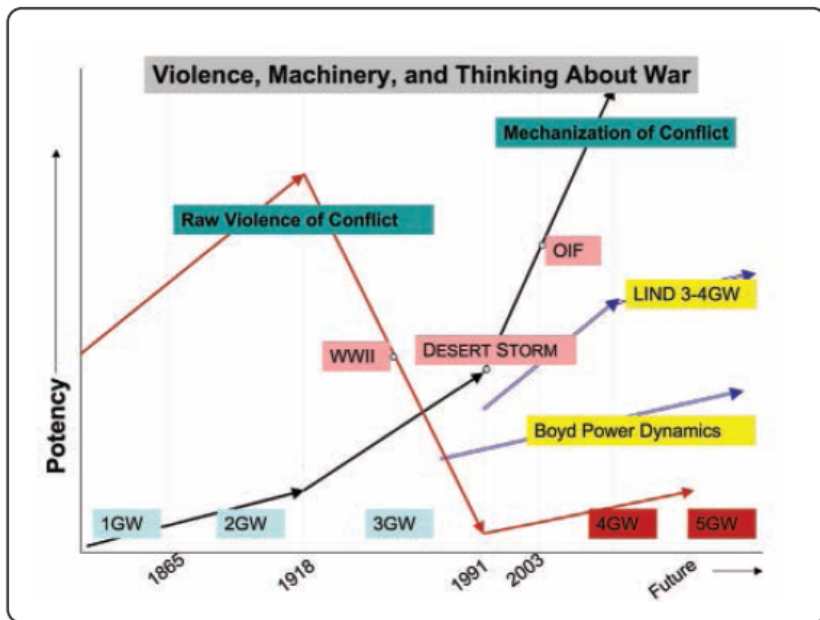


Figure 1

The 4GW, the generation in which we are now, is a dynamic, frightening, freewheeling type of 360-degree violence, with centers of gravity unlike any to which the military has trained. It is driven by and motivated by the rise of radical Islam as an ideological counterweight to what retired Marine and professor Dr. Mackubin Owens calls American “benevolent primacy.”

2. Developments in 4GW

Current events suggest that there are a number of ongoing major developments in 4GW: a *strategic shift*, an *organizational shift*, and a

shift in type of participants.

Strategic shift -Strategically, insurgent campaigns have shifted from military campaigns supported by information operations to strategic communications campaigns supported by guerrilla and terrorist operations.

Organizational shift -. The emergence of civil war as a part of insurgency is based on the major organizational shift that has occurred since Mao formulated his concept. It reflects the continuous, worldwide shift from hierarchical to networked organizations. The rise of networked coalitions is in keeping with the fact that both the societies in conflict and the dominant business organizations of our time are networks. Like society as a whole, insurgencies have become networked, transnational, and even trans-dimensional. Going beyond simple real-world networks, some elements of their organizations exist in the real world, some in cyberspace, and some in both dimensions.

Shift in participants. As part of the organizational shift, we have seen a change in who is fighting and why. It is essential for us to understand that, even within a single country, the highly diverse armed groups that make up a modern insurgency have widely differing motivations. Studying the motivation of a group gives us a strong indication of how that group will fight and what limits, if any, it will impose on its use of force. In terms of founding motivations, armed groups generally fall into three categories: they can be *reactionary*; they can be *opportunistic*, meaning that they seized on a political or economic opportunity to enhance their own power or positions; or they are founded to further *ideological* objectives.

Reactionary groups often form when communities feel threatened. They tend to be sub-national or national groups that operate in specific geographic areas and attempt to protect the people of those areas. In essence, these armed groups represent a return to earlier security arrangements; they are the result of a state's failure to fulfill its basic social contract of providing security for its population.

Reactionary groups need to protect populations but lack the military power to do so. As a result, they usually resort to 4GW—but gen-

erally use only conventional arms. While highly effective, such weapons are familiar to Western armies and thus easier to anticipate and defeat. Reactionary groups also tend not to be a threat outside their areas since they are focused mainly on defending their own people. However, they still conduct sophisticated communication campaigns to defeat outside powers.

Opportunistic groups spring up to take advantage of a vacuum to seize power or wealth. Criminal by nature, these groups have been around for centuries. Opportunistic groups include organizations like Mara Salvatrucha 13 (MS-13) and, increasingly, the Irish Republican Army (IRA). Opportunistic groups conduct their own strategic communications campaigns, usually citing a religious or national cause to claim legitimacy for their criminal activities.

A third great motivator, **ideology**, gives birth to the most dangerous armed groups— organizations like Al-Qaeda, Aryan Brotherhood, and Aum Shinrikyo. They are more likely to use society's infrastructure—chemical plants, mass shipments of fertilizer, even biotechnology—as weapons of mass destruction than groups motivated by self-defense or opportunism. Of even more concern is the fact that ideological groups are essentially impossible to deter. First, their "cause" provides moral justification, and sometimes a moral requirement, to use any available weapon. Second, they have no return address, so they do not fear massive retaliation. Ideological groups will not be deterred even by the danger inherent in the use of biological weapons. While other groups may hesitate to release a contagious biological agent for fear of killing their own people, ideological groups believe the higher power guiding their actions will either protect their members or call them home for their earned reward. Thus, the combination of extraordinarily rapid advances in biotechnology and the spread of ideologically driven armed groups represent a major threat to the global population.

Criminals are yet another player in 4GW. Most 4GW discussions still focus on politically motivated insurgent groups, however, criminal organizations are using 4GW techniques.

3. Four Generation Warfare Updated

Organizationally, the insurgents are evolving into an ever-increasing variety of armed groups linked into coalitions of the willing. Also, the types of players and their motivations have changed significantly over time. The proliferation of motivations and merging of ideological, reactionary, and opportunistic groups makes it increasingly difficult to tell who is fighting and why. Fortunately, the bottom line remains effective security and governance for the people, and the new counterinsurgency field manual (FM 3-24, *Counterinsurgency*) provides solid guidance on how to achieve that.

To deal with the numerous changes in 4GW, we will have to find new ways to provide security while building the political coalitions that are the only way to defeat an insurgency. We will also have to apply our diplomatic, economic, and political resources more broadly and effectively than we have done in the past to deal with the expanding nation-state use of 4GW.

4. Fifth Generation Warfare

Like always, the old generations of war continue to exist even as new ones evolve. Today, we see grim 2GW firepower-attrition battles in parts of Africa even as the first hints of 5GW emerge. This should not be surprising—countries that lack the political, social, and economic systems to support new forms of war will continue to use the older forms. Yet a new generation must also evolve and, given the fact that 4GW has been the dominant form of warfare for over 50 years, it's time for 5GW to make an appearance. The threats he will present will be “the marriage of instability and initiative,” not standing and fighting but in projecting “the smallest force at the quickest time at the farthest place.” Such a place will not be a battlefield of our choosing; such a force will not be an infantry squad, or an airplane, or a ship. The weapon will not be a club but a stiletto. The battlefield will be something strange—cyberspace, or the Cleveland water supply, or Wall Street's banking systems, or YouTube.

We should be able to get some idea of what this new form of war

will be by examining how political, social, and economic systems have changed since 4GW became dominant.

Politically, there have been major changes in who fights wars. The trend has been and continues to be downward from nation-states using huge, uniformed armies to small groups of like-minded people with no formal organization who simply choose to fight. We have slid so far away from national armies that often it is impossible to tell 4GW fighters from simple criminal elements. Many of the former are, in fact, criminal elements—either they use crime to support their cause or they use their cause to legitimize their crime.

Economically, we have seen a steady increase in the power of information. Insurgent groups have seized on the improving information grid to execute the strategic communications campaigns that are central to their victories. The content and delivery of information has accordingly shifted from the mass propaganda of Mao to highly tailored campaigns enabled by the new methods of communication and new social patterns. Insurgents have been quick to exploit such powerful communication tools as the cell phone and the Internet for recruiting, training, communicating, educating, and controlling new members. They have shifted from mass mobilization to targeted individual mobilization.

Today's *key businesses* are becoming ever more productive because of their access to or manipulation of information. One result has been a proliferation of small companies that have created great wealth, a phenomenon in accordance with the long-term trend of power devolving downward to smaller entities—whether they are business or military. The epitome of this tendency is that just two guys essentially created Google.

Communications is not the only burgeoning sector with implications for 5GW. Two industries with even greater potential to change our world—biotechnology and nanotechnology—are on the verge of huge growth. In many ways military and business problems are merging as the world becomes more interconnected and power is driven downward. In 2006, a group of about 20 angry Nigerians took hostages from a Shell oil platform in the Gulf of Guinea. Shell shut down

its Nigerian Delta production and world oil prices rose dramatically. The interconnected world is highly vulnerable to disruptions in key commodities, and business issues can very rapidly become matters of serious international security. Today, very small armed groups can impact the entire world's economy immediately and dramatically.

Socially, we have seen a major shift in how communities are formed. People are changing allegiance from nations to causes, a trend dramatically accelerated by Internet connectivity. In fact, many people are much more engaged in their online causes than in their real-world communities. Of particular concern are members of groups who are willing to go to extremes to advance their causes—from the woman who lived in a redwood for two years to suicide bombers. Such actors place their causes above any rational analysis of the impact of their actions—and they can be found through the Internet.

In sum, political, economic, and social trends point to the emergence of super-empowered individuals or small groups bound together by love for a cause rather than a nation. Employing emerging technology, they are able to generate destructive power that used to require the resources of a nation-state. All of these new developments are of particular concern because emerging political, business, and social structures have consistently been more successful employing nascent technology than older, established organizations. Today, two emerging technologies, **nanotechnology** and **biotechnology**, have the power to alter our world, and warfare, even more fundamentally than information technology. Today's biotechnology can give small groups the kind of destructive power previously limited to superpowers.⁵

The October 2001 anthrax attack on Capitol Hill may have been the first 5GW attack. Given the enormous investigative effort expended on finding the perpetrator(s) and the fact that we have not made a single arrest, one has to believe the attack was executed by an individual or a very small group. Had more people had been involved, someone would have leaked information or been found. If this is a valid assumption, then we had a super-empowered individual or small group attack the legislative body of a nation-state using an advanced biological weapon in support of an unknown cause. This individual or

group disrupted the operation of Congress for several months, created hundreds of millions of dollars in clean-up costs, and imposed mail screening requirements (and associated costs) that are still in effect today—not a bad payoff for a few ounces of anthrax and some postage.

The anthrax attack provided stark evidence that today a single individual can attack a nation-state. Over time, the combination of political motivation, social organization, and economic development has given greater and greater destructive capability to smaller and smaller groups. While some technologists thought we had reached a peak of destructive power with the advent of thermonuclear weapons, the fact remains that creating and delivering such weapons required an elaborate and expensive developmental effort. By contrast, the following recent developments suggest that the potentially massive destructive power of bio-weapons is within reach of motivated groups:

- Three years ago, a team led by Dr. Craig Venter created a functioning virus from off-theshelf chemicals. Venter's team selected a specific virus, purchased the necessary genetic base pairs to make the virus, and then "assembled" the pairs into a functioning synthetic virus. All of the materials and equipment the team used are commercially available without restrictions. Venter has predicted that what took an elite team and a very well-equipped lab to do the first time could be done by any competent graduate student in a university lab in less than a decade.
- Paul Boutin, a science writer, decided to take up Venter's "challenge." Despite not having been in a biology lab since high school, Boutin, with a little guidance from Dr. Roger Brent to keep him out of dangerous experiments, created glowing yeast. While yeast is not smallpox, the equipment, techniques, and nucleotides Boutin used are similar to those needed to create smallpox from its base pairs².
- The complete smallpox genome has been published on line and is widely available. Boutin found it in about 15 minutes. . The nucleotides to make smallpox can be purchased from a variety of suppliers without identity verification. . Smallpox has about 200,000 base pairs. DNA with up to 300,000 base pairs has al-

ready been successfully synthesized.

- An Australian research team heated up mousepox virus by activating a single gene. The modification increased its lethality from 30 percent to over 80 percent. It is even lethal to 60 percent of an immunized population. They posted their result on the Internet. It turns out smallpox has the same gene.
- The cost of creating a virus is dropping exponentially. If Carson's Curve continues to hold true, the cost of a base pair will drop to between 1 and 10 cents within the decade. Thus, a researcher could order all the necessary base pairs to create a smallpox virus for between \$2,000 and \$20,000.⁷ The equipment he needs to assemble the virus will cost an additional \$10,000.
- Bio-hackers are following in the footsteps of their info-hacker predecessors. They are setting up labs in their garages and creating products. Last year, a young British researcher invested \$50K in equipment and produced two new biological products. He then sold his company, Agribiotics, for \$22 million. We can assume hundreds, if not thousands, of young biology students are now in their basements attempting to make new biological products.

These discrete but related events mean that it is becoming increasingly easier for a **small group** and perhaps even **an individual** to create a virus such as smallpox and use it as a weapon.³

Some experts have reassured us that even if a small group can create a biological virus, it is the testing, storage, and dissemination that are the most difficult steps in weaponizing a biological entity. They are right—if the creator uses traditional methods. However, a person can avoid the requirement for testing by selecting a known lethal agent, such as smallpox. He already knows it can thrive outside the laboratory. Storage and dissemination problems can be solved by tapping into the increasing trend of suicide attacks worldwide—he simply injects the smallpox directly into suicide volunteers, who become both the storage and the dissemination systems.

Using a few volunteers and commercial airlines, a terrorist group can create a near-simultaneous worldwide outbreak of smallpox. *Dark Winter*⁴, an exercise conducted in 2001, simulated a smallpox

attack on three U.S. cities. In a period of 13 days, smallpox spread to **25 states** and **15 countries** in several epidemiological waves, after which one-third of the hundreds of thousands of Americans who contracted the disease died. It was estimated that a fourth generation of the disease would leave 3 million infected and 1 million dead. The exercise was terminated at that time.

It is essential to remember that not only will smallpox cause an exceptional number of deaths, but it will also shut down world trade until the epidemic is controlled or burns itself out. Given that the 2002 West Coast longshoreman's strike cost the U.S. economy \$1 billion per day, the cost of a complete shutdown of all transportation will be catastrophic.

Biological weapons have the capability to kill many more people than a nuclear attack. Further, unlike nuclear weapons, which are both difficult and relatively expensive to build, smallpox will soon be both inexpensive to produce and difficult to detect until released. While I selected smallpox for this brief paper, a biologist can obviously select any of the known effective contagions. He can also attempt to create an entirely new disease. But of course no one can predict how a lab-raised disease will fare against the natural enemies it will face when released into the environment. Thus, a terrorist is more likely to use an existing disease or modify one to be more lethal. He can also release both versions of the disease—the naturally occurring virus and the enhanced virus—to insure success.

5. Summary

Drawing on changes in the political, economic, social, and technical fields, 1GW culminated in the massed-manpower armies of the Napoleonic era. In the same way, 2GW used the evolution to an industrial society to make firepower the dominant form of war. Next, 3GW took advantage of the political, economic, and social shifts from an industrial to a mechanical era to make mechanized warfare dominant. Fourth-generation warfare uses all the shifts from a mechanical to an information/electronic society to maximize the power of insurgency. It continues to evolve along with our society as a whole, thus making

4GW increasingly dangerous and difficult for Western nations to deal with.

Fifth-generation warfare will result from the continued shift of political and social loyalties to causes rather than nations. It will be marked by the increasing power of smaller and smaller entities and the explosion of biotechnology. 5GW will truly be a ***nets-and-jets war***: networks will distribute the key information, provide a source for the necessary equipment and material, and constitute a field from which to recruit volunteers; the jets will provide for worldwide, inexpensive, effective dissemination of the weapons.

The key fact to remember is that changes in the political, economic, social, and technical spheres are making it possible for a small group bound together by a cause to use new technologies to challenge nation-states. We cannot roll back those changes, nor can we prevent the evolution of war. Clearly, we as a Nation, and particularly our military, are not ready to counter the coming attacks. It's time to start thinking about how we might deal with this next step in warfare.

References

1. William S. Lind, et al, "The Changing Face of War Into the Fourth Generation," *Marine Corps Gazette*, October 1989. See also Thomas X. Hammes, "The Evolution of War: The Fourth Generation," *Marine Corps Gazette*, September 1994.
2. "Biowar for Dummies,"
<http://paulboutin.weblogger.com/stories/storyReader1439>
3. Robert Carlson, "The Pace and Proliferation of Biological Technologies," *Biosecurity and Bioterrorism: BioDefense Strategy, Practice and Science*, Volume 1, Issue 3, 2003.
4. Mark Mientka, "Dark Winter Teaches Bio Lessons,"
<www.usmedicine.com/article.cfm_articleID=322&issueID=33>.

PLANNING, PROGRAMING, BUDGETARY SYSTEM – AN EFFICIENT, MODERN AND USEFUL INSTRUMENT IN MANAGEMENTUL ROMANIAN FORCED ARMED

Lt. Col. Doina Mureșan, PhD

Associate Professor, Deputy Director

National Defence College Bucharest, Romania

The beginning of the XXth century meant deep transformations in the international architecture of security and, therefore, the prevention of conflicts and the management of crisis are based on the extension of the processes of democratization, on the promotion of human rights and national principles and on the growing role of the international community. The challenges that appeared in the process of globalization, the conflict between globalization and tendencies to regionalization and fragmentation are generating new tensions and risk factors worldwide. The global security environment, as well as the European and the regional ones, given the experience of these last years, will stay, at least for the next decade, fluid, extremely complicated and very complex, with developments often chaotic, difficult to predict, and with numerous hotbeds of tension.³⁰

Although the international system still contains some traditional features of the policy of power, Europe is heading towards a cooperation security environment, based mainly on political and economic integration and on the extension of the community of states sharing and promoting democratic values. It is becoming more and more obvious that the interests and security objectives of the states can only be attained by international cooperation. In analyzing the risk factors, the tensions, threats and global or regional challenges, Romania envisages the philosophy of getting out or, more precisely, staying out of isola-

³⁰ National Security Strategy, project, introduction

tion, the utmost participation in the international community, the assimilation of the process of democratic values and, thus, the undertaking of responsibilities in order to improve the security environment, to contribute to it rather instead of being just a consumer.³¹

In order to promote its security interests, Romania uses a range of opportunities offered by the extension of NATO and EU, the ability to play an active part in OSCE, the development of good neighbourhood relations and the strategic partnerships existing on the international scene. The accession to EU and NATO is the only rational option that guarantees the security of Romania in medium and long term. The strategy defines directions to follow in order to adapt to the actual strategic concept of NATO and takes into consideration the perspectives of the participation of Romania to the development of the European Security and Defence Policy.

The acceleration of the process of integration in the European and euro-Atlantic structures (from the point of view of politics, economy and security) and the consolidation of an undivided, democratic and prosperous Europe that can generate an extended area of stability will lead to better ways to fight risks and threats, to efficiently manage crisis and to actively participate in the common regional defence.

Romania aims at: the integration in the euro-atlantic military structures, the continuation of the reform in the army, in accordance with the standards of NATO and EU member states, the development of a reliable, modern and efficient capacity of defence; the strengthening of the civil control over the armed forces, in keeping with the principles and values of democracy; the consolidation of Romania's status of security-generator, by improving its contribution to the regional stability³². Integration must be achieved at an institutional, organizational, technical and intellectual level. This will allow the shaping and the guarantee of the forces that are necessary to achieve quick effects and to attain the desired objectives by selective and progressive use of military means. By its accession to NATO and EU, our country ex-

³¹ Ibidem, Chapter III. Risks, tensions, challenges, threats, paragraph 4.

³² The National Security Strategy of Romania, Bucharest, 2001, chapter 5, General directions in national security policy, points 5.6 in the field of national defence

pects from these organisms recognition of the values of the Romanian space, balance, European and regional stability, acknowledgement for its status of a member state that respects all commitments but that also benefits of all rights, beginning with those related to economic and social growth and continuing with those related to the European and regional security and cooperation environment³³.

Romania, by its integration in these structures, wishes to participate more actively in the economic, political, cultural, social and military trade and, on these grounds, to raise the standard of living of the population, to better fulfil its potential, for the its own benefit and for the benefit of the continent³⁴. One basic principle must be respected to achieve this desiderate: “assessing a minimum ceiling of expenses for the operationalization of the forces necessary to achieve national and military goals”³⁵, and not ensuring the functionality of the military system according to the allocated funds.

The allotment of resources is closely related to the budget provided for the process of the army reform that contains two phases: the first phase 2000-2003 intended to orientate resources towards the restructuration of the operational forces, at the level of minimum requests, by creating a military organism of smaller dimensions, mobile, flexible, that can achieve a reliable defence and a growth of the degree of interoperability in a multinational frame ; the second frame 2004-2007 intended to modernize the equipment in order to develop the battle capabilities and to increase the degree of technical interoperability with the euro-atlantic structures. The phases of the process are interwoven, and the deadline for their completion was modified according to the allotment of additional funds.

The allocation of financial resources, their repartition and consumption in relation to programs and categories of expense is an extremely complex activity that makes the object of the Planning, Pro-

³³ National Security Strategy, project., chapter X, the Strategy of accession to NATO and to the European security structures, point 4, Expectations, paragraph 1.

³⁴ Ibidem, Chapter X, , the Strategy of accession to NATO and to the European security structures, point 4, Expectations, paragraph 2.

³⁵ Strategic Vision – 2010 Romanian Army, Military Publishing House, Bucharest, 2001, Chapter VI, Capabilities

gramming, Budgeting, and Execution System (P.P.B.E.S.) of the forces, activities and resources of MOD.

With a view to increase the transparency and to establish the necessary co-ordinates for an integrated frame for the management of defence resources priority is given to the improvement of the Planning, Programming, Budgeting, and Execution System (P.P.B.E.S.), already compatible with NATO procedures. At the same time started the process of getting connected to NATO system of planning by use of the Defence Planning Questionnaire –DPQ).

Key Aspects to Achieve an Efficient System of Planning the National Defence

The security environment has dramatically changed as, besides terrorism, there is no direct threat and the main goal is to act as an efficient NATO member state. The financial resources allocated to the defence have been increased in real time, which is an essential element that influences the capacity to cover the requirements of modernization for the main equipment (this is largely above the financial resources). The reform of Romania's army is in progress, which implies reduction and restructuration of the army staff, professionalization, modernization and abolition of the excessive infrastructure. We will enumerate some requirements regarding the modernization of defence equipment: Efficient management (replacing the analogical communication technique with digital one); Implementation of STAR 2000 (the mobile component) and C41; The realization of an integrated management system of the air space (FPS-117, Gap Filler, ASOC, IFF); The improvement of the fire power, mobility and precision (TR-85 M1, MLI-84 M, GEPARD, COMBAT and efficient ammunition); Increasing the fire power of airships (MiG-21 LANCER, IAR 330 H, GHIDUL and ATTNA) ; Frigates, systems of refuelling at sea, improving the systems of sailing, communication and automatic fire; Means of individual and collective protection (NBC, equipment for special forces); Optimization of the logistic system (informatics, efficient transport); The guarantee of the physical security of the building M-100 (SIS-M100); Providing medical assistance – instruments and

medical equipment.

NATO's values and standards are closely connected to those of democracy and political transparency. The alignment of Romania's defence system to NATO's requirements and procedures aims both at politico-diplomatic aspects and strictly military aspects that define directly the military potential.

The famous analyst Jeffrey Simon (USA Institute for Strategic Studies) identifies four critical conditions for the development of the defence system, that every democratic state in transition should adopt. Here they are: A neat separation of authorities between the President and the Government (the Prime Minister and the Ministers of Interior and of Defence) by the Constitution or by laws; Parliamentary control over the army according to laws; The governmental control at peace time over the General Staff and over the military commanders by the intermediary of the civil Minister of Defence. The management of the Ministry of Defence means elaborating the budget of defence, access to information, commitment in strategic planning, development of the structure of forces, acquisitions and modernization of equipment and promotion of the military staff; The rebuilding of the military prestige, credibility and responsibility, necessary for the efficiency of the Armed Forces.

The central objective of the system of national defence is the co-operation between the Romanian army and all the public institutions in order to defend the national sovereignty, independence and unity, the territorial integrity and the constitutional democracy, simultaneously with the extending the contribution to the consolidation of peace and stability in Europe and in other regions in the world, by accelerating the reform, the restructuration and the modernization of the armed forces and by raising the degree of their interoperability with the euro-Atlantic structures.

The main objectives in order to achieve a complete interoperability with the armies of NATO member states are: restructuration, modernization and endowment of the army in a unitary frame, according to the possibilities and to the resources allotted.

In Romania this process underwent four main phases. The first

stage (1990-1993) meant mainly dismantling of structures of “Warsaw Treaty” type, testing new structures and elaborating new doctrines and concepts. The second stage (1993-1995) outlined the restructuration of the Ministry of Defence towards an organization that allows authentic democratic control, the reduction of staff and equipment in keeping with the commitments assumed by Romania.

The period 1996-2000 was characterized by an enthusiastic but insufficiently coordinated candidature to access the structures of NATO. Beginning with 2001, the process can be seen as an accumulation of previous experiences and as a sustained effort to re-establish Romania’s credibility, effort that resulted in the accession of our country as a full member. The most significant accomplishment that we should mention is the new relation established between the military and the civil structures.

The NATO member states planned an alliance of the Armed Forces in which for the militaries’ assimilation in the multinational structures it is absolutely necessary to train and educate the military staff in superior teaching institutions from our country and from abroad, so that, by its professional, cultural and social behaviour, the army can become an elite class of the Romanian society as a whole.

A major influence in the development of this process was exerted by the participation of Romanian military and civil people (both decision-maker factors and experts) in prestigious institutions such as The “George C. Marshall” European Center for Security Studies, Monterey Superior Navy School, Oberammergau NATO School, and by the assistance offered by experts from the USA Institute for Defence Analysis, a program of consultancy initiated in 1995, that can be thus considered as an organic part of the whole process. A great impact also had the CUBIC Company, which offers a broader spectrum of consultancy regarding the restructuration of the Ministry of National Defence, as well as the Britannic and German counsellors.

The reform in the field of the staff is a national responsibility. Preferably, the planning of the categories of forces should be strictly focused on missions. In reality, the structures and the army workforce are the result of some long processes of planning, in which the allo-

cated budget seems to be the key factor. Not even the best planning can be viable unless the necessary staff –qualitatively and quantitatively- can be recruited from the society. In reference to this aspect, prognostic data for 2020 was provided by the National Statistics Commission so that we can see how the predicted evolution of our country's population will influence both the quality of the incorporated force and the possibility to ensure the necessary personnel for mobilization, in territory and in specialized fields. The obvious conclusion was the necessity to create an army of proficient employees.

In the frame of the process of reshaping the army staff the "Guide of the military career" was elaborated, comprising social protection and professional reconversion strategies of the laid off laid off personnel.

In order to adjust the fighting capabilities of the new structure of force to NATO's standards and procedures, efforts are being made in these directions:

- Achieving and maintaining, mostly by national effort, a credible, modern and efficient defence capacity, based upon the action of early prevention forces, response forces, principal and backing forces.
- Providing the armed forces with modern operational instruments that can allow Romania to play an active role in NATO's and other international organizations' efforts towards conflict prevention, crisis management and common defence, to participate in multinational military peace supporting actions,

It can be achieved by modernizing the equipment that has reached less than 50% of its life expectancy and whose performance can be brought to a level close to that of the equipment of NATO member states, by acquiring, from the internal production, certain efficient technique realized with improved technology and by importing some categories of complex technique, that can not be realized in the country or that do not justify the expense. There are several major programs that are dealing with these aspects:

- Acquiring equipment to achieve command integrated systems (STAR), systems of air traffic control (ASOC, FPS-117), early

warning and electronic countermeasures (AZUR)

- Acquiring information systems and simulators for training
- Modernizing and acquiring planes (MIG-21 L, IAR-99 SOIM, C-130 etc) and helicopters (IAR-330 PUMA and attack ones)
- Acquiring and modernizing systems a.a. (VIFOR, GEPARD)
- Acquiring cannons, howitzers, ammunition and missiles
- Acquiring and modernizing armoured vehicles (TR-85 M, MLI-84M) etc.
- Acquiring and modernizing warfare ships (frigates)

The adjustment of the national defence systems to NATO's requirements and procedures is a complex process that is still being developed. This needs the adoption of an efficient management of the defence resources. The integrated approach of the management of resources takes in consideration the missions of the armed forces, the structural modifications, as well as their influence upon the military capabilities. To achieve this system it was necessary to implement a new system, the Defence Acquisition Management Integrated System. It is modern, adaptable to changes in politics, doctrines and management, and is based on team command in the spirit of total management of quality. According to this system, the acquisition process is formed by three main systems that interact and guarantee the efficiency of decisions:

(1) The system generating requirements that provide information necessary for decision, regarding the real needs of the troops that carry out missions.

(2) The system of acquisitions management that provides a structure of management and the process based on decision points

(3) The system of planning, programming and budgeting, that guarantees the decisions regarding the planning and the allotment of the necessary resources for the acquisition programs, according to the priorities set by Romania's Military Strategy.

The three systems must operate in correlation to ensure the process of program management, the efficient use of resources, having distinct but correlated responsibilities and using a unitary system of reference.

The responsibilities ascribed by the three systems go to:

(1) The **Requirement Surveillance Council** that validates and approves "The Mission Requirement Document" and "Operational Requirement Document".

(2) The **Council for Defence Acquisition (CODA)**, the decision factor in the Ministry of National Defence that, together with the Defence Planning Council, ensures the decisions making regarding the development of the acquisition programmes in the defence acquisition management integrated system.

(3) The Defence Planning Council, the body that analyses and decides the objectives and actions of major importance that need to be developed so that the Ministry of National Defence fulfill its missions, it is responsible for financial, human and material resources management;

A full interoperability with NATO member states' armies requires the restructuration, the modernization and the equipment of the army in a unitary conception, according to the possibilities and to the resources allotted. This can not be achieved without an efficient defence resources management. This is why the Defence Acquisition Management Integrated System was created. It is modern, adaptable to changes in politics, doctrines and management, and is based on team command in the spirit of total management of quality.

The main goals of the Romanian armed forces are: alignment to NATO's standards, ongoing reforms and establishing a modern, credible and efficient structure or forces. This demands important budgetary efforts and generates a significant pressure upon the transitional economy.

The planning, programming, budgeting and evaluation system implemented in the Romanian army reflects a classical approach of resources planning, endorsed and recommended by NATO's decision structures. The implementation of the objectives of the main Romanian planning documents will lead to a realistic correlation between objectives and available resources. The execution of the Planning, Programming, Budgeting and Evaluation System in the Ministry of National Defence started in 1999, with the support of American ex-

perts from the Institute for Defence Studies. The process of implementation went through till 2002, when the system became operational.

The central objective of PPBES is the correlation of efforts in all structures of the Ministry of Defence in order to efficiently use resources to achieve the planned military capabilities. PPBES ensures the management needs at a national level and the elaboration of the planning documents requested by NATO.

The Romanian implemented Planning, Programming, Budgeting and Evaluation System aims at Identifying the necessary military forces and capabilities and determining the deadline and means of their realization, as well as the costs, guaranteeing the real possibility of attaining the desired objectives, the allotment of the necessary funds in order to achieve this; Making sure that the allotted resources are being efficiently used and Proving to the Parliament and to the citizens that the public funds allocated are being properly and accurately spent.

The legislative frame for the development of the planning activity in the Ministry of National Defence was created by the elaboration of a new Concept regarding the defence planning.

Initially introduced by the Government Emergency Ordinance No. 52 of 1998³⁶, improved by the Law no. 63/ 2000³⁷ and Law 473/ 2004 on national defence planning, the Planning, Programming, Budgeting and Evaluation System permits Adopting of comprehensive methods of measuring performances; Establishing some indicatives for measuring the performances; Focusing the budgetary process on results; Possibility to level the costs on physical unity; Efficient use of resources and Transparency in public resources management.

Here are some of the advantages created by the implementation of the defence planning system. These are:

- Realizing the correlation between the objectives of the national security and the available resources, ensuring the control of the civil society over the military body;

³⁶ Published in the Official Journal no. 525 of 25.10.2000

³⁷ Published in the Official Journal no. 1052 of 12.11.2004

- Institutionalizing the rights and the responsibilities of the state's political leaders in national security issues and interoperability with defence planning systems from NATO member states;
- Providing the conditions for the development of a rational, transparent, objective, accurate process of resources allotment;
- Structuring the military forces according to the missions established by the domestic political leadership and offering the frame for an institutionalized but flexible process;
- Facilitating the control and revising the means of resources allotment, as well as guaranteeing a free circulation of budgetary information;
- Ensuring a total comprehension of the costs necessary to fulfil the objectives of the military strategy and the evaluation of the military equipment;
- Realizing a data basis to support the decisions of the allotment of resources;
- Providing a mechanism of communication between organizations that share common interests but that often have different goals and professional backgrounds, directions for measuring the performance and means to establish the value of the investments;
- It presents itself as a medium and long term planning instrument, that can be used by any organization and that represents a barrier-process against the arbitrary allotment of resources;

It allows a central approach regarding the general problems of the governmental prioritizing and offers the possibility to make rational decisions at the level of the ministerial leadership³⁸.

The Planning, Programming, Budgeting and Evaluation System of MoND's forces, activities and resources³⁹ is a group of measures and actions, by which we determine, establish, track and evaluate the activities undertaken in order to create, train and modernize the structures of army according to the missions assigned by the constitu-

³⁸ Col. (r.) William Clontz, Director for Integration Programs "Management of resources in developed democracies", International Seminary 14-15 December, Brasov

³⁹ Order of Minister of Defence M 12/2000 on implementing the system of planning, programming, budgeting and evaluation of MoND's forces, activities and resources, Chapter 1, art. 1

tional decisional bodies of the state and to the available resources. This system aims at realizing the compatibility between Romanian Army's objectives and the resources that society can allocate at peace time, at ensuring the unitary planning and programming of the activities supposed to guarantee the fulfilment of the established goals, at managing, in an integrated way, the human, material and financial resources allocated and at strengthening the responsibilities of all military structures in carrying out the approved programs and in properly using the available resources. The functioning of the system requires the existence of a relation of interactive and continuous collaboration between all structures concerned⁴⁰, as the activities have a cyclic development, on distinct, interdependent levels: planning, programming, budgeting and evaluation.

The activities undertaken by the structures of planning, programming, budgeting and evaluation at the level of the directors of MoND's major programs and at the level of other ministerial structures with responsibilities in the implementation of the objectives and requirements established by the Defence Planning Directive are coordinated in a unitary system by "Determinations regarding the planning, programming, budgeting and evaluation in MoND in April 2007-march 2007", elaborated according to the specifications of article 46 from The Defence Planning Directive 07/2007-2012.

The Planning, Programming, Budgeting and Evaluation System (PPBES) combines the centralization of the planning and development of programs with decentralization of the budget execution and elaboration, of the competition for resources and of the transparency in using the financial resources. The main actors are the program directors (chiefs of main categories of forces, chief of the Logistic Command, the chief of J6, the General Secretariat, the chief of Defence Intelligence General Directorate, chief of the Integration and Defence Policy Directorate). At the present the directors of programs have the means (and are responsible for) allotting the resources according to

⁴⁰ Order of Minister of Defence M 12/2000 on implementing the system of planning, programming, budgeting and evaluation of MoND's forces, activities and resources, Chapter 1, art. 6

the strategic priorities. Most of the expenses initially planned at central level have been decentralized and properly programmed. We can notice that the commitment of the General Staff is no longer an administrative one, by directly coordinating the funds, but a strategic one, by managing the system of requirements emission. The Planning, Programming, Budgeting and Evaluation System accomplishes the correlation between the objectives of the national security and the available resources, ensures the control of the civil society over the military body provides the conditions for the development of a rational, transparent, objective, accurate process of resources allotment, facilitates the control and revises the means of this allotment, guarantees the free circulation of budgetary information.

The Planning, Programming, Budgeting and Evaluation System of MoND's forces, activities and resources⁴¹ is a group of measures and actions, by which we determine, establish, track and evaluate the activities undertaken in order to create, train and modernize the structures of army according to the missions assigned by the constitutional decisional bodies of the state and to the available resources.

The system of planning, programming, budgeting and evaluation is not a solution for accomplishing all the army's purposes in taking realistic decisions for allocating objectively and transparently the human, material and financial resources on the requests level in world-wide plan.

We consider that, although the current budgetary system is still ponderous (nowadays it is in attention for being alienate to the European Union rules) and the programming is not a panacea, it can at least help us to accentuate the future costs for the military capacities, as to the fundament of the budgetary requests. The passage from a budgetary system based on request (necessities) to a new system based on objectives and priorities requires changes in thinking and in approaching the institutional level. In the same time, the system is "lance peak" of the progress, meaning strategic change.

⁴¹ Order of the Minister of Defence M 12/2000 on implementing the system of planning, programming, budgeting and evaluation of MoND's forces, activities and resources, Chapter 1, art. 1

Through the lessons learned since the pilot phase of implementation, must be mentioned the re-alignment of the programs in order to grow the power of decision (and of responsibility) of the beneficiaries (especially the army's categories of forces) on the allocation of funds for specific requests.

Thereby, the structures that previously had a role in control and execution (J6 – on tactic level, The Department for Armament, The Direction Fields and Infrastructure) have more liberty in exercising the role of control.

The system operationalization brought important changes regarding the correlation of the objectives with the resources, significant growth of the implementation speed of the programs and it can be considered as the effect of the SPPBE implementation.

Into the Ministry of National Defence this year is dedicated to the improvements of the planning structures at level of program manager, as to the total integration of the budgetary execution into the system. The last evaluation made by NATO's Experts mention:

"Romania has made important progresses in establishing a system of defence planning that is compatible to those of NATO countries. The defence planning is based on procedures and responsibilities well defined and on a large set of planning documents."

The programmatic frame of the Romanian Armed Forces was established by the 9 Defence Programs on a period between 2003 and 2008. An effort of testing the system was made in 2000 and continued in 2001. The process will be perfected once the experience is gathered.

In conclusion, the System of Planning, Programming, Budgeting and Evaluation of the Ministry of National Defence offers the necessary means to take realistic decisions, to allocate objectively and transparently the resources, forming a modern, useful and efficient planning instrument. We appreciate that its total implementation will represent a major step for realizing the inter-operability with NATO. In comparison to three new NATO members, we consider that Romania keeps the same rhythm regarding the defence planning.

Endnotes

The Counsel of European Community, IV Directive from regarding the annual financial situation of the societies;

Instructions regarding the planning, programming, budgeting and evaluation of the forces, activities and resources in MoND, D.P.I.A., Bucharest, 2000;

Professional Norms approved by the Superior Counsel of the Body of Expert and Licensed;

Manual NATO, Office of Information and Press, NATO-1110, Brussels – Belgium, 2001;

Accord of standardization NATO (STANAGs);

The documents from the base data of the Finance-Accountancy Direction - from MoND;

SOCIAL SECURITY IN THE CONTEXT OF EUROPEAN SECURITY STRATEGY (CHALLENGES AND RESPONSIBILITIES OF BUSINESS)

Assoc. Prof. Stefka Dacheva, PhD

Department of Information Technologies and Communications,
University of National and World Economy

Summary

The social security is investigated as a national priority for Bulgaria in the context of European security strategy. The social responsibility of business is still a challenge for Bulgarian enterprise due to deficiencies in the internal and external security environment. The interaction between the business and the state is in the bases of European security strategy including the rise of welfare of citizens and their security. It is stressed upon the application of analytic models for social security taking into account the different development concepts and the significance of ICT in the process for the profit of business.

Key words: structural characteristic of social security, vector of crucial dangers for social security and business, security index.

The European policy and strategy set in 2003 stress upon the problem of the security of the state system. From the view point of social security this focus is implicitly contained in the ability of the state to guarantee the welfare as a priority in the concept of national security. The limitation of the dangers, threats and risks in that direction inevitably concerns the functioning of the basic subsystems that guarantee the social security. Among them the subsystems of education, health care, internal order and security for citizens, including their property, by restricting the influence of such a risk factor as juvenile delinquency. From the view point of keeping safe the state system as one of the goals of European security policy of crucial importance are

the dependencies between:

First. The public expenditures guaranteed from the state for the so called social transfers, which are defined as “substitute” incomes in this work. The relation between the three basic groups of incomes – labor incomes, incomes from property and substitute incomes, should be estimated through criteria for the real profit that they guarantee to the citizen. The underestimation of such type dependencies leads to reproduction of the different social systems without clear criteria for their operation and for achieving concrete gains corresponding to the needs of the citizens.

Second. The estimate of the interaction of different subsystems that guarantee social security should rely on the degree of effective communication and coordination between them and with basic structures of the civil society, representing the interests of target groups of consumers and professional groups. The coordination over the national level, including the European community level, fix the direction for modernization of state system as a process developed on the base of European democratic values and the social rights of the citizens.

Third. The state system ensures the achievement of social security and through legitimating of business profits, the social responsibility of the private entrepreneurs in the interest of population at national, regional or local level. The strengthening of the processes of legitimating the national identity of business is the natural way for confining unconventional payment moreover without clear criteria for the quality of the services defending basic social rights. In this process the state is only one of the subjects of regulations needed for business legitimacy. The other subject is the active community of citizens by the earnings of which the operation of every one subsystem that guarantee the social security is supported. European security strategy includes also priorities in military area, defense, measures against terrorism, the accomplishing of which also depend on the security of the state system in every single country. The help that Bulgaria receives in the frame of European security strategy is one of the basic resources to limit the dangers, the threats and risks for the state system in the aspect appointed above.

The bilateral and multilateral agreements in support of European security strategy are another potential resource for strengthening of the state system of every member state of European community. The strategic partnerships of EU with USA, Russia, China and India have considerable importance for European security.

A priority is the strengthening of strategic dialog between EU and USA. The main component is the collaboration in crises management and conflict prevention. Equally important is intensifying economy and trade collaboration, joint work in energetics, collaboration on regional matters and relations with third parts, for example the nuclear program of Iran.

The strategic partnership between Russia and EU continues to develop and is especially important, particularly in energy area. Primary economic and trade partners of EU in Asia are China and India.

The importance of these strategic partnerships is undoubted. The responsibility of Bulgarian state is the stimulation through adequate regulations of business in its aspiration to have active presence on European and international markets. The information communication technologies (ICT) stimulate these processes globally and modernize the rule of business and the state.

The development means improvement of the manner of life through better education, higher incomes, development of skills and better employment, more care for elders, children and people with disabilities. The development means that people must have suitable living conditions, healthful and secure habitation. The development means also that people must have literacy, the number of ignorant people should be reduced under a healthful minimum through social protection activities and programs for continuous education. This is a problem of crucial social importance especially for rural regions or for settlements with compact ethnical population. For instance nobody argues the opinion that in order to develop and to achieve better life the Bulgarian Roma should receive better education. As the ignorant people do not develop as well as the educated people it is important for all the people to strive toward better education or to send the children to school in order to receive such education.

In the various definitions of development the basic component is the information.

The information communication technologies and telecommunications contain the answer of substantial importance for the development concept, namely how this information is disseminated, spread and reaches the people. There are different reasons to disseminate information: information about new technologies in industry and in agriculture, new raw materials, city planning, building in the community, health (e.g. AIDS care), educational and informational campaigns and so on. The educational process relays on informational dissemination of ICT as the information teaches (or information is instruction) and ICT spread education or information. Through the communication using ICT the world is a global village where the people of a country get acquainted for the developments in many other countries from the news reports. ICT and the traditional mass medias, such as TV, newspapers and radio broadcasting are therefore some of the elements of the system for transfer of information in international communications.

When certain country makes investments in education that is productive investment because the well educated labor force promotes the productivity. But to be educated doesn't matter if the educated man has not a good health and acceptable housing, if this education could not help to the person to find a good job in order to live, to advance, to receive good health care, to buy a good house, to educate his children and to keep his living standard. Otherwise the development should improve all these aspects of the life that define the so called "multidimensional development". ICT are used to share educational information between the peoples and the countries again for the purpose of development. Consequently one could hardly speak for independent development taking into account the mutual over national connection of the different countries. We agree with the authoritative economist from the World Bank Joseph Stiglitz who considers the "development as a transformation of the society".

The theoretical idea in achieving social security is reasoned in such understanding of development as a movement of the society from

traditional relations, traditional mind, towards optimal social perspective. Naturally this includes the necessary transformation of traditional methods of production in modern methods.

The modern social perspective adopts the necessary change that we as individuals and the societies could undertake actions in order to achieve for example reduction of mortality-rate and increasing the life expectancy and productivity. The ICT influence this change from traditional to modern contemporary societies through the process of information transfer, explained above. For instance the telecommunication technologies, the mass medias and their content influence the manner and the style of life of the people in many countries world wide due to the content that dominates the local medias as TV, Internet and Web TV, especially in countries, where telecommunication infrastructure for access is created. Bulgaria has not guaranties against these new forms of risk, especially for children. A society intolerance and activity against dissemination of porno movies at school with the participation of pupils, and sometimes of teachers, violence in different forms – from sexual abuse to purely physical maltreatment.

The theoretical basis for the analysis of the problem is the social content of the development concept. It is characterized from two basic theoretical perspectives.

The first one is the so cold “technology and economics” perspective.

The second one is the “cultural” perspective in the development of the community and the individual.

The main characteristic of the “technology and economics” perspective in the development of the community is that it is a perspective “from inside to outside” and “from up to down”. The human creatures are considered mainly as factor for economy, as economy agents of the market and the major kind is that of the “market man”, who organize and follow in his activity the economic interest and profit. From this point of view the advance of technologies is a necessity for economical development. The social and cultural factors remain in the background.

The characteristic of the cultural perspective of the development

of the community could be presented with the following research accents:

- Close connection with the political development, politics and regulation reform.
- Close connection with social development, the democratization and human rights struggle.
- The technological development is a necessity for the economic development and the economic development must help the public and cultural development.

The cultural perspective is leading aim for different media forms to build a bridge over the digital divide and in this way to close the information gap between and inside the smaller groups as the family. The leading aim is to propose adequate, cultural and socially sensitive information. The media is selected to be suitable for the society. The perspective is information (software) with dominant social and cultural orientation. Both theoretical perspectives use the abilities of ICT to establish the aims of communication supporting the development.

In this broader theoretical scope the new paradigm “communication of the development” is revealed. In 70’s alternative paradigm (called “alternative of the dominant paradigm”) was formulated known as “pluralist” perspective or another development. In a tight frame the followers of the pluralist perspective recognize the failure of former models of the development and accept a few new approaches to the development inclusively with respect to its goals, namely:

- The movement must promote participation at all levels;
- The development must support the equal access;
- The development must support the public values;
- The development must correspond to local culture, values and norms.

In the scope of theoretical approach to the development the role of communication is described as communication supporting the development of the community. The main accent is on bidirectional, interactive, with active participation, communication, in response of unidirectional, from up to down, piped and restricted communication.

Another model of development is that based on communication

with participation. It is oriented towards people, as it supports the idea, that all connected with development must have the possibility to share and collect their ideas and to help the different innovation projects in development including the social programs and projects of governments and different authorities on central and local level.

The main frame of this kind of investigations adopts that the functional characteristics of the development includes dialog between institutions and dialog with the citizens. The social groups in the society have special meaning in this model of development. For instance it is stressed upon the crucial role of the women in development and international communications. The state, the political authority, the national governments and local authorities in the regions must support this role of women for the development of the country and the regional communities.

The security environment during 21 century is dominated of information communication technologies. In the same time their application contributes for positive economical, social and cultural development. But it is possible as well these ICT to have negative influence on the targets of public development. For instance the reconstruction and especially the privatizations of state propriety (such as BTC) lead to loss of working positions what is negative contribution to the development of the country.

The poverty and the loss of working places is one of the dangers and threads for the national security. They rise other danger connected with increasing of criminal activity and inclusion of young people and children in international criminal groups and human traffic. Conversely, if the reconstruction of state property does not lead to loss of working places but creates such places in newly privatized sectors of economy, that implements positive development, because more working places promote economic development, decrease the risk of poverty and confine the criminality.

Originally the social security was mentioned in Universal Declaration of Human Rights from 1948. But in this declaration the concept was used only descriptively. In article 22 the common will of signed states is expressed to create in their own countries the necessary con-

ditions that guarantee the social security of citizens. In Declaration is written: "Everyone, as a member of society, has the right to social security and is entitled to realization, through national effort and international co-operation and in accordance with the organization and resources of each State, of the economic, social and cultural rights indispensable for his dignity and the free development of his personality."

As it is seen from this fundamental for human rights document with respect to human rights and international relations the lack of social security is considered as absence of one of basic conditions for normal life of the human creature – the aggregate of "one or more factors which make the individual and the families capable to accept their fundamental responsibilities and to implement their fundamental rights". The meaning of social security and protection finally is connected with tranquility in the home of everybody and the real need of it for the functionality of the society itself.

As fundamental subsystems the interaction of which guarantees social security and confines the threads and risks for it the author considers the following:

- order and security,
- labor, employment and welfare,
- education,
- health,
- security of business,
- limitation of new social dangers of net society as criminality for children and young people,
- human traffic – labor and sexual exploitation,
- information security and net crimes including with involvement of children and young people.

Every one of mentioned subsystems contains potential resources for safety and limitation of threads and risks for the social security. As it was already mentioned the origins of such threads and risks contain:

- institutional defects of different public central and local institutions,
- inconformity in norms of their regulations,

- faults in realization of reconstruction of some of subsystems.

All these aspects of the process of achieving of social security require specific research approaches and tools. For example, for the sake of comparative analysis a security index is elaborated that represents the dynamic of criminal activity in EU. It is based on official Eurostat data for the crimes in 14 member states for the period 2000 – 2006. The data are presented in tables for the number of crimes of certain kind at 1000 people in every selected country including Bulgaria.

The comparative analysis is made for Bulgaria and three groups of countries:

- The group of “large” countries contains United Kingdom, France, Germany and Italy.
- The group of “small” countries involves Belgium, Netherlands, Portugal and Finland.
- In the group of “neighbor and close” to Bulgaria countries are Greece, Romania, Slovenia, Hungary and Austria.

The security index $FC(t)$ for certain country, e.g. Germany, is obtained for selected year t , say $t = 2001$, by appointing to every data type quantity Q_i an estimate $q_i(t)$ varying from 0 to 10 obtained from the formula

$$q_i(t) = 10(Q_{\max} - Q_i) / (Q_{\max} - Q_{\min})$$

Then the security index is

$$FC(t) = \sum_{i=1}^k P_i q_i(t),$$

where the weights P_i are nonnegative numbers with sum equal to 100 and k is the number of different kind of crimes. The integral security index is greater for less criminal activity. The results of computations are presented in following table.

Security index *FC*

	2000	2001	2002	2003	2004	2005	2006
Austria	737,70	762,40	736,05	699,29	658,98	682,02	703,38
Belgium	324,55	332,43	314,63	399,13	437,05	461,73	459,38
Bulgaria	732,01	745,42	766,78	774,70	787,97	820,53	831,58
Germany	735,79	741,46	739,86	747,35	745,39	760,75	773,12
Finland	516,81	517,75	618,02	642,13	623,13	666,48	688,07
France	574,43	532,53	537,83	579,32	608,86	622,12	634,87
Greece	836,09	824,89	836,33	826,73	857,26	835,59	836,86
Hungary	780,21	758,18	789,24	791,27	784,15	798,54	806,00
Italy	680,84	695,70	701,99	693,77	707,37	712,37	690,13
Netherlands	588,99	562,77	556,00	556,68	588,27	619,41	642,05
Portugal	747,35	741,60	720,57	706,17	704,02	727,35	717,29
Romania	898,28	896,58	905,96	912,59	919,56	931,35	928,52
Slovenia	848,40	884,50	849,91	888,53	853,71	875,54	872,17
United Kingdom	373,49	325,17	290,76	322,54	381,90	406,01	418,36

The trends could be seen well on the following figures where the results for a group of countries and Bulgaria are visualized. In first figure Bulgaria is compared with United Kingdom, France, Germany and Italy.

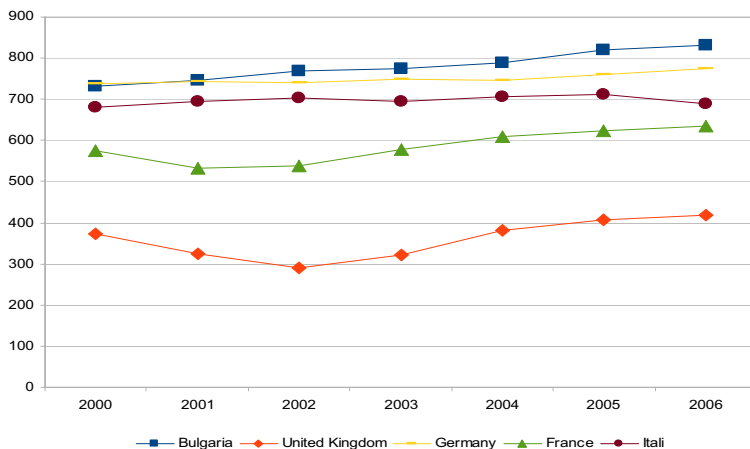


Fig. 1. Security index *FC*

It is seen that the security index for Bulgaria is most high, that is the criminal activity is most low during considered period of time. The security index is most low for United Kingdom.

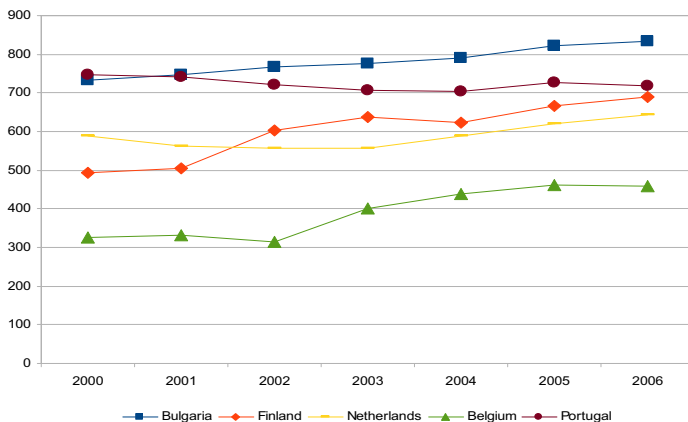


Fig. 2. Security index FC

In next figure Bulgaria is compared with Belgium, Netherlands, Portugal and Finland. The lowest criminal activity is in Bulgaria, the most high is in Belgium.

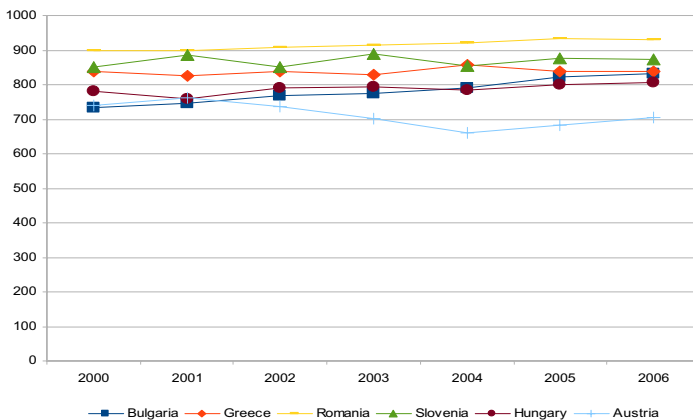


Fig. 3. Security index FC

In figure 3 Bulgaria is compared with Greece, Romania, Slovenia, Hungary and Austria. The lowest criminal activities have Romania, Slovenia and Greece and since 2004 next comes Bulgaria. The highest criminal activity is in Austria.

The social responsibility is considered in the context of social dimensions of the economic growth, adopted by European community as social rights of the citizens and the responsibility of business organizations for their protection. The legitimacy of the profits, their distribution, also for social protection of workers, identification of business organizations as subjects of social development of regional communities – this is the field of author's theoretical arguments for achieving of corporative social responsibility.

The Bulgarian business persistently announce its desire to take part in public process of creating legislation and this especially clearly reveals in already accomplished to a large extent ambition of business to participate in local parliaments and executive power at recent local elections in the country. For the business it is not sufficient to influence through lobbyism but it intimates the desire to be legitimated as a subject exerting the power.

The process of legitimating of business involves the possibility of awareness of its social responsibility. That is not only with respect to the people employed in business organizations, but also with respect to the local or regional community where operate these business organizations. No matter that the concept of corporative social responsibility in the country is now perceived as modern ideological construction, it contains potential for legitimacy of profits of business organizations and strengthen of their corporative identity. There isn't more popular and accessible way for a company to be accepted well in the society or in regional community respectively, to establish its image, to be recognized as a place for professional implementation and career development through the included in economical growth social activities that the company can organize and have resources to support for their workers and employees and their families, and at a subsequent stage also for regional community. The different forms of public-private partnership are the other possibility to achieve corpora-

tive identity of business organizations which have to participate and implement social programs of interest for the citizens, in collaboration with or parallel to the local authorities and the public social sector.

The social responsibility in the context of the proposed working hypothesis reveals as structure determining element in market behavior of the organization. It is supposed that parallel to economic targets of development should be determined also social goals both obeying to the criteria of concurrent growth of organization and dynamic presence at the market. So, the strategy for economy growth, have to involve arguments for concurrent social development of the organization. The presented above comprehension for corporative identity of the organization, through its social responsibility includes also a projection of social responsibility on the life of local communities in the regions. The gain of confidence and prestige could not be achieved with accidental and campaign driven behavior and activities, to a less extent they can influence accumulated during the years negative public attitudes to the business.

DEFENCE R&D POTENTIAL IN BULGARIA AFTER 1989

Assist. Prof. Konstantin Poudin, PhD

Department “National and Regional Security”

University of National and World Security

“...A strategic goal for the next decade: to become the most dynamic and competitive knowledge based economy in the world”

(Lisbon 2000 EU Council Strategy objective)

Development and maintenance of defence R&D potential is a challenge before actors engaged with defence R&D, such as government institutions, scientific and academia organizations, other NGOs – foundations, independent institutes and business sector. All of them have a specific role. The government has to give strategic direction, prioritizing R&D and defence R&D in the country and creating suitable internal environment. It includes allocation of enough money and its well management, enact of proper legislation, establishment of good communications with all other organizations and among them, establishment of useful contacts with foreign structures as well. Business sector plays a dual role. In the first place it is end user of the results of R&D activity. That is why it is the driving force of the researches. In the second place it carries out R&D activity, maintaining its own potential. This is so called “applied science”. In both cases private companies invest money. Academies, universities and all other NGOs are directly involved in R&D. Their activity is the base of “fundamental science”.

This paper presents the development of defence R&D potential in Bulgaria after 1989. It has mainly informative goal. Some ideas of the future of the defence R&D potential are presented and analyzed as well.

Defence R&D potential 1989 - 1999

A well developed system of scientific entities in defence, including Military Industrial Complex /MIC/, existed until 1989. A lot of highly qualified specialists worked there. They were perfect in the implementation of Soviet licenses and technologies, and the start of special production.⁴² In the beginning of the 90-s the main scientific institutes working for the needs of defence were: Military scientific and technical institute, Military institute of design and technology, Rear institute, Navy scientific and technical institute in MoD and Military research institute of the General Staff. All of them had well build laboratories, research and production base, libraries and technical archive, keeping all documentation of the research projects.⁴³

Besides, almost every bigger producer from the MIC had own scientific institute – e.g. NITI – Kazanlak, the institute of “Arcus” – Lyaskovetz, the institute of VMZ – Sopot, the institute of “Dunarit” – Ruse, Elektron Progress – Sofia etc.

The R&D activity in defence sector was seriously affected by the political changes and the economic reforms after 1989. In the beginning of the 90-s, more than 1000 highly qualified researchers worked at the Bulgarian military institutes. Between 1992 and 1996 the first reorganization was conducted. The number of working specialists in the system of military science was reduced to about 600.

The reforms of the science in defence sector run most intensively after 1997. In this period the modernization and reorganization of the BAF started. Unfortunately the R&D activity was ignored and the financial resources for it were considerably diminished. Even more, in 1998 and 1999 no money was allotted for R&D in defence sector. The standpoint of the MoD leadership was that in the future the defence could relay on civilian research organizations.⁴⁴

⁴² Radev, V. “Economic aspects of the management of defence R&D resources and the reform of the BAF”, collection with reports from workshop in Economics of Defence and Security “Balkan Security and Reform of the Armed Forces: Economic aspects”, p. 141, Sofia, 1999

⁴³ Pashev, G., “The lack of R&D strategy and priorities was a shortcoming”, interview with Col. Dr. M. Patechkov, Bulgarian army, 29.03.2006

⁴⁴ The same source, 23.03.2006

According to the Concept for reduction and consolidation of the scientific institutes in defence, based on the Plan 2004 for modernization and reorganization of the BAF, a Defence Advanced Research Institute /DARI/ had to be created. It would include all other institutes of MoD and General Staff. At the beginning of the reform about 350 researchers had to work for it. Their number would be reduced to 150 in 2004.

In 1999 DARI was established but according to government decree it became a part of “G.S.Rakovski” Defence and Staff College /“G.S.Rakovski” Military Academy since 2009/. Their staffs have been 25 researchers for a long period of time since its establishment.⁴⁵

The lack of money constrained the producers from MIC to restrict or totally liquidate their R&D activity. Many highly qualified specialized were dismissed, some of them relinquished because they could not accept the low payment. /Fig. 1/

In 1999-2001, the R&D activity of MoD was administered by Defence Planning Directorate of MoD and was carried out by some institutes of Bulgarian Academy of Sciences /BAS/, Technical University – Sofia, University of Chemical Technology and Metallurgy – Sofia, University of National and World Economy /UNWE/ – Sofia.

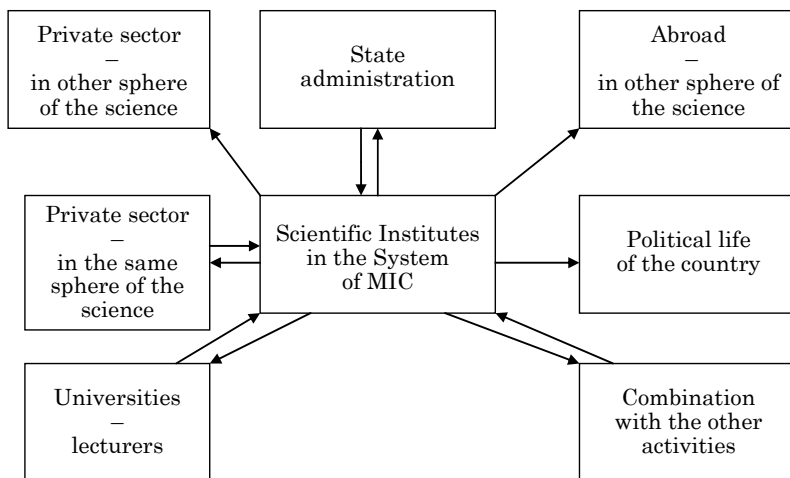
According to V. Radev the administration of defence R&D from 1990 to 1999 was chaotic, without national strategy and if there was a successes, it was due to a remained past potential and good management of the leaders of particular scientific teams.⁴⁶

Defence R&D potential after 2001

After 2001 the defence R&D continued to be carried out by state scientific and academic entities but a lot of non-government organizations /NGOs/, established during the government of the United Democratic Forces and in the beginning of the government of the royal party – National Movement Simeon II, successfully found their niche. The activity of these organizations in support of defence R&D, mainly

⁴⁵ The same source, 23.03.2006

⁴⁶ The same source, p. 146, Sofia 1999



**Figure 1. Movement of scientific specialists
from the defence industry after 1989⁴⁷**

with expertise and development of different projects funded by foreign donors – NATO, EU, UN and some western governments, was positively accepted by the society as a symbol of its democratization. Most of played a significant role on Bulgaria's road to NATO and EU membership. Despite that fact their contribution for the development of the fundamental science was not big.

Studying the security sector reform /SSR/ in Bulgaria in the beginning of 21st century and the role of the institutions of the civil society, N. Pavlov points out that there is an extensive wider "security community" in Bulgaria. In fact there are a number of NGOs active in the security area. Some of them are an individual, business card and

⁴⁷ Radev, V. "Economic aspects of the management of defence R&D resources and the reform of the BAF", collection with reports from workshop in Economics of Defence and Security "Balkan Security and Reform of the Armed Forces: Economic aspects", p. 143, Sofia 1999

notepaper. A few, though, do substantial work – NGOs such as:

- The Atlantic Club of Bulgaria,
- Centre for the Study of Democracy,
- “George C. Marshall” Association – Bulgaria,
- “Democracy and Security” Foundation,
- Centre for South-East European Studies,
- Institute for Security and International Studies,
- Institute for Regional and International Studies.

Considerable work regarding SSR in Bulgaria has been done by academic institutions such as the Centre for National Security and Defence Research at the BAS and the Department National and Regional Security at the UNWE.⁴⁸

In the beginning of that period the state did not have clear concept about national R&D policy and national defence R&D policy. These were the last years of Bulgarian political and economic transition in which the science was put in the background. The business, striving for making bigger profits, demonstrated weak interest in development of applied science. It was not interested in development of fundamental science by the academic and scientific institutions as well. Most of Bulgarian defence industrial companies /some of them privatized/ were not able to start any R&D activity. It did not make sense for many of them. The number of innovative companies was small. /Table 1/

In the context of Bulgaria’s membership in NATO and EU the national government started paying more attention to the scientific and technological development in the country. Two very important documents were adopted Innovation Strategy of the Republic of Bulgaria and Measures for Its Implementation in August 2004 which is modified in 2006 and R&D Stimulation Act in October 2003. Ministry of Economy, Enterprise Policy Directorate and Ministry of Education, especially National Council of Scientific Researches and “Scientific Researches” Fund had to pursue the national scientific and innova-

⁴⁸ Pavlov, N., “Democratic control of the security sector as an informal condition for Bulgaria’s EU membership”, December 2006

tion policy.

After Bulgaria becoming member of NATO in 2004 and in the context of transformation processes of the Bulgarian Armed Forces /BAF/, MoD also activated its R&D policy. Some documents were adopted, such as: Regulations for R&D activity in MoD and BAF in 2004, Regulations for management of the life cycle of the product in MoD and BAF in 2004, etc. According these documents, several directorates from MoD special administration and expert committees /e.g. - Defence Acquisition Council, R&D Consultative Council etc./ are in charge with formulation and realization of the defence R&D policy.

In 2006-2009, the period of SfP-982063 project, the situation regarding defence R&D did not change significantly. It looks as follows:

- The states has declared scientific and technological development as priority for all spheres of the social life;
- Several institutions are responsible for R&D activity and defence R&D activity in particular, such as Ministry of Education, Ministry of Economy and Energy, Ministry of Defence. Sometimes the coordination between their actions is not good enough;
- Several scientific and academic organizations – civilian and military once carried out research activity for the needs of defence. Unfortunately the results of their work most often do not find practical implementation. There are some NGOs having potential to fulfil particular projects;
- Bulgarian research institutions look for partners from other European countries for short or long term cooperation;
- Few companies carry out R&D activity and few of them are interested in keeping potential for such activity /Table 1/. The business demonstrates weak interest in the implementation of scientific products.

Having in mind this situation the future of defence R&D have to be oriented to more cooperation between actors in the country and cooperation between national entities and foreign institutions. The state has to continue stimulating R&D activity. Clear government R&D policy need to be elaborated and implemented. The results of SfP Projects could be very useful in this context.

Table 1

**Bulgarian Defence Industry Producers, Property,
Activity/Products
and
Market Segmentation - 2006**

THE NAME OF THE PRODUCER	PROP-ERTY	ACTIVITY / PRODUCTION	MARKET SEGMENTA-TION
AVIOTEHNIKA	Private Property	Design and production of gliders - targets and aviation services.	-
ARCUS	Private property	Production and trade with military and civilian articles, such as: pistol 9x19 mm, grenadier 40x46 mm, fuzes etc.	Special production: – 10% national market; – 90 % foreign market. Civilian production: – 20 % national market – 80% foreign market
ARMITEH	Private Property	Electronics	Special production: – 100% national market; Civilian production: – 100 % national market
ARSENAL	36 % - State Property 64 % - Private Property	Development, production and trade with light and artillery weaponry, ammunition, gunpowder, caps etc. Among the most popular products of “Arsenal” are: Submachine-gun “Kalashnikov”; Pistol “Makarov”; Machine-Pistol “Shipka”	Special production: – 7 % national market; – 93 % foreign market. Civilian production: – 9 % national market – 91% foreign market

THE NAME OF THE PRODUCER	PROPERTY	ACTIVITY / PRODUCTION	MARKET SEGMENTATION
BESTTEHNIKA-TM-RADOMIR	Private Property	Metallurgic activity	–
BETA INDUSTRIES CORPORATION AD	Private Property	Machine-building	Special production: – 0 % Civilian production: – 70 % national market – 30% foreign market
BITOVA ELEKTRONIKA	Private Property	Electronics	Special production: – 20% national market; – 80 % foreign market. Civilian production: – 100 % national market – 0 % foreign market
VIDEKS LTD	Private Property	Development and production of explosive products – hand grenade and engineering ammunitions;	–
VMZ	State Property	Production of special and civilian products – artillery ammunitions, anti-tank unguided missiles, anti-tank guided missiles, fuzes etc.	Special production: – 3,89 % national market; – 96,11 % foreign market. Civilian production: – 98 % national market – 2 % foreign market
GAMA PROEKT AD	Private Property	Manufacturing of specialized machines and equipment, Production of medical apparatures	Special production: – 100 % national market; – 0 % foreign market. Civilian production: – 90 % national market – 10 % foreign market

THE NAME OF THE PRODUCER	PROP- ERTY	ACTIVITY / PRODUCTION	MARKET SEGMENTA- TION
DUNARIT AD	8 % State Property 92% Private Property	Production of anti-fire equipment, industrial explosive substances and blasting system, plastic and elastic explosive materials etc.	Special production: – 0 % national market; – 100 % foreign market. Civilian production: – 90 % national market – 10 % foreign market
ELECTRON PROGRESS AD	Private Property	Electronics	Special production: – 100 % national market
ELOVITZA AD	-	Production of hand grenades and ammunition	–
ZEBRA AD	-	Production of protective clothing, gas masks and filters, rubberized rollers etc.	– 70 % foreign market – 30 % national market
INSTITUTE OF METAL SCIENCE AND TECHNOLOGY OF METALS – BAS	Private Property	R&D	Special production: – 5 % national market; – 95 % foreign market. Civilian production: – 80 % national market – 20 % foreign market
IMPULS AD	Private Property	Production, R&D activity, Trade Electronics	Special production: – 0 % Civilian production: – 24 % national market – 76 % foreign market
METALIC BCP	Private Property	Metal casting	Civilian production: – 71 % national market – 29 % foreign market
MIHAN AD	Private Property	Electronics and Communication Systems	Civilian production: – 90 % national market – 10 % foreign market

THE NAME OF THE PRODUCER	PROPERTY	ACTIVITY / PRODUCTION	MARKET SEGMENTATION
MONBAT AD	-	Production of accumulators	Civilian production: – 35 % national market – 65 % foreign market
MUSALA AD	-	Production of accumulator batteries	–
NITI	State Property	R&D and production of ammunitions	Special production: – 78%. Civilian production: – 22%
OMZ	0,7% State Property 99,3 % Private Property	Production of optic sight	Special production: – 0 % national market; – 100 % foreign market. Civilian production: – 73 % national market – 27 % foreign market
OPTICOELEKTRON GROUP AD	Private Property	Production of optic system and products	Special production: – 24 % national market; – 76 % foreign market. Civilian production: – 4 % national market – 96 % foreign market
OPTICS AD	Private Property	Production of optic system and products	Special production: – 63 % national market; – 37 % foreign market. Civilian production: – 8 % national market – 92 % foreign market
RADOMIR METAL AD	Private Property	Metallurgic activity	Special production: – 15 % Civilian production: – 85 %
SAMEL 90 AD	Private Property	Electronics and Communication Systems	Special production: – 25 % Civilian production: – 75 %

THE NAME OF THE PRODUCER	PROPERTY	ACTIVITY / PRODUCTION	MARKET SEGMENTATION
TEREM	State Property	Repair of all kind of land forces vehicles, naval ships and aircrafts	Special production: – 60 % national market; – 40 % foreign market. Civilian production: – 55 % national market – 45 % foreign market
CHERNO MORE	State Property	Electronics and Communication Systems	Special production: – 47% national market; – 53 % foreign market Civilian production: – 14 % national market – 86 % foreign market

Source: MoD issue – “Defence Industrial Policy of the Ministry of Defence of the Republic of Bulgaria”, 2006

Reference

1. Pavlov, N., “Democratic control of the security sector as an informal condition for Bulgaria’s EU membership”, December 2006
2. Pashev, G., “The lack of R&D strategy and priorities was a shortcoming”, interview with Col. Dr. M. Patechkov, “Bulgarian army”, 29.03.2006
3. Radev, V. “Economic aspects of the management of defence R&D resources and the reform of the BAF”, collection with reports from workshop on Economics of Defence and Security “Balkan Security and Reform of the Armed Forces: Economic aspects”, Sofia, 1999;
4. Rangelov, A., “Defence industry needs a co-ordination body”, interview with Assoc. Prof. Dr. Dimitar Dimitrov, “Bulgarian army”, 26.05.2009.

ABOUT SOME PROBLEMS AND OPPORTUNITIES TO INNOVATIONS

Lt. Col. Nikolay Atanasov, PhD

BGR AF HQ, A3

Department "National and Regional Security",
University of National and World Economy, Sofia

In the report I support the idea that there are needs for innovations and inventions in the area of the security and defence because the technologies and the human potential depend on the level of quality and quantity not only of the information and knowledge. There is unknown unity of try and lessons learned and new costs, value and competition, mind and wisdom, new crises and development of the crisis management.

Problems

In the public areas for the security subjects write and speak usually in general. But the political and military, economical and social security's define the underlying frameworks of the being and development of the contemporary economy and information society on the base the industries, science and dynamics of the enlargement in the social and economic relations. They determine a need of interdisciplinary multi system researches through which to be analyzed and presented the entity of these kinds of securities from the viewpoint of novelties and good and better practices and collaboration. The meaning of the same researches is especially topical with a deficiency by on one hand, and by the other hand, it is close to lose of information and a philosophical cognitive sense. It is esteemed just with opportunity for reasonable choice of more safe and security decisions in the political and social societies and markets of competition. Therefore is increasing the cost of the searches and innovations also in a correlation

with the European cooperation.

By origin the innovation is a problem of the new as any sort of way and whenever and wherever from everyone and in whatever relation and connection to be something unknown fully or particularly given. This is a precondition that gives information and warning for something important and estimated. The difficulty is in what meaning it exists and will be used for development of the information and knowledge, economy and society and union of societies and economies.

With the scientific and economic innovations and inventions the multidimensional information unit and knowledge change faster and more than a subject and teams can think and imagine, and search and manage it. The Philosophy of the economy and the information society has a new age-long join object – the multidimensional information innovation, technologies and knowledge.

The area of the NATO and European security and defence with the new world's threats and risks need more innovations that someone could imagine and plan, and represent on the markets. Therefore the economic research and analysis, information and knowledge have important role for projects and programs to business and science which seek resources. The innovations could change the management and the management could change the life with or without the innovations if there have others, which are more useful and effective for the life, values, freedom and security of the societies.

The innovations and the inventions have indefinite or unknown exactly conditions and environment in which they will or do happen. In this significance of reflections seeking of the devices that enable realizing of the ideas and plans could help for the improvement of the management and widening of the markets. Nevertheless, if there isn't a market there is a society and economy. There is not also constantly an objective complex model and by structures and functions full integrative innovative political, social and economical system for equal changes in the effectiveness. Such model of question is a challenge for students, researchers, creators and managers.

Military defence and security have integrated character of transformations. The experience of commanders and headquarters and

troops is the base of operational capabilities and acquiring of new such, and for effective participation in operations. But there isn't a creative Mind of the transformations, competitive cooperation and economic efficiency without the European Philosophy.

The European Innovation in the areas of the defence and security is not only an idea and priorities. Its reality and actuality require work with more than only European Mind. It is a need to reach the standards of the world requirements and upper, for example for Euro Army within cooperation. The European Philosophy and European and NATO Innovations transform the Bulgarian Army, economy and society faster than we try to recognize it. Therefore we need research collaboration and integration, and effective strategic innovative management between universities and industries easily to make decisions and to be competitive in the different type of crisis.

There are difficulties and problems for their optimal decision as well:

- Political unusually rights and low personal trust with non-transparency accountancy.
- Impersonal management with imaginary nets of interests and others.

The cooperation and competitive innovative station of the defensive systems and technologies, products and services, and the power of the state and its potential for independence and sovereignty depend on the management and the volume of researches in the areas of the defence and security. They are improving in the new paradigmatic challenges as like:

- Modern complexes of technologies;
- Global economy and Slender resources;
- Environment and stable growth and crisis;
- Demographic changes;
- Professional education for life and coordination by construction of societies and Economy of knowledge;
- Spread of information and special networks;
- Cognitive revolution and variety of executions;
- Strategic analysis of the future and Creative decisions;

- Continuously innovations and renew of infrastructure.

I would like to stress your attention to some problems as followings:

a.) Revealing of potential and more difficulties of full potential from possibilities for taking of scientific researches in the country and the areas of the defence and security.

b.) Supporting of inside and outside reorganizations which to be serviced by scientific research information and knowledge. There is not a uniform effective information model and device for coordination of the restructured building and using of the research and innovative opportunities.

c.) Existing of the tendency for creating of powerful administrative structures and bureaucracy of the scientific researches which is bigger more than free and fast accelerating of cooperation;

d.) Uncovering of the new scientific fields is predetermined. Instead of discoverers and innovators it depends on absolutely from politic decisions on macroeconomic level and macro institutional activities. It doesn't lead to presentation of need reputation of subjects on individual and organizational level in integrated Europe and international surroundings in SME-area, which create and use scientific and innovative products and services. There is a need for delimitation in the polices by financing of the projects for joint scientific researches and contract scientific researches, which in correlation to be connected with basic competitive indexes and assessments, and priorities for long term period.

e.) Widening and diversification of the forms of the financing scientific researches by seeking of additional sources and devices in the universities, excepting contract scientific researches in the state and private sectors and state financing of the regional and local level. There is different kind of difficulties to real policy to SME on the base the assessment of capabilities to creation and adoption innovations and increasing of them competitive capability in the Europe and world.

f.) The migration of the high qualified experts or the so-called "Brain gain". It isn't pay from making of networks and scientific co-

operation and mobility of the scientists. It is of account of limited resources and information, and technical capabilities for communications and special features of the scientific recognition, and competitive matter of the subjects, which are super sensitive by sharpened social and economical competition.

g.) The Continuing of the processes of destruction and free moving of demotion than seeking of new opportunities for change and challenges, and advantages to enhancement the quality of standards and researches, and innovation to their betterment. The scientific positions are not flexible and don't allow mobility from and to industries.

In the view of the fact there is a shortage of resources and the investments in good managers and better strategists and the best innovators and inventors that determine and make factors in structures of the Sustainable Development in middle and long term period aspect. A problem is we to uncover them still in the present. There is a need for a new cooperative different by kind of systematic and complex interdisciplinary researches or training of experts as in NATO and European management because there are increasing the international novelties and requirements to subjects, works and products and services in a competitive cooperation.

There are different scientific researchers and creative communities that observe the reorganization and rebuilding of the new scientific and research system in the country in the transition period. But there is missing the indication of seeking on the markets of the users and competitive scientific research products and services in the national economy. The private businesses invest little in scientific researches and making of novelties, and it prefers to buy and use prepared such from markets products and technologies. The private businesses don't put in risk resources for scientific researches.

Researches and development of cooperation and integration without innovations and participation on the markets are only abstract.

There is a need to clear contemporary and future orientated technologies, values and priorities in short-term period and middle term period. And there is a need to transparency of investments for

growth of the science and scientific disciplines that are related with them researches and projects in the areas of the defence and security to attract the scientists on the national and international level. It is so because the origin of the innovations and investments in them has not only political and economical meaning, and scientific and educational, which predetermine the meaning of the interdisciplinary transformations and international changes in the technologies and on the markets.

Without innovations the researches are fated to disclose one and the same and the management to repeat mistakes from 50-60 years of XX-th century market's forms of the West European Democracies.

The innovation criteria actualize and supplement, and increase the economical measures and social expertise and analysis by questions concerning as followings:

- Assessment of the projects on the national, regional, European and world level.
- Jointly financing of new appearance scientific research areas.
- Populating of Bulgarian and European inventions and innovations in the region, Europe and world.
- Bringing out deadlock and crisis national, NATO and European, and international scientists and researchers.
- Acquire and sustain of the capability for exact assessment of the economical costs and competitive capability and cooperation.
- Reality of assessment of policies and concepts, and models.
- Harmonization of strategic frameworks or strategies and priorities of the policies, for example concerning education and researches.
- Widening of the stability of the capabilities and potential for scientific searches between business and education on new surroundings and markets by cooperation.

It is so because the innovations bring always information and new knowledge and, of course, positive relations. The economic innovations are high profitable, but they have life if they are supported and serviced with all conditions of the markets, societies and security. It depends on the philosophical matter for researches, planning and im-

plementation and assessments.

The economical researches on the objects/subjects and events, and facts from the past and present without a strategic analysis of projections of the futures bring high risk for everyone management and economic security. Further, economical researches without innovations are not competitive concerning the national and international and world markets and economy.

The competitive races for attracting Brains, the so-called “Brain gain”, and new ideas and innovations can be winning as attract innovators and creators, and managers in science, art and business or they are making to be buying. There could be constant national processes of increasing the mobility and emigration on the Balkans in the following 8-10 years. The crises of the Kosovo case will go on to be a complex indicator for strategic analyses and European policy and operations not only to region, but to the world.

Opportunities

Nevertheless the national law and administrative changes are orientated to building of as well:

- Bigger internalizing system with mobility and presentation of high achievements than that from 01.01.2007 at least till 2013.
- Bigger dynamic system for opening of new laboratories of new branches than that from 01.01.2007 at least till 2013.
- And with bigger putting into practice system as it puts the European requirements than that from 01.01.2007 at least till 2013.

The crisis management marks on a new stage in the development of national and NATO and European Union economies. It is connected with the gaps in the scientific recognition and development of the new materials and high technologies and quality in the standard of life, growth of communications and increasing of the mobility on the global level.

Bulgaria has positive results concerning the global financing crisis in the last and present year on the Balkans, but we need new researches of the regional and national risk management and crisis management for the European security and operations. The Bulgarian

economy is a good example for European cooperation and integration in the South-East European region as real indicator and factor. And there are many challenges to wealth innovative and knowledge economy that without researches and innovations it is not possible to become really. There could be very useful to be realized researches between universities and businesses concerning of the reliability and its assessment of the financial and economic systems.

The following of good practices and better decisions in the perspectives and world traditions leads to new ideas and wider choice and effectiveness of the management and competitive cooperation. In the context of the strengthening tendency to internationalization of the science, scientific cognitions and education I consider that the University of national and world economy (UNWE-Sofia) is in potential for regular opening of an international master class or international entrepreneurial class. There already are conditions (international classroom and project course in the UNWE) by end results of the projects and attempt from the participation and execution of NATO and EU-projects. It could use for making of international master class for education, consulting and training of experts and teams, and implementation of economical researches in the areas of the defence and security. It could be make easier taking of decisions for national and European institutions with scientific information and analysis by crisis situations and training of civilian and military means for participation in operations. It is so because the complex innovative and creative economical analysis helps easier to taken of real decisions by join work of different specialists and experts, as the knowledge requires real information capabilities by parties in the area of the defence and security.

The UNWE is a suitable place for a regular international master class or international entrepreneurial class because it is middle by structure between the high levels of the state, administrative institutions and corporations, and businesses, students and specialists. It gives flexible ways for exchange information and knowledge to many directions. It could be very useful for the national and European economic security.

The regular international master class could popularize the innovations in technologies and markets, and cooperation on the Balkans in the European and world societies and to expert and esteem the competitive innovative products and services from the national and international scientific educational and industrial areas and cooperation between them.

Further, there could be useful establishing and giving a year award for innovation or invention, or realizing of the innovation project in the area of defence and security with cooperation between education, research centres and institutions and businesses on the national and international level. It could be also single-handed or in cooperation. For example, it could be given in the honour to David Greenwood (Germany) for his works and contributions to the UNWE and to modern planning, cooperation and European economy in the area of the defence and security.

There are problems and opportunities could help us to understand and to seek better management by scientific and practical co-researches within an innovative core of multidimensional information and knowledge. The innovations, risk of assessment and crisis management may help for it.

Literature

1. ICT - INFORMATION AND COMMUNICATION TECHNOLOGIES. EC, Work Programme 2009-10, EC, Brussels, 2008.
2. The place of Bulgaria in international rankings. IME (<http://ime.bg/en/articles/the-place-of-bulgaria-in-international-rankings/>), Sofia, 03.02.2009.
3. Atanasov, N. Key-meaning of the Innovations for funding researches and development: the Edge of the European competitiveness - In: Public-Private Partnership in Defence and Security sector – national practices. Annual International Conference on Economics and Management of Security and Defence. UNWE, Sofia, 2007.
4. Atanasov, N. Philosophical aspects of the information and their influence for development of the technologies. HEMUS-2008, MoD, Sofia, 2009.

USER INTERFACE FEATURES OF THE MOBILE WEB ACCESS

Assoc. Prof. Alexandar Kolev, PhD

“G.S.Rakovski” National Defence Academy, Sofia

Annotation: Topics discussed in the paper are related to the mobile WEB database access. Most popular mobile WEB browsers are described in the paper, which is tested by W3C(World Wide Web Consortium) provided compliant on-line test. Practical results of mobile WEB database access according NATO project SfP- 982063 are presented.

Key words: mobile, WEB, database, access.

1. Introduction

A mobile browser, also called a microbrowser, minibrowser or wireless Internet browser (WIB), is a web browser designed for use on a mobile device such as a mobile phone or Personal digital Assistant (PDA). Mobile browsers are optimized so as to display WEB content most effectively for small screens on portable devices. Mobile browser software usually is small and efficient to accommodate the low memory capacity and low-bandwidth of wireless handheld devices.

2. Overview of most popular mobile WEB browsers

- **Internet Explorer Mobile** - is developed by Microsoft , and comes loaded by default with Windows Mobile and Windows CE, first version was released in 1996.
- **Iris Browser** - a web browser for Windows mobile smartphones and PDAs developed by the Torch Mobile company. The first version of Iris Browser was released in 2008.
- **Opera Mobile** – is developed by the Opera software company. Opera Mobile was ported to the Windows mobile operating system in 2003.

- **SkyFire** – is open beta product by Skyfire Labs., founded in 2006.

3. Generic test

Acid2 tests a variety of web standards published by the World Wide Web Consortium and the Internet Engineering Task Force[3]. With the exception of CSS 2.1, all web standards tested were codified before the year 2000. CSS 2.1 was a candidate recommendation at the time of Acid2's release, and is still a candidate recommendation as of March 2009.

On Figure 1 is shown the reference image for Acid2.



Fig.1. The reference image for Acid2 test

Specifically, Acid2 tests:

- **Alpha transparency in PNG-format images:** The eyes of the smiley face use *alpha transparency* which is part of the 1996 Portable Network Graphics specification. The alpha transparency provides an elegant way to have the eyebrows smoothly blend into the face. This was a significant issue because Internet Explorer 6, the most widely used web browser at the time Acid2 was released, did not support alpha transparency. This deficiency was rectified in Internet Explorer 7, bringing Internet Explorer in line with other web browsers in this regard;
- **The object element:** The eyes also test support of the HTML object element. The object element has been a part of HTML since HTML 4 was released in 1998, yet by 2005 it still was not completely supported in all web browsers. The creators of Acid2 considered object element support important because it allows for content fallback—if an object fails to load, then the browser can

display alternative (generally simpler, more reliable) content in its place;

- **data URIs:** The actual images that form the eyes are encoded as data URIs. Data URIs allow embedding multimedia directly into web pages rather than being stored as a separate file. Acid2 tests the most common case, where a binary image is base64-encoded into text and then that encoded text is included in a data URI in the web page. Interestingly, although the IETF published the data URI specification in 1998, they never formally adopted it as a standard. Nonetheless, the HTML 4.01 specification references the data URI scheme and data URI support has now been implemented in most browsers;
- **Absolute, relative, and fixed CSS positioning:** Absolute positioning means that the web developer specifies the exact X and Y coordinates where an element is to be placed into the page. Relative positioning means that the web developer specifies an X and Y offset from the usual position of the element. Fixed positioning means that the element is placed relative to the browser window, and scrolls with the window rather than with the rest of the page;
- **The CSS box model:** This feature allows specifying dimensions, padding, borders, and margins, and was the focus of the original Acid1 test. Acid2 not only retests margin support but also tests minimum and maximum heights and widths, features new to CSS 2.0.
- **CSS table formatting:** This part of CSS allows applying table formatting without traditional HTML table markup;
- **CSS generated content:** Using CSS generated content, web developers can add decorations and annotations to specified elements without having to add the content to each one individually;
- **CSS parsing:** A number of illegal CSS statements are present in Acid2 to test error handling. Standards-compliant browsers are expected to handle these errors as the CSS specification directs. This helps ensure cross-browser compatibility by making all browsers treat CSS with the same level of strictness, so that what




works in one browser should not cause errors in another;

- **Paint order:** Acid2 requires that the browser have standard paint order. That is, overlapping elements should be placed or *painted* on top of each other in the correct order;
- **Hovering effects:** When the user moves their mouse over the smiley face's nose, it turns blue. This is called a hovering effect, and while it has traditionally been used for hyperlinks, it should work on a wide variety of HTML elements.

Because Acid2 is not a comprehensive test, it does not guarantee total conformance to any particular standard. A variant of the Acid2 test that does not test for data URI support is also available from the Web Standards Project.

On Table 1 are shown the results for Acid2 on mobile WEB browsers listed above.

Table 1

Tested WEB browser	Graphical results	Comments
Internet Explorer Mobile 6.1		Fully distorted picture, many HTML markup and CSS problems.
Iris Browser		Some absolute, relative, and fixed CSS positioning and Alpha transparency problems.
Opera Mobile 8.5		Some CSS table formatting and paint order problems.
SkyFire	Acid2 test not passed	Probably web page switching or multitab problem.

4. Mobile WEB access and Database for The State of Scientific Research

The NATO project SfP-982063 “Management of Security Related R&D in Support of Defense Industrial Transformation” has a WEB based Database for the State of Scientific Research[1]. It consists of few WEB pages, driven by PHP server-side interpreter and JavaScript menu-oriented user interface. Database WEB pages are tested on software device emulator [2] and on a real hardware under Windows Mobile 6.1 Professional Operating System.

Results based on software emulator included Internet Explorer Mobile 6.1, Iris Browser and Opera Mobile 8.5 are on Figure 2 below:



Fig. 2. Software emulator results

These examples come into view that different mobile WEB browsers on the same operating system have not a same functionality and layout view about. That is due at various JavaScript interpreters and Layout engines not fully W3C specifications compatible are implemented.

5. Conclusion

Results, based on Microsoft Device Emulator and real PDA device, both equipped with Windows Mobile 6 operating system shown, that Internet Explorer Mobile 6.1 has significant HTML markup and CSS styling problems, needs special tasks for Database WEB Mobile access. Iris Browser looks nicely and has only CSS styling problems. Iris Browser is semi suitable for Database WEB Mobile access in this Database WEB project. Opera Mobile 8.5 is fully functional and may be successfully used.

6. References

1. Database for the State of Scientific Research Project, <http://webdev.e-dnrs.org>;
2. Microsoft Device Emulator, <http://microsoft-device-emulator.en.softronic.com/pocketpc>;
3. World Wide Web Consortium compliant test, <http://acid2.acidtests.org>.

SOME METHODS FOR RISK ASSESSMENT OF CRITICAL INFRASTRUCTURE ELEMENTS

Assoc. Prof. Plamena Zlateva, PhD

Institute of Control and System Research – BAS

1. Introduction

In the recent decades, a trend of increasing impact of natural disasters and technogenic accidents on the environment and quality of life has been observed. In a rapidly expanding urbanization, high rates of construction, development and renewal of infrastructure in Bulgaria increasingly become important issues related to information security as a necessary element of sustainable development. Throughout the country various natural hazards have been manifested. These hazards and related technological hazards and accidents can lead to a number of critical situations - suspension or partial disruption of the functions of infrastructure [1].

Preserving the functionality of various systems and critical infrastructure is crucial in the event of a disaster and immediate action to curb the consequences. Analysis and risk assessment of natural disasters on critical infrastructure (CI) in a municipality can help to avoid or mitigate the effects of the negative impact of different types of threats.

At the end of the twentieth century, critical infrastructure protection is an essential element of security policy in many countries, especially in NATO members' countries and the EU countries. This is related on the one hand, with globalization processes and the fight against climate change, on the other hand, with an increased risk of natural disasters, technological accidents and technogenic catastrophes. The other main reason is the development and control of major infrastructure projects to transport oil, gas and other strategic raw materials. Protection of critical infrastructure is a relatively new research in the world, and it is on a good National level in the U.S.,

Canada, Australia and certain European countries.

Adopted by the Bulgarian legislation, the definition of "critical infrastructure" is similar to those imposed by the EC. Critical infrastructure is a specific and complex system that includes elements with different physical characteristics, behaviour, functions, etc. It includes: facilities, services and information systems, which stop functioning irregular or destruction would have serious negative effects on health and safety of population, environment, national economy or the effective functioning of government. Critical infrastructure elements are characterized by great uncertainty in their behaviour to external and internal interference because of their strong non-linearity and interdependence.

The aim of this paper is to define the problem for risk assessment of critical infrastructure elements and to propose several methods for risk assessment.

2. Risk assessment problem

There is a great number of risk definitions. The risk is commonly expressed numerically as the product of the probability of occurrence and expected consequences associated with an adverse event.

The risk is the expected cost from or expected loss due to a threat on a given infrastructure, is determined by the product of consequences of the threat, likelihood of the threat and vulnerabilities to the threat.

The risk assessment is formed as related to the expected damage in case of occurrence of a hazardous event (phenomenon, process), due to its intensity, time and place of occurrence and depending on the degree of vulnerability of this location. The risk is linked to the regress of the system as ordinary damage, destruction, impaired functioning, capacity reduction and others, associated with various natural phenomena and the occurrence of hazards related to critical or disaster situations [2].

Critical infrastructure is a complex system of interconnected and interoperable components. Expected consequences for critical infrastructure (damage, destruction and losses) are directly and/or indirectly related to the quality of life of people. In this context, the risk

assessment suggests a preliminary quantitative and/or qualitative assessment of the effects of adverse events (hazards). The risk for a given infrastructure element is linked to the possibility of distortion or loss of functionality due to damage or even destruction occurred as a result of natural hazards and/or critical events.

In this paper the risk is described by following function:

$$\textbf{Risk} = F(\textbf{Threat}, \textbf{Vulnerability}, \textbf{Consequences}),$$

where:

the threat is associated with the probability or likelihood that a hazard/danger/ attack scenario with the potential to disrupt the critical infrastructure element and cause undesirable consequences will occur. Threats are characterized by their means and likelihood of occurrence;

the vulnerability is related to the ability of the critical infrastructure element to resist the effects of any threat;

the consequences are the negative outcomes associated with degradation or failure of the critical infrastructure element. Consequences of a threat can be measured by loss of life, economic impact, loss of public confidence or other metrics.

Generally the risk assessment is to estimate the likelihood (possibility) for the occurrence of certain consequences, through the realization of the threat with certain characteristics (strength, intensity, duration, etc.).

It is necessary to emphasize, that the risk assessment of the critical infrastructure element is done under subjective and uncertain conditions. This requires development and application of modern innovative methods of risk assessment [3].

3. Risk assessment methods

The methods that will be used in the present project will be applied and adapted for critical infrastructure assessment and analysis. They can be divided into following categories: inductive, deductive, probabilistic and intelligent.

3.1. Inductive methods for risk assessment

The inductive methods for risk assessment start with definition of

potential scenarios describing different risks for a given system. Further they identify the risks and the consequences of previously defined scenarios. The major limitation of these methods is related to the fact that the scenarios can be defined only at the beginning and definition of new once is not allowed during the analytical stage.

The following two basic classes of such methods are used in practice:

Methods for analysis of failure modes and their consequences

- The methods FMEA, FMECA and HAZOP give qualitative estimation of risk and reliability of the given system.

Failures modes and their effects analysis (FMEA). This method analyses every potential failure and assesses its individual impact on system's functioning;

Failures modes and effects of critical once analysis (FMECA). The scope of FMEA is extended with analysis of criticality of the individual failures;

Hazards and workability analysis (HAZOP). The method makes qualitative estimation of key parameters' deviation from their nominal values in order to determine the "weak" links in the system.

- Event tree analysis

The consequences are presented as sequence of events that appear in the case of given initial conditions. The events happen with given probability or can depend or not by one other.

The method's limitations are related to the fact that the event tree is acyclic graph by definition. In this way it is difficult to describe the behavior of a system that includes backward connections and cycles.

3.2. Deductive methods of risk assessment

The deductive methods of risk assessment begin with definition of possible consequences of given risks for a given system.

Fault tree analysis

A logical diagram is constructed in order to investigate cause-consequence relations between faulted normal functioning of the system as a whole and the logical order of failures in its different parts.

The method is appropriate for multi-object interaction representation. Its limitations are insufficient reflection of time dependences and difficult presentation of backward relations in the systems since

the fault tree is acyclic graph.

3.3. Probabilistic methods for risk assessment

The insurance mathematics methods and acuter techniques usually apply probability theory methods. The methods that estimate the insurers' (respectively the community's) losses will be mainly applied and adapted. The possibilities of CI risk's redistribution analogically to insurance risk's redistribution will be analyzed too.

- Risk's redistribution methods

In that method the risk is redistributed between insurers and re-insurers.

Models form ruin theory

In the analysis of ruin task different theoretical methods are applied. The basic one is the method of finding the distribution of moment of the first approaching of the critical area (the point of ruin).

- Actuary techniques

There are different acuter techniques that estimate the quantity of presented damages claim that will be obtained if a given unfavourable event happened. In actuary practice the individual and collective risk models are the most usually used for determining of the value of exigible insurance premium (the value of insurance bill).

Individual model. The individual model considers the separate individual (object) with respect to its risk value and the respective losses of the insurance company;

Collective model. The collective model considers the company's losses obtained by a flow of claims from the insured population.

3.4. Intelligent risk assessment methods

The intelligent methods are applied for uncertainty handling tasks. In different systems for risk assessment expert judgments, fuzzy logic, neural networks, genetic algorithms etc. are effectively applied.

- Expert judgments

The information about risk's estimation is obtained by questioning number of experts. The answer could be qualitative or quantitative assessment depending on the chosen scale. The method is subjective

tive and contains a huge amount of uncertainty. There are numerous factors that influence the quality of the obtained information: qualification and loyalty of experts, time, resources etc.

- Fuzzy logic

The methods for risk assessment based on fuzzy logic have wide and successive practical application. This is mainly due to their attractive characteristics: representation of experts' knowledge by "if-then"; universal approximating characteristics; ability to account for information's uncertainties. All these make them extremely appropriate as a method for processing of uncertain expert information in risk's estimation.

- Neural networks

The neural networks have different applications due to their ability to approximate almost every function using training data and to classify samples. They use training data set with known class's belonging and after the training they are able to assign to a new sample its corresponding class. Neural networks are widely applied for different purposes as: estimation, identification, prediction and optimization.

4. Conclusions

The problem for risk assessment is defined. Several methods for risk assessment of critical infrastructure elements are proposed.

References

1. Analysis and Assessment for Critical Infrastructures Protection (ACIP), <http://www.iabg.de/acip/index.html>
2. Report on the project "Methods for critical infrastructure evaluation on the level of municipality" (2007), S., National security and defence research centre – BAS.
3. Stoyanov, V., Zlateva, P., Kirov, G., Stoyanov, K., (2007). Fuzzy logic application for forecasting of the potential damages from natural disasters, Second scientific-practical conference on the problems of management at emergencies and the protection of people, November 9, Sofia, 214-224.

CLOUD COMPUTING SECURITY RISKS AND BEST PRACTICES

Assoc. Prof. Dimiter Velev, PhD

Department of Information Technologies and Communications,
University of National and World Economy

Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them [1, 8]. The term **cloud** is used as a metaphor for the Internet, based on how the Internet is depicted in computer network diagrams and is an abstraction for the complex infrastructure it conceals. Cloud computing services often provide common business applications online that are accessed from a web browser, while the software and data are stored on the servers.

The concept generally incorporates combinations of the following [1]:

- Software as a Service (SaaS) - Network-hosted application;
- Data as a Service (DaaS) - Customer queries against provider's database;
- Platform as a Service (PaaS) - Network-hosted software development platform;
- Infrastructure as a Service (IaaS) - Provider hosts customer VMs or provides network storage;
- Identity and Policy Management as a Service (IPMaaS) - Provider manages identity and/or access control policy for customer;
- Network as a Service (NaaS) - Provider offers virtualized networks.

The concept of cloud computing has certain key components:

- Abstraction of infrastructure - where infrastructure is separated from other resources.

- Resource democratization - resources become a pool which can be combined and mashed up in various ways.
- Services oriented - everything is a service, including software, platform, and infrastructure.
- Dynamics - use of resources in the cloud can be scaled up or down as necessary based on an organization's needs.
- Utility model of consumption and billing –users of cloud computing pay only for the services they use, as with a utility.

Currently the lead topic of every information technology conversation is cloud computing. The key point in the conversations is cloud computing security. Traditionally these conversations tend to focus on all the standard security pros, cons and requirements. While protecting data from corruption, loss, unauthorized access, etc. are all still required characteristics of any IT infrastructure, cloud computing changes the environment in a much more profound way.

Organizations are looking to cloud computing to improve operational efficiency and reduce costs. Security typically improves due to centralization of data, increased security-focused resources, etc., but definite concerns can arise about loss of control over certain sensitive data. Security is often as good as or better than under traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. Ownership, control and access to data controlled by cloud providers may be made more difficult and the management of sensitive data is placed in the hands of cloud providers and third parties. In an age when the consequences and potential costs of mistakes are rising fast for companies that handle confidential and private customer data, IT security professionals must develop better ways of evaluating the security and privacy practices of cloud services. Different from traditional outsourcing where it is still very much standalone computing, cloud decouples data from infrastructure and obscures low-level operational details, such as where data is and how it is replicated. While it is rarely used in traditional IT outsourcing, is almost a given in cloud computing services. These differences give rise to a unique set of security and privacy issues that not only impact risk management prac-

tices [3, 5, 6], but have also stimulated a new evaluation of legal issues in areas such as compliance, auditing, etc.

Among the key security concerns related to cloud computing are: confidentiality, privacy, trust, identity, compliance, portability, interoperability, reliability, visibility, manageability, etc.

Leading IT experts and consultants, such as Gartner and Forrester, have already outlined the main security aspects of cloud computing:

Gartner has defined seven such key points [5]:

1. Privileged user access sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs. Get as much information as you can about the people who manage your data. "Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access," Gartner says.

2. Regulatory compliance. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions," according to Gartner.

3. Data location. When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers, Gartner advises.

4. Data segregation. Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. "Find out what is done to segregate data at rest," Gartner advises. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability," Gartner says.

5. Recovery. Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure," Gartner says. Ask your provider if it has "the ability to do a complete restoration, and how long it will take."

6. Investigative support. Investigating inappropriate or illegal activity may be impossible in cloud computing, Gartner warns. "Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible."

7. Long-term viability. Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application."

Forrester has synthesized three main areas companies should consider [2]:

1. Security and privacy - Concerns such as data protection, operational integrity, vulnerability management, business continuity, disaster recovery, and identity management top the list of security issues for cloud computing. Privacy is another key concern—data that the service collects about the user gives the provider valuable marketing information, but can also lead to misuse and violation of privacy. One way for customers to evaluate a provider's security and privacy practices are through auditing, which can help to lend some visibility into the vendor's internal operations. However, auditing goes against the very grain of cloud computing, which attempts to abstract away the operational details by providing easy-to-use interfaces and APIs. A cloud provider may not allow internal audits, but they should offer

provisions for some form of external audits on their infrastructure and network.

2. Compliance - Users who have compliance requirements need to understand whether, and how, utilizing the cloud services might impact your compliance goals. Data privacy and business continuity are two big items for compliance. A number of privacy laws and government regulations have specific stipulation on data handling and planning.

3. Legal and contractual issues - Liability and intellectual property are just a few of the legal issues that must be considered. Liability is not always clear when it comes to cloud services. The same is true about intellectual property — the cloud provider owns the infrastructure and the applications, while the user owns her data and computational results. In other cases, the division is not quite so clear. In software mashups, or software components-as-a-service, it can be difficult to delineate who owns what and what rights the customer has over the provider. It is therefore imperative that liability and intellectual property issues are settled before the service commences. Other contractual issues include end-of-service support—when the provider-customer relationship ends, customer data and applications should be packaged and delivered to the customer, and any remaining copies of customer data should be erased from the provider's infrastructure.

Proper implementation of security measures is highly recommended for cloud computing. The pure fact that the application is launched through internet makes it vulnerable to any time of attack. An application available in LAN only could even be infiltrated from the outside so placing an application over the internet is always a security risk. This is the unique situation of cloud computing. Implementation of cloud computing could require millions of dollars in infrastructure and applications development but it still places itself at risk for different types of attacks.

The most common security measures could be targeted at [3, 6]:

1. Protecting the Users - Developers of cloud computing services must make sure that data related to the user should not be mishandled and could be extracted just by one. There are two ways to ensure

cloud computing security: restrictive user access through and certifications. restrictive user access is to limit the access privilege of the user. Each user will have to be assigned manually with security clearance to ensure limitation of access to different files.

2. Data Security - Aside from user protection against different types of attacks, the data itself should be protected. In this aspect, the hardware and software linked to cloud computing should be scrutinized. Certification is highly desired in this part of cloud computing. Data privacy and business continuity are two big items for compliance. A number of privacy laws and government regulations have specific stipulation on data handling and planning.

3. Recovery and Investigation - Cloud computing security should not only focus itself on prevention. Certain resources should also be focused on recovery if the unfortunate event really strikes. Even before disaster happens, certain plans have to be in place to ensure that everyone will be working in unison towards recovery. The plans do not have to be focused on software attacks alone – certain external disasters such as weather conditions should have separate recovery plans

The idea above could be expanded to match the best practices for improving the cloud security [4, 6, 7]:

1. Encryption of all sensitive data / information: a) Network Communication – The network traffic must be encrypted for all communication channels that has sensitive information flowing across, you should encrypt the network traffic; b) Data Storage -all sensitive data that will be stored into the cloud, must be encrypted.

2. Securing all private keys - The basic idea is to increase the number of independent systems that attackers need to compromise before gaining access to your sensitive information.

3. Abnormality detection - Continuous monitoring is needed to detect security attacks or abnormal workload in the applications.

4. Keeping sensitive data within well defined data centres - any sensitive information and the associated operations must be kept within known data centres and carefully a set of sensitive operations to be exposed as a service must be selected.

5. Data Storage and persistence - the data is stored in a highly reliable environment such that the chance of data lost or corruption is practically zero even in event of disaster. To achieve high data resilience, cloud providers typically create additional copies of your data and put them into geographically distributed locations. An auto-sync mechanism is also involved to keep the copies up to date.

6. Cloud data backup - to guarantee the data is not lost even when the cloud provider goes out of business. The backup should be in a format restorable in a different environment and also should be transferred and stored in a different location.

7. Simultaneous operation on multiple clouds – A good approach is to prepare the applications to run on multiple clouds simultaneously. Such an approach will isolate the applications from vendor specific features.

8. Exercising trust in the cloud provider – There is a certain need to establish some level of trust to the cloud provider since as a rule the cloud provider have no incentive to steal information.

9. Legal norms compliance - Country laws, auditing practices, compliance requirement typically evolves pretty slow compare to technology. There is a need to identify these set of data as well as the corresponding application that manipulate them because they have to be complied with them at the data centre residing in that particular geography location.

The treatment of security, privacy, and compliance issues of cloud computing must be with the highest possible assurance level in order the end users to take full advantage of the power of the technology. Hence there is an obvious need for an industry with open standards, clearer regulations, and community-driven interoperability. A standards-based approach will make it easier for vendors to support flexibility, agility and expanded cloud service offerings such as collaboration, as well as it will also make it easier for customers to evaluate cloud vendors and build trust in its privacy and security promises.

Literature

1. Cloud Computing, http://en.wikipedia.org/wiki/Cloud_computing.
2. CHENXI WANG, A CLOSE LOOK AT CLOUD COMPUTING SECURITY ISSUES, WWW.FORRESTER.COM/SECURITYFORUM2009.
3. Chris Hoff, Disruptive Innovation and Security Implications of Cloud Computing, Multimedia User Briefing, February 2009, IANS Faculty, 7 p.
4. DAVID BINNINGS, TOP FIVE CLOUD COMPUTING SECURITY ISSUES, [HTTP://WWW.COMPUTERWEEKLY.COM/ARTICLES/2009/04/24/235782/TOP-FIVE-CLOUD-COMPUTING-SECURITY-ISSUES.HTM](http://WWW.COMPUTERWEEKLY.COM/ARTICLES/2009/04/24/235782/TOP-FIVE-CLOUD-COMPUTING-SECURITY-ISSUES.HTM)
5. JON BRODKIN, SEVEN CLOUD-COMPUTING SECURITY RISKS, [HTTP://WWW.INFOWORLD.COM/D/SECURITY-CENTRAL/GARTNER-SEVEN-CLOUD-COMPUTING-SECURITY-RISKS-853](http://WWW.INFOWORLD.COM/D/SECURITY-CENTRAL/GARTNER-SEVEN-CLOUD-COMPUTING-SECURITY-RISKS-853).
6. KEVIN JACKSON, CLOUD COMPUTING: THE DAWN OF MANEUVER WARFARE IN IT SECURITY, [HTTP://KEVINJACKSON.SYSCON.COM/](http://KEVINJACKSON.SYSCON.COM/)
7. Paul T. Jaeger, Cloud Computing and Information Policy: Computing in a Policy Cloud ?, *Journal of Information Technology and Politics*, 5(3), 35 p.
8. Steve Hanna, Cloud Computing: Finding the Silver Lining, 2009 Juniper Networks, Inc., 41 p.

СЪОТНАСЯНЕ НА НАУКА, ТЕОРИЯ И ЗНАНИЕ В КОНТЕКСТА НА СИГУРНОСТТА

проф. д.ик.н. Димитър Й. Димитров

Президент на Българската асоциация на конфликтолозите

Резюме

В изложението се прави опит за съотнасяне на наука, теория и знание и значението им за сигурността схващана в широк смисъл. Науката се интерпретира като отворена самоорганизираща се нелинейна система, която прониква в теоретичното мислене и праксеологичната дейност. Теорията се разглежда като система с по-малка (облекчена) информационна и методологична натовареност. Авторът смята, че възникването на конкретна нова теория от рода на синергетиката и конфликтологията е синтезиран израз на множество знание, притежание на различни научни области, чиято евристична сила е "складирана" в статично състояние.

Изясняването на съотнасянето на науката, теорията и знанието има принципно методологическо значение за разкриване на тяхното значение за сигурността разбираана в нейния широк смисъл. Настоящото тезисно изложение е посветено на този проблем.

1. Наука

Известно е, че наукоедите предлагат около 90 определения на науката, а всяко едно от тях считат за предпоследно. За нашето изследване е актуален процеса на самоидентифицирането на науката като отворена нелинейна система, която прониква в теоретичното мислене и праксеологичната дейност. По този начин тя се самодокazuje като решаващ фактор за социалния, икономическия, духовния процес и неговото управление.

Науката като самоорганизираща се система се формира от генериране на теории, знания и методи, социални институти, институции за публикации и накрая технология, която я превръща в непосредствена производителна сила. Всяка наука е концептуална система от понятия и теории, а нейната сложност се определя от

сложността на обекта, чието отражение е тя. Като самоорганизираща се система науката произвежда знания, теории и методи. Тя има своя логика и закономерности на саморазвитие, свързано с цялостната духовна и материална дейност на епохата. Тази връзка и взаимозависимост се осъществява на различни равнища в структурата на науката: емпирично, теоретично и методологично. С помощта на тяхното синтезиране се изграждат: теория на науката, логика на науката, философия на науката, теория на познанието, теория на наследствеността, теория на относителността, теория на организацията и самоорганизацията и т.н.

Самото понятие “наука” се саморазвива и самоорганизира. Доказателство за това са примерите, които се появиха в средата на XX в. Става дума за нови термини, чрез които се описва разгръщането на науката. Учените започнаха да я наричат “голяма наука”, “нов етап на науката”. Науката се структурира в нова система, непозната за миналите векове – научно-техническа революция (НТР). Появи се “наука за науката”, “самосъзнание на науката”, възникна нова теория за нея – наукознанието.

Визираните процеси, възникнали в науката, не само обогатяват теоретичната представа за нея, но улесняват описанието на общото и различното между нея и теорията. Науката се превърна в основен производител на духовен продукт – идеални обекти, производство на теоретични модели и др.

Функционирането на науката се осъществява с помощта на абстрактни понятия, теории, принципи и закони за познание на природата и обществото. Това показва, че теорията се поставя в структурата на понятията, законите, принципите и методите, чрез които науката произвежда знания за обективната реалност.

Ако до тук приключим с описанието на науката не бива да се остава с впечатление, че е казано всичко за нея. Защото както пише Дж. Бернал: “науката е толкова стара, през своята история е претърпяла полкова промени, всяко нейно положение е толкова свързано с другите аспекти на обществената дейност, че всеки опит да се даде определение на науката, а такива е имало немалко, може да отрази повече или по-малко само един от нейните аспекти, често

второстепенен, съществувал през някои от периодите на нейното развитие”⁴⁹. Ето защо вместо поставяне точка на тълкуването характера на науката, прибягваме до категоричния извод, че теорията като елемент на науката се ражда и функционира както в “ставащата”, така и “станалата” наука. Няма съмнения, че тя осигурява приемственост в науката и обогатява нейната самоорганизация. Взети в генетично единство, теорията и науката са най-важната част на духовното производство през всяка епоха.

Предпочитанието към това непрецизно науковедческо тълкуване на науката се обяснява с факта, че то съдържа, както бе подчертано, познавателно удобство при определяне характера на отделните научни дисциплини – наука или теория са те? Това оправдава изпускането на важни елементи на науковедческата структура на науката: кадри, материална база, организация и организационни структури. Цялостната система на науката се осъществява от институции, свързани с други сфери на функционирането на обществената система.

От непретенциозната инвентаризация на новите аспекти на науката, естествено не бива да се изпуска важния за нея проблем: методологиите и методите, парадигмалната проблематика, новият стил на научното мислене, който замени изследването на вещите с “отношенията в техните структури”. Синтезираното описание на съвременните белези на науката би добило по-задоволително значение за нашата тема, ако се напомним за интересното обобщение на Р. Акоф: “трябва да престанем да действаме така, като че ли природата е организирана по дисциплини подобно на университетите...”⁵⁰. Във връзка с тази констатация, той подчертава, че научните дисциплини са само методи, които свързват учените в комплексен колектив, за “производство” на научни знания и теории.

2. Теория

Теорията, от гледна точка на системно-структурната методология, е основен елемент на науката като цялостна система, органич-

⁴⁹ Бернал, Дж. Наука в истории общества. М., 1956, с. 17

⁵⁰ Акоф, Р., М. Сасиени. Основы исследования операции. М., 1971, с. 21-22

на част от нея. Затова релацията теория и наука се основава на принципа – част и цяло.

Теорията (от гръцки ез. – *theoria* – т.е. изследване) произвежда знание, което е обобщено и подредено на системна основа. Теоретичното знание се отнася към духовната и мисловна дейност. То е “копие” на реалната действителност, нейно “възпроизвеждане”. От своя страна тази действителност е неизчерпаема по сложност и системно-структурна организираност. Като обект и предмет на изследване действителността предопределя адекватна на себе си сложна структура на теорията. В нея се включват логически символи, правила, понятия, принципи, закони, съдържателна интерпретация на фактите, формулиране на хипотези и други технологични изисквания на познанието.

Теорията е система с по-малка (облекчена) информационна и методологична натовареност. Тя формира нови области в науката, с ярка проблемна насоченост. Това може да се илюстрира с много примери: социалният дарвинизъм се определя като теория, а не като наука. Признато е съществуването на теорията на игрите, теорията на информацията и решенията, теория на отражението и теория на познанието, теория на относителността, на наследствеността и теория на принадлежната стойност, квантовата теория и др. Като правило почти във всяка научна област има самостоятелни теоретични направления и дисциплини.

С основание се говори за теоретично осмисляне на нови емпирични (природни и социални) факти. Може да се каже, че в тези случаи теорията добива характер на процедура в научното познание. Знаем за динамичното противоречиво взаимопроникване между емпиричното и теоретичното, което чрез експеримент прераства в нова теория. Тъкмо тази нова теория изпреварва емпиричните факти.

Съществена черта на теорията е, че тя също изгражда собствен единен общ изследователски апарат за решаване на конкретни научни и праксеологични проблеми. Тя е нов източник на знания и методи, предлага нова технология за опредметяване на своите открития. Теорията винаги е обслужвала социалните функции на

науката, която произвежда познание за обективната реалност (природа и общество), а неговото използване се осъществява от теорията. От функционирането на теорията не се изключва производство на нови знания, но в нея доминират правилата, технологията за изменение на реалността, изследвана от науката. Теоретичното познание си самопроизвежда технология за превръщането на духовното в материално. Теорията, чрез знанието угасва в произведения материален продукт.

Накратко: от една страна, науката е интелектуална познавателна дейност, а от друга – сила, която чрез теорията неотразимо влияе върху материалната и духовна дейност. Тази същност на науката привлича вниманието на представителите на техническите науки и свързаните с тях технически теории и технологии. Учените говорят за отехничаване на науката и онаучаване на техниката. Самата техника е приложна теория, извлечена от науката, родствена, но различна от нея. Науката “тръгва” от хаоса в обекта и го възпроизвежда в идеален модел, в който става неговото превръщане в ред. Както в производството на този модел, така и в неговото превръщане теорията изпълнява доминираща функция. Констатацията не противопоставя науката на теорията, а ги диференцира и интегрира. Колкото е по-зряла науката, толкова по-актуална и ефективна става системата на малка информационна натовареност, т.е. проблемната теория. Това означава създаване на нова теория за производство на знания и технология за определяване на науката. Визираната нова теория е синтезиран резултат от знания, притежание на различни науки, чиято евристична сила е “складирана” в “неподвижно” състояние.

3. Знание

Разкриването на съдържанието на понятието знание има пряко значение както за определяне на теоретичния характер на синергетиката и конфликтологията, така и за техния предмет и функции. Генетичната зависимост между теорията и знанието се формира от процесите, които протичат в един и същ обект, предмет на тяхното изследване. Именно тази специфична особеност предопределя ре-

лацията и между теорията и знанието. Същата се основава на корелацията между емпиричното и теоретично познание на процеси, които протичат в един и същ обект.

Същият този обект е пространството, където става съединяването и раздалечаването между знанието и теорията. От същото пространство се извличат признаците на тези свързани, но различни понятия – теория и знание.

Типичен признак на знанието е неговата локалност, чрез която се съотнася към теорията. По тази причина знанието се формира както на емпирично, така и на теоретично равнище. Въпреки това, знанието е елемент на теорията, тъй като тя го е акумулирала и “отнесла” в собствената си абстракция, като нейна иманентна същност. Това показва, че знанието присъства както на емпирично, така и на теоретично равнище и се превръща в елемент на теорията.

Представата за фундаменталната теория се основава на различието между понятията знание и теория. Тезата се потвърждава с примери от физиката. Тази наука е изградена от система фундаментални теории, а не от знания. Но във физиката има много теории, които не са фундаментални. Наред с тях обаче съществува научна теория която е “не само обширна, универсална област на научното знание, но е основна единица на неговия анализ”⁵¹. От гледище на тази теза, теорията стои в основата на научното знание, а вътре в научната област се формират нови теории. Тук става дума за т.нар. “спомогателни науки”. Те формират допълнителни познавателни елементи в структурата на теорията и формират ново отношение между част и цяло (или между научното и теоретичното) познание. Анализирането на процесите в това ново отношение формира верижната структура: наука – теория – знание и разкрива техния характер.

От тази верижна структура може да се изведе тезата, че всяка теория е изградена от знание, но те не са тъждествени помежду си. Констатацията има отправно значение при определяне на научния или теоретичен характер на дадена самостоятелна дисциплина, на

⁵¹ Огурцов, А. П. Дисциплинарное знание и научные коммуникации. – В кн.: Системные исследования. Методологические проблемы. М., 1980, с. 318

нейния предмет.

Знанието предлага факти, емпирични и теоретични събития, свойства и качества на предметите. То установява емпирични закономерности. Редица автори тълкуват знанието като надстройка на теорията, защото то отразява “живата” реалност чрез наблюдения и експеримент. При анализа на отношението между знание и теория се преоткрива значението на тезата на Л. де Бройл, „че няма нищо по-измамно, отколкото ясната и нагледна идея”⁵². Той посочва категорично къде се намира източника на измамата в познанието и значимостта на очертаване разликата между знанието и теорията.

Знанието за “живата” реалност е необходимо за изграждане на т.нар. идеален обект, като средство за отдалечаване от нея. Идеалният обект или факт е важен елемент на теорията и разкрива нейната същност. Идеалният обект се превръща в предмет на изследване и формира нови теоретични направления. Като елемент на теорията идеалният обект се формира от обработване на емпиричните знания и тяхното превръщане в абстракция, която се изследва от теорията. Това показва, че е възможно развитие на една и създаване на друга нова теория, без да са налице факти за нея. В това се състои силата на теорията и изпреварването на емпирията. Описаната познавателна технология става основа за формиране елементите на теорията: понятия, категории и закони. Тяхната съвкупност формира нейната абстрактна система, отдалечена и освободена от сетивните факти. Теорията не само описва, но синтезира и обяснява натрупаното знание на емпирично равнище. Тя изгражда абстрактен понятиен апарат, формира закони, изработва принципи, изказва и издига хипотези и др. Веднъж проникнала в дълбините на структурните образувания на изследвания обект, теорията по обратен път поставя задачи на емпиричното и експериментално равнище на познанието. Тук движението на познанието се обръща от теорията към емпирията.

Теорията изобщо и възникването на конкретна нова теория от рода на синергетиката и конфликтологията е синтезиран израз на

⁵² Л. де Бройл. Революция в физике. М., 1963, с. 187

множество знание, притежание на различни научни области, чиято евристична сила е “складирана” в статично състояние. Това не бива да се тълкува като тривиална констатация, а трябва да се потърси подобно състояние в духовния свят: култура, общокултурен смисъл на много научни понятия от рода на модел, информация, комуникация, самоорганизация, отворена нелинейна система, бифуркация и др.

Новата теория не само открива нови насоки на развитието, но участва във формирането на нова стратегия на науката. Тази впечатляваща функция на теорията гарантира нейното самостоятелно съществуване като абстрактна форма на познанието. Синтезираните признаци на теорията имат отправно значение за определяне на теоретичния характер на синергетиката и конфликтологията. Екстраполирането на теорията като абстрактна форма на познание в синергетичната и конфликтологичната проблематика с лекота установява връзката между знанието за конфликта, за процесите на неговото протичане и хаотичните причини, които го пораждат в нелинейната самоорганизираща се система, бифуркацията и новият атрактор на развитието на социума.

MAJOR PROBLEMS IN THE DATABASE SECURITY

Dr. Violeta Bogdanova, PhD

Senior Researcher

Institute for Parallel Processing,
Bulgarian Academy of Sciences

The data stored within a database management system (DBMS) are frequently a target of attack from malicious users. The effect of such an attack can result in financial loss, a breach of national security or any other type of corruption that can result from unauthorized access to sensitive data.

Security is defined as: availability (access to information for authorized users), secrecy (no access to information to unauthorized users) and integrity (only authorized users should be able to modify data). Database security has become an essential issue in assuring the integrity, protection, and reliability of the data stored in a database management system (DBMS).

Introduction

Currently, as a result of the widespread use of various types of computer networks, the task of designing and introducing new and more sophisticated methods to protect information in databases are of particular importance. Choosing the right strategy to protect information in DB is crucial. Protection of information in the DB can be investigated mainly in two aspects: protection against unauthorized access and protection from indirect access.

1. Protection from unauthorized access

To provide protection from unauthorized access, it is necessary first to perform the classification of different levels of information according to its secrecy and accurately to specify the users who have ac-

cess to different levels. Thus avoiding unwanted transfer of information to unauthorized users. To allow control and inspection, all access to protected data and the operations over them have to enrol in a special file (**control journal**).

The management of access to information in DB is by the system **access control**. It provides the access of the users to DB for reading, recording, updating and deleting the information. The access for the different users is determined in accordance with the following conditions:

- a partial reading - the user can read only a certain part of the data that can not be changed;
- full reading - the user can read the entire DB, but can not change it;
- inserting records of a particular type - the user can insert records of a particular type, but can not change them;
- inserting records of all types – the operator can insert records of all types, but can not change them;
- deleting records from a particular type;
- removing records from all types;
- updating records of a particular type;
- updating records of all types;

The system **access control** includes subjects (users), who have access to the DB for reading, recording and processing the information. It consists of two main parts:

- file or table where the different users are fixed, so-called user profiles and access rules;
- file with control procedures to verify the applications of users and their access rights. After verification, access may be permitted, denied or modified.

The table with access rules is an expression of the selected strategy for the organization's protection. The appropriate method of protection must be chosen after taking into account the purpose of the DB. Typically, when DB is for universities or research centres that do not require strict protection may be chosen the method of maximum benefit (**maximum availability**), allowing the users to have access to maximum information in the DB. The organizations that need of strict protection, for example the organizations connected with the

national security and defence, must choose the method of least privilege (**need-to-know policy**), in which the users in the system are using a minimum amount of information necessary for their activity.

The choice of a strategy of protection of information in the DB includes determining the type of the system for access control. The system for access control can be closed or open type.

In the **closed systems** for every person there are rules giving the access privileges of a subject to the system objects.

In the **open systems** for each subject there are rules giving the forbidden privileges for the system. This will be the only rights that will be refused.

Open and closed systems are mutually exclusive. The selection of either system depends on the characteristics and requirements of the DB from organizational aspects, etc. closed systems require the use of the method of least privilege (**need-to-know policy**), while open systems - the method of maximum benefit (**maximum availability**). Protection is higher in the closed systems as in the open systems some errors, such as a missing rule can lead to unauthorized access. Advantage of the closed systems is that the procedure for processing of access rules is easier.

2. Protection from indirect access

Another major problem in the implementation of the protection of information in the DB is to protect from an indirect access. Indirect access means the ability to obtain confidential information by public information. Typical examples are the correlated data, where X is public information associated with the confidential information Y. Therefore, the information relating to the Y can be obtained by reading of X. Another classic example is the so-called **join inference**, where the access to confidential information is got by encircling roads. In this case it is necessary to analyze possible encircling ways.

There are various means to protect information in the DB. The following general requirements can be formulated to them:

- ensuring the semantic integrity of data. This requirement aims to maintain the logical connection of the modified data through control of the data values in the range;

- ensure the integrity of the data, which aims not to violate the logical structure of data.

The following key stages in the design of reliable protection of the information in DB can be defined:

- organizational phase, in which the functions of the DB administrator for ensuring the security are defined, the classification of the information in terms of confidentiality is made, the organizational activities to control access to information are determined. The determination of identifiers and passwords of the users is of great importance, because the information security is largely depending on their secrecy;
- choice of a system for access control, providing management of the access to information in the DB. At this stage, the type of the system and the type of the control (centralized, decentralized or hierarchic decentralized) is chosen.
- choice of a method of protection against indirect access to the information in the DB. At this stage, the different methods of protection have to be compared according to the following criteria: level of protection, quality (lack of information), accuracy, compatibility and costs of implementation.

Conclusion

In conclusion it may be emphasized that the complexity of the system of protection increases the cost of its implementation. It is necessary to find the optimal option in terms of system complexity and the costs required for its implementation.

References

1. Castano S., Fugini M., Martella G., Samarati P., Database Security, Addison Wesley, 1994);
2. Michael Gertz, Sushil Jajodia, Handbook of Database Security: Applications and Trends, Springer, 2007;
3. Csaba Egyhazy, Security of Database Systems: Authorization Features and Mechanisms.
4. Database Security Technical Implementation Guide, 2007

RESEARCHING OF THE INDIVIDUAL MANAGERIAL DECISIONS MAKING IN THE CONFLICT CRISES SITUATIONS IN SUPPORT OF SECURITY AND DEFENCE R&D MANAGEMENT

Mr. Ivan Tsanov, PhD

Bulgarian Association of the conflictologists

In the period 2007-2008 we conducted empirical conflictological study of the individual managerial decisions making in the conflict crises situations (IMDM in CCS) with 30 examined persons. The scientific results of the survey may be in support of Security and Defence R&D management. Briefly present the main results we received in the course of that empirical research:

1. Confirmed the assumption that the management practices used in the procedures and techniques for making IMDM in CCS are mechanically transferred from the management practice in non-conflict conditions.

2. It was found that there are pronounced differences in performance (accuracy, timeliness) for making IMDM in CCS between the different actors (people taking individual managerial decisions).

3. Was confirmed that the subjects of the management taking effective (accurate, timely) IMDM in CCS are distinguished by very specific professional and individual characteristics (specific professional psychological-conflictological-profile).

4. Not clearly confirm the assumption that by taking the IMDM in CCS the management subjects (individuals taking individual managerial decisions) operate primarily intuitive.

5. Was confirmed that the performance (accuracy, timeliness) of making IMDM in CCS is due mainly to psychological and physiological subject's characteristics of management (the person taking individual managerial decisions) – i.e. the crucial role of human been factor.

6. It was found that the specificity of IMDM in CCS require specialized crisis and individualized type of training.

Research and highlight some unresolved issues to be studied in depth and detail in the future:

- Need for additional specific management, physiological and neuro-physiological research problems using methods of equipment and tools;
- Further study the issue needs to intuition in making IMDM in CCS;
- The issue has particular importance for IMDM in CCS in the field of security. It was observed strong specificity that must be specifically studied.

Allow you to make some recommendations to researchers, professionals and institutions that relate to issues of IMDM in CCS:

- The problems of IMDM in CCS fruitful would affect the inclusion of a greater number of researchers from various sciences (particularly in the fields of economics, management, security and conflictology);
- You would be experts in economics, management and security to get more details with the issue of IMDM in CCS which will be helpful in daily work;
- To work more effective the public institutions need to take into account the specifics and peculiarities of IMDM in CCS. There is no doubt that they can only gain.

The problem of IMDM in CCS with high scientific and practical significance is and the boom in its study has yet to come. We hope our modest contribution to research of benefit to future researchers of the scientific problems of providing in support of Security and Defence R&D management.

RISK MANAGEMENT IN DEFENCE ACQUISITION – BEST PRACTICES

Mr. Yuri Tsenkov, PhD Student

Department “National and Regional Security”

University of National and World Economy

Introduction

Defence acquisition is the process by which the Offices for National Security and Defence provide equipment and services required for the performance of its tasks. The equipment includes devices intended solely for use as military weapons systems and ammunition, and products which are not specifically military service (from food to boots). Many services and tasks previously performed by the armed forces from supply of food and logistical support to collection and analysis of intelligence information are now supplied by private companies and are also subject to the process of acquisition. This article will be limited to that part of the acquisition, which includes the acquisition of weapon systems and ammunition through the defence projects.

Acquisition projects are unique and most of them very complex, spread over a large period of time and require involvement of a wide range of resources - people, finances, facilities, materials and intellectual property. The specific topics and objects of these projects and the related classified information further complicate the process of acquiring weapon systems. These are prerequisites for the emergence of a significant number with diverse nature risks thus you need good management to minimize the probability of failure of the final results.

Most difficult in such activities is to find the exact boundary between permissible uncertainty and recklessness. This is precisely the role of risk management. This activity is needed wherever the development of an organization or process is planned and the accompany-

ing risks are identified and assessed in order to assist in making informed decisions in an environment determined by risk and uncertainty.

The Bulgarian defence acquisition needs a documented risk management practice with clearly stated and thoroughly described methods and roles of every participant in the process in order to raise its efficiency and reach the necessary level of defence capabilities, required by the new dynamic and unstable security environment.

1. UK risk management in defence acquisition

In the UK the process of risk management is set out as a part of the standard associated with the requirements for safe management of military systems, which covers the whole process of acquisition.

The standard (UK Defence Standard 00-56 (Safety Management of Defence Systems))⁵³ was revised in June 2007 and the fourth edition is issued which sets high requirements for security in acquisition, including risk management without obliging to specific methods and procedures.

There are two key players in the process of risk management in the standard 00-56 – the contractor and the responsible authority (Ministry of Defence). The new fourth edition of the standard accurately and clearly lists the rights and obligations of both sides in the different stages of the risk management process. This is essential because both sides are actively participating in each activity during the process. Generally the process goes more on the basis of agreement between them and less on the basis of assigning tasks from the Ministry to the contractor.

The contractor is obliged to implement a process of risk management, which covers both the current contract terms and the life cycle of the weapon systems.

According to the standard the process of risk management involves four steps:

⁵³ Ministry of Defence, Defence Standard 00-56, Safety Management Requirements for Defence Systems, Issue 4, United Kingdom, 01 June 2007

1. Identification and analysis of hazards - identify and analyze hazards and accidents associated with the project, including related series of accidents.

2. Risk estimation – estimation of the likelihood of risk occurrence and the magnitude of the consequences due to its occurrence.

3. Risk assessment – is done according to pre-established criteria for tolerance based on legislation, standards, policies and negotiating with the ministry.

4. Risk reduction - if some of the risks are outside the criteria for tolerance and acceptance of risk, the contractor must implement a strategy for risk reduction, which may be based on engineering decisions or human factors, etc.

5. Risk acceptance – the contractor have to negotiate with the Ministry for the terms of risk acceptance. Individual risks and overall systemic risk can be accepted only if both the ministry and the contractor agree that they have presented sufficient evidence to reduce the risk within acceptable limits, according to the criteria for tolerance.

Besides working through these four stages the contractor has to establish a register for the hazards, which would be the main mechanism for monitoring the effectiveness of the risk management process. This register should be updated constantly during the time of the contract to ensure accurate registration of the different risk management activities.

2. Australia and New Zealand risk management in defence acquisition

In Australia and New Zealand risk management is regulated by standard AS / NZS 4360:1995 in 1995 his goal is to provide a common framework of the process of risk management, which consists of five consecutive stages: establishing the context, identification of risk analysis of risk, valuation risk, dealing with risk, and two co: communication, consultation and monitoring and review.

Process of risk management according to AS / NZS 4360:1995⁵⁴ includes five main stages:

- Establishment of context;
- Identification of risks;
- Risk analysis;
- Risk evaluation;
- Risk treatment;

And two supporting activities with feedback to the whole process:

- Monitoring and review;
- Communication and consultation.

Establishment of context

Establishment of context is associated with developing a structure for risk identification and assessment tasks to be fulfilled. This step:

- Establishes organizational and project environment in which the risk assessment will be performed;
- Defines the main objectives and desired outcome;
- Specifies a set of criteria for success, so the consequences of identified risk can be measured;
- Defines a set of key elements for structuring the risk identification and assessment process.

Identification of risks

Risk identification determines what can happen which will affect the project objectives and how it could happen.

The process of identification of risk should be comprehensive, because unidentified risks can not be evaluated and their appearance at a later stage may lead to negative results for the project. The process should be structured using the key elements in order to systematically examine the risk affecting every aspect of the project.

⁵⁴ Cooper D, Grey S, Walker P, Raymond G, Project Risk Management Guidelines, John Wiley and Sons, West Sussex, 2005

Risk analysis

Risk assessment is a general process of analysis and evaluation of risk. Its purpose is to develop priorities for the identified risks.

- Risk analysis is the systematic use of available information to determine the frequency of occurrence of some events and the magnitude of their consequences.
- Evaluation of risk is the process of referral of the estimated risk to given risk criteria to determine the significance of the risk.

The process of assessment:

- Determines the consequences of each risk if it occurs;
- Assess the probability of occurrence of these consequences;
- Converts the consequence and probability rates to an initial priority of the risk;
- Develops agreed priorities of risk and inherent levels of risk.

Agreed priorities are used to determine where to focus the greatest efforts in the treatment of identified risk. They facilitate the structural planning and allocation of resources.

Risk treatment

The purpose of risk treatment is to determine what will be done in response to the risks that have been identified, in order to reduce the overall risk exposure. Risk treatment converts the earlier analyses into substantive actions to reduce risks.

The primary inputs to this step are the lists of risks and their agreed priorities from the previous step and the current project plans and budgets.

Risk treatment includes:

- Identification of alternatives to reduce the likelihood or consequences of each risk (very large, large and medium);
- Identification of potential benefits and costs of alternatives;
- Selection of the best alternatives for the project;
- Development and implementation of detailed risk action plans.

Monitoring Review

The process of monitoring and review of risks ensures that new risks are detected and managed, and that action plans are implemented and improved effectively. This process links the risk management to the other management processes. The main results from this process are registration of new risks in the risk register and related risk treatment measures.

Communication and Consultation

Communication and consultation with the parties involved in the project may be a critical factor for the adoption of sound risk management and the achievement of broadly accepted project results. These processes help contractors, customers and end users to understand the risks and compromises that have to be made in a project. This ensures awareness of all parties and avoids unpleasant surprises. For the project team this helps to maintain consistency and accountability in the risk assessment process.

3. US risk management in defence acquisition

The Department of Defence (DoD) recognizes that risk management is critical to acquisition program success.⁵⁵ It is important to recognize that risk management is part of the job of everyone and not just the program manager or systems engineer. That includes the test manager, financial manager, contracting officer, logistician, and every other team member.

To assist DoD and contractor Program Managers (PMs), program offices and Integrated Product Teams (IPTs) in effectively managing program risks during the entire acquisition process a guide is adopted by the US government, developed with Defence Acquisition University.

This guide has been structured to provide a basic understanding of risk management concepts and processes. It offers clear descriptions and concise explanations of core steps to assist in managing

⁵⁵ Defence Acquisition Guidebook (DAG), Section 11.4, Department of Defence, United States of America

risks in acquisition programs. It focuses on risk mitigation planning and implementation rather on risk avoidance, transfer, or assumption. The guide is not laid out in chronological order of implementing a risk management program, but rather in a sequence to facilitate understanding of the topic.

Since it is a guide, the information presented within is not mandatory to follow, but project managers are encouraged to apply the fundamentals presented in it to all acquisition efforts, both large and small and to all elements of a program (system, subsystem, hardware, and software). It should be used in conjunction with related directives, instructions, policy memoranda, or regulations issued to implement mandatory requirements.

According to this guide risk is “a measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule and performance constraints. Risk can be associated with all aspects of a program (e.g., threat, technology maturity, supplier capability, design maturation, performance against plan,) as these aspects relate across the Work Breakdown Structure and Integrated Master Schedule. Risk addresses the potential variation in the planned approach and its expected outcome. While such variation could include positive as well as negative effects, this guide will only address negative future effects since programs have typically experienced difficulty in this area during the acquisition process”.⁵⁶

The difference in the American approach to risk is that they consider each risk to have three basic elements:

- A future root cause (yet to happen), which, if eliminated or corrected, would prevent a potential consequence from occurring,
- A probability (or likelihood) assessed at the present time of that future root cause occurring, and
- The consequence (or effect) of that future occurrence.

A future root cause is the most basic reason for the presence of a risk. Accordingly, risks should be tied to future root causes and their effects.

⁵⁶ RISK MANAGEMENT GUIDE FOR DOD ACQUISITION, Department of Defence, United States of America, August 2006

US model for risk management process

The risk management process model includes the following key activities, performed on a continuous basis:

- Risk Identification,
- Risk Analysis,
- Risk Mitigation Planning,
- Risk Mitigation Plan Implementation, and
- Risk Tracking.

For the successful execution of every key activity from this process various methods and approaches like modelling and simulation, risk matrix etc. are thoroughly described. In the risk management guide there is a separate chapter for planning and preparation of the organization for risk management. Just like in the UK standard the roles of every participating member of the project team, both from the DoD and the contractor is clearly stated.

In addition to this guide there is a standard MIL-STD-882D⁵⁷ dealing with mishap risks. This standard practice addresses an approach (a standard practice normally identified as system safety) useful in the management of environmental, safety, and health mishap risks encountered in the development, test, production, use, and disposal of DoD systems, subsystems, equipment, and facilities. The approach described in it conforms to the acquisition procedures in DoD Regulation 5000.2-R.

5. Bulgarian practice in risk management in defence acquisition

At present the Ministry of Defence of Bulgaria and the General Staff of the Bulgarian Army have adopted program and project type of management of resources and achievement of defence capabilities. On the other hand a project for armaments development is associated with significant resources such as money, time, labour, and most of the projects finish late according to the predefined deadlines and ex-

⁵⁷ STANDARD PRACTICE FOR SYSTEM SAFETY, US Department of Defence, MIL-STD-882D, 10.02.2000

ceed their allocated budgets. As reasons for this the occurrence of certain events, which have affected negatively the implementation of the project is always indicated.

One of the main principles of the armaments development system is an effective process management, which includes implementation of modern risk management systems.⁵⁸ Although this is set as a principle, such a system is not yet implemented. Further more it is not yet in a process of development. Despite the fact that risk management is a modern and very often used term in all the official documents of the ministry, there is insufficient knowledge in the field. In addition there is no document obliging the program and project managers and the contractors to use any established practices, models, methods or approaches to implement a risk management activity in the programs or projects. This is why a large part of decisions affecting the future are taken with uncertainty and incomplete information on factors that, in the medium and long term, may provide favourable opportunities for development or turn out to be great obstacles for achievement of the previously set objectives.

The 2015⁵⁹ plan predicts increasing of capital expenditures for defence at the expense of current costs. The establishment and the development of the armed forces will be implemented in terms of increasing demands and shortage of resources. Security environment is characterized as dynamic and rapidly changing, which in turn will have a direct impact on the implementation of the armaments development projects.

Such an environment is a bearer of many risks which requires an efficient risk management system to be implemented in the defence acquisition cycle in order to achieve the necessary capabilities of the Bulgarian army.

⁵⁸ Armaments Development System (concept), Ministry of Defence, Republic of Bulgaria, Armaments Policy Directorate, 23.10.2001

⁵⁹ Updated Plan for Organizational Establishment and Modernization of the Armed Forces until 2015, Ministry of Defence, Republic of Bulgaria

Conclusion

Risk management is a vital part from the whole management system, thus being a necessity for a best practice in management and a base for achieving good project results. This is an activity that many managers perform in a certain way but the question is whether they are familiar with the tools and their implementation in order to achieve something efficient or they rely on chance and best guesses.

It is essential for the success of the defence programs the risk to be well managed. Considering the very long term planning in the defence programs and some of the defence projects, an officially documented risk management practice, describing the whole process and the various roles of the different participants, as well as offering various methods and approaches for each risk management step is a necessity in order to be able to cope with the uncertainty of the future surrounding environment.

There are various good practices in risk management that could be used as a base for the development of a Bulgarian one.

References

1. Defence Standard 00-56, Safety Management Requirements for Defence Systems, Issue 4, Ministry of Defence, United Kingdom, 01 June 2007
2. Cooper D, Grey S, Walker P, Raymond G, Project Risk Management Guidelines, John Wiley and Sons, West Sussex, 2005
3. Defence Acquisition Guidebook (DAG), Section 11.4, Department of Defence, United States of America
4. RISK MANAGEMENT GUIDE FOR DOD ACQUISITION, Department of Defence, United States of America, August 2006
5. STANDARD PRACTICE FOR SYSTEM SAFETY, US Department of Defence, MIL-STD-882D, 10.02.2000
6. Armaments Development System (concept), Ministry of Defence, Republic of Bulgaria, Armaments Policy Directorate, 23.10.2001
7. Updated Plan for Organizational Establishment and Modernization of the Armed Forces until 2015, Ministry of Defence, Republic of Bulgaria

R&D AND CRITICAL INFRASTRUCTURE PROTECTION (CANADA'S EXPERIENCE)

Ms. Teodora Gechkova, PhD Student

Department "National and Regional Security"

University of National and World Economy

The term infrastructure itself has evolved over the years from including only a nation's defense capability and economic growth to including public safety, health and social welfare. Most recently, assets that could result in major damage or widespread injuries and fatalities, such as nuclear facilities, industrial sites, or bio - chemical materials, as well as those which could affect the morale of the population, such as national icons, are being defined as national critical infrastructure.

Critical Infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy. Most commonly associated with the term are facilities for:

- electricity generation, transmission and distribution;
- gas production, transport and distribution;
- oil and oil products production, transport and distribution;
- telecommunication;
- water supply (drinking water, waste water/sewage, stemming of surface water (e.g. dikes and sluices));
- agriculture, food production and distribution;
- heating (e.g. natural gas, fuel oil, district heating);
- public health (hospitals, ambulances);
- transportation systems (fuel supply, railway network, airports, harbours, inland shipping);
- financial services (banking, clearing);
- security services (police, military).

I. About Critical infrastructure in Canada

Canadian critical infrastructure "consists of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well - being of Canadians or the effective functioning of governments in Canada"⁶⁰

The Canadian critical infrastructure consists of ten sectors:

- Energy and utilities (e.g. electrical power, natural gas, oil production and transmission systems)
- Information and communications technology (e.g. telecommunications, broadcasting systems, software, hardware and networks including the Internet)
- Finance (e.g. banking, securities and investment)
- Health (e.g. hospitals, health care and blood supply facilities, laboratories and pharmaceuticals)
- Food (e.g. safety, distribution, agriculture and food industry)
- Water (e.g. drinking water and wastewater management)
- Transportation (e.g. air, rail, marine and surface)
- Safety (e.g. first responders, emergency services and dams)
- Government (e.g. services, facilities, information networks, assets and key national sites and monuments)
- Manufacturing (e.g. defense industrial base, chemical industry)

Not every element of each critical infrastructure sector is equal importance. For example, the Transportation sector is critical, but not every bridge or tunnel is, in itself, considered a critical infrastructure. Selection criteria are necessary to identify which critical infrastructure elements are of national importance.

Canada's critical infrastructures are highly connected and interdependent. A disruption to a service in one sector may impact upon multiple sectors. Compounding this interdependence is the increasing reliance on information technologies. Problems can cascade through these related infrastructures, causing unexpected and increasingly serious failures of essential services. Interconnectedness and interde-

⁶⁰ Public Safety Canada, www.publicsafety.gc.ca/prg/em/nciap.about-eng.aspx

pendence make Canadian infrastructure more vulnerable to disruption or destruction.

Canada's federal and provincial or territorial governments and Canada's industry are critical infrastructure partners. The main roles of these partners are:

- The all partners have to: develop, lead and manage the risk, strategies and programs; develop and lead training and education programs; develop multi – jurisdictional partnerships and share information and have to collaborate on exercises and R&D efforts.
- The federal and Provincial or Territorial Governments have to: provide leadership and guidance (analyzing, interdependencies, developing tools, assessing and reporting programs); establish critical infrastructure assurance or protection programs for government services within their jurisdiction; develop and implement regulations and standards; issue guidelines and direction within government regulated sectors and develop public alerting initiatives.
- Owners or operators (including federal, provincial and municipal governments in their role as owner or operator). Their roles are; strengthen partnerships among owners or operators and with governments; participate in sector or sub – sector wide risk management and critical infrastructure protection programs; share threat and vulnerability information on subjects where the owner or operator has unique information or access to information.
- Citizens – become aware of critical infrastructure issues; take basic steps toward action to secure infrastructures such as IT; take precautions for temporary disruption of critical products and services.

The Government of Canada has a unique role to play in raising awareness and leadership at the national level and international collaboration (U.S. Department of Homeland Security, NATO and G8). In addition, the Government of Canada protects its own critical infrastructure, support provincial and territorial programs and provide consistent, consolidated threat and vulnerability information nationally. The federal government's sector lead department and agencies.

These agencies and departments are responsible for one of the critical infrastructure sectors.

The next table show these responsibilities and engagements.

Canada's departments and agencies responsibilities⁶¹

Sector	Department/ Agency
Energy and Utilities	Natural Resources Canada(NRCan) Supported by: Canadian Nuclear Safety Commission (CNSC), International Joint Commission (IJC), National Energy Board (NEB)
Communications and Information Technology	Industry Canada (IC) Supported by: Public Safety and Emergency Preparedness (PSEPC)
Finance	Finance Canada
Health Care	Health Canada (HC)
Food	Agriculture and Agri – Food Canada (AAFC) Supported by: Canadian Food Inspection Agency (CFIA), Canada Border Services Agency (CBSA), Health Canada
Water	Environment Canada (EC) Supported by: Health Canada
Transportation	Transport Canada (TC) Supported by: Canada Border Services Agency
Safety	Public Safety and Emergency Preparedness (PSEPC) Supported by: Health Canada and National Defence
Government	Public Safety and Emergency Preparedness (PSEPC) and Treasury Board Secretariat (TBS)
Manufacturing	Industry Canada Supported by: National Defense, Natural Resources Canada and Environment Canada

⁶¹ Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection

II. R&D Organizations for critical infrastructure protection and the most interesting projects

Canadian Space Agency

The Canadian Space Agency was established in 1989. The agency operates like a government department. The president is an equivalent of a deputy minister and reports to the Minister of Industry.

The most important program of the Agency is “Critical infrastructure protection: Mine Site Monitoring From Space in Canada”.

Canada's critical infrastructure is vulnerable to disasters, whether natural (e.g., pandemic, floods, ice storms) or human-induced (e.g., terrorism, computer viruses). As the rate and severity of disasters increases, so does the possibility that disruption of critical infrastructure could result in widespread effects, cascading across borders and sectors, rapidly escalating from local to national levels and causing social and economic damages. The mining industry is among Canada's largest actual and potential employers in rural and northern regions, with mines like Diavik and Ekati in the Northwest Territories offering short and long-term employment opportunities. Protecting mining infrastructures and prevent and mitigate the impact of disasters (i.e. ground subsidence, triggering of slope failures, etc.) is important to assure economic stability. To this aim, the Canadian Space Agency (CSA) Earth Observation Application & Utilization division is supporting a private and scientific consortium led by MacDonald Dettwiler and Associates Ltd. (MDA) to improve Canadian ability to assist mining companies to execute safe, economic and sustainable underground mass mining by integrated RADARSAT-2 in SAR imagery to monitor surface and slope deformation. This new project supports the new National Strategy and Action Plan for Critical Infrastructure and the Science and Technology Strategy.

Centre for Security Science

The Centre for Security Science is joint endeavour between Defense Research and Development Canada (DRDC) and Public Safety Canada. It provides science and technology services and support to address national public safety and security objectives. It is part of the

Government of Canada' s approach to public security science and technology.

The main priorities of the Centre are Critical Infrastructure Protection. To build the necessary capabilities for the critical infrastructure protection mission area, there are two identified fields:

- physical critical infrastructure protection – applies to Canada' s physical infrastructure such as a power generation, transmission and distribution systems; water – supply systems and transportation systems. To protect Canada' s physical infrastructures, it is necessary to; clearly identify each infrastructure; assess the vulnerabilities of each infrastructure to all identifiable hazards, including attacks, accidents or natural disasters; identify the interdependencies between the infrastructures to understand how the failure of one infrastructure may affect others.
- Cyber critical infrastructure protection – applies to Canada' s networked information systems that manage communication and IT across the country. Modern – day Canadian society relies heavily on networked information systems and the protection of these systems is paramount to both Canadian security and economy. To build the capabilities required to understand and combat the growing problem of cyber crime. PSTP must focus on identifying knowledge and situational awareness gaps and understanding the frequency and severity of cyber crime incidents.

Public Safety Canada

Public Safety Canada was created in 2003 to ensure coordination across all federal departments and agencies responsible for national security and the safety of Canadians. This organization delivers programs and develops policy as well. For example:

- Emergency management – Public Safety Canada works with other levels of government and operators of critical infrastructures (such as utility companies) to help ensure essential services will be available to Canadian during an emergency.
- National security – Public Safety Canada runs the Government Operations Centre, which monitors potential threats to the national interest around the clock. The Centre can also provide co-

ordination and support in the event of national emergency.

Public Safety Canada and Natural Sciences and Engineering Research Council, have joined forces for an academic research program to investigate infrastructure interdependencies. The Joint Infrastructure Interdependencies Research Program is part of ongoing national efforts to secure and protect Canada's Critical Infrastructure.

What does it mean "Infrastructure Interdependency"? Major infrastructures such as hydro and water utilities, communications, banking and transportation networks and hospitals have many complex interaction points and depend critically on each other to function properly.

The project will produce new science – based knowledge and practices to better assess, manage and mitigate risks to Canadians from failures related to critical infrastructure interdependencies.

If there is a earthquake or tsunami or another disaster, everywhere will be a sound of breaking glass, metal scraping metal, walls falling, car alarms will down of screaming. Electrical, telecommunication and transportation systems will be interrupt. Hospitals and emergency services will be unable to cope as the city succumbs to the chaos of disaster. This is exactly the kind of emergency situation. The new Joint Infrastructure Interdependencies Research Program aims to avoid it. Most major infrastructure companies have well defined internal plans for how to deal with emergencies, but there is no enough development in coordinating these plans. In a situation such as an earthquake, tsunami or terrorist attack, the disaster response of all essential services and utilities must be coordinated in real time to minimize loss of life and damage communities. In this context the decision making processes need to be modelled considering the non – linear highly dynamic evolution of the crisis situation.

A better understanding of critical interdependencies among core infrastructures is one of the most important requirements to mitigate the impact of extreme events and improve survivability. This knowledge allows implementing effective dynamic islanding schemes. This dynamic segmentation of critical infrastructures helps to assign valuable and limited recovery resources to the most critical areas, while

avoiding the propagation of the emergency by cascading collapses of critical infrastructures to neighbour areas. Natural disasters such as earthquake, tsunamis, forest fires and global disease outbreaks can dramatically impact at first the socio – economic well – being of the countries, and the second they can impact our basic survivability. The extent of the damage resulting from a catastrophe must and can be minimized by the implementation of better preparedness organization and action plans among the National Critical Infrastructures Operators at Federal, Provincial and Regional levels.

The project takes a systems engineering approach to the problem of operators coordination among multiple infrastructures in order to minimize the impact of large disasters on human lives and bring the system of infrastructures back to operation as soon as possible. A solution framework in terms of multiple – delay difference equations is formulated to simulate the system of infrastructures in a step – by – step time domain solution suitable for real time event - driven simulation. The form of the solution allows for dynamic system optimizations in scenario playing and during disaster operations.

The basic participants in the project, are:

- University of British Columbia – the budget of this university is \$ 1, 020, 000. The role of the University is to study decision making for critical linkages in infrastructure interdependencies.
- York University - \$ 586, 500 for to model interdependencies for emergency management using geographic decision support systems.
- University of Saskatchewan - \$ 462, 048 to develop models that simulate critical infrastructure networks.
- University of Montreal – \$ 347, 250 to study interdependencies and domino effects in life – supporting networks.
- University of Toronto - \$ 310, 000 to develop a model of infrastructure interdependencies through an analysis of stakeholder needs, risks and competencies.
- University of Guelph - \$ 256, 000 to study ways to improve resilience of water infrastructure and health response systems against waterborne diseases.

Every participant in this project has a specific goals and roles. They are:

- University of British Columbia – focus on how to effectively make critical infrastructure decisions during emergencies. The key goal of the project is to use systems theory to help save human lives. The main objective and first priority of managing disasters is to maximize human survival rates. Since each infrastructure (power, water, etc) knows best how to recover its own system, the goal of the this project is focused solely on the coordination of the recovery.
- York University – focus on the modeling of interdependencies for emergency management using geographic decision support system. The project looks at the issue of emergency management from a geometrics perspective. The key objectives of the project are to: study location based infrastructure interdependences; study the interoperability of systems during emergencies; use scenario – based approach to analyze interdependencies; develop and design a prototype for supporting decision making.
- University of Montreal – this part of the project is about the study of interdependences, relationships and vulnerabilities in critical infrastructure life – supporting networks in the city of Montreal. There are three key objectives of the research; to develop a new methodology of risk management based on the interdependences between Lifeline Networks; to develop concrete risk management tools to prevent domino effects regardless of the events likely to generate failures; to increase the team's knowledge of problematic areas related to interdependent infrastructures
- University of Toronto – the focus of the project is on making critical infrastructures stronger by addressing interdependency issues at the design stage. The project is a way of understanding how to help engineers design a product by making them fully aware of the critical linkages to other systems. The work of this project focuses on the representation of knowledge at the engineering or design level
- University of Saskatchewan – the potential users of the tool that

will come out of this project will be key decision makers in government agencies. There are two key components to the project; the first is to develop a model that will capture all interdependent relations in a critical infrastructure; the second is to create a simulation of the critical infrastructure interdependencies.

- University of Guelph – the focus of the project is on studying ways to improve the resilience of the water system infrastructure and the health response systems to the waterborne diseases. The project deals with how systems fail, the communication between systems and how key players must respond in the event of failure. A goal of the project is to make sure that things happen the way they are supposed to with respect to emergency management and prevention.

The project has also received some \$ 650, 000 in additional financial support and \$ 1 million in - kind assistance from a diverse group of private and public sector partners, such as municipalities, industrial associations, infrastructure operators and corporations. They are:

- Bell Canada
- British Columbia Transmission Corporation
- Canada Research Chair Funds
- Canadian Red Cross
- Centre de Sécurité – City of Montreal
- City of Guelph
- City of Peterborough
- Consulting Engineers of Ontario (CEO)
- Devel-Tech Inc., Saskatoon
- Emergency Management Ontario
- EmerGeo Solutions Inc.
- Environment Canada
- Gaz Métropolitain
- Greater Toronto Sewer and Watermain Contractors Association
- Greater Vancouver Regional District (GVRD)
- Hinz Automation Inc.
- Hydro Québec

- Macquarie North America Ltd.
- Ministère de la Sécurité Publique du Québec
- Ministère des Transport du Québec
- Ontario Ministry of Agriculture and Food
- Province of British Columbia
- Public Safety and Emergency Preparedness Canada
- SENES Consultants Limited
- Tecsult
- Telus Corporation
- Toronto and Area Road Builders Associations
- Vancouver International Airport Authority

Dalhousie University – Critical Infrastructure Initiative

The goal of the initiative is to create opportunities for citizens, industry and governments to engage with questions and ideas concerning the management of Canada's critical assets, exploring technical as well as historic, social, political, legal and economic opportunities and constraints.

The University seeks to enrich the discussion about the complexity of the infrastructure and the holistic approaches necessary to make it more secure and resilient for the benefit of all Canadians.

In the end of the year Dalhousie University will organize symposium about the critical infrastructure protection problems.

Critical infrastructure protection – activities that enhance the physical and cyber – security of key public and private assets – is garnering increased attention among governments and industry stakeholders largely due to the complexity and interdependence of the sometimes fragile systems upon Canadians rely. Failure in one system can have a cascading effect; it can cause multiple, simultaneous failures, across industries and sectors. There is no single authority to take the binging risk management decision: instead the nature of risk often requires collaboration between different stakeholders. The challenge is not merely a technical one. There are many social, legal, business and environmental obstacles that impede successful management of critical assets. These challenges require imaginative solutions that take a broad approach to understanding and managing the risk.

Goals of the symposium: first to create cross – sectoral and cross – jurisdictional space in which participants can access and share diverse and expert perspectives on protecting the critical infrastructure, exploring technical as well as managerial issues; second goal is to employ the recent Renn Governance framework to provide a coherent structure to the workshop while at the same time examine and test the utility of this new framework; the third goal is to focus on understanding the nature and characteristics of different risks and threats to critical infrastructure and examine distinct and appropriate approaches to managing them; the last one goal is to consider future prospects for shared dialogue and collaboration on this subject.

The target audience of this project will include academics, as well as public and private sector representatives that have an interest in and responsibility for managing and securing critical infrastructure.

III. Conclusion

The Government of Canada defines “these national critical infrastructures as those physical and information technology facilities, networks and assets, which if disrupted or destroyed would have a serious impact on the health, safety, security or economic well – being of Canadians or effective functioning of governments in Canada.

One of the most serious and important problems in Canada is, that Canadian critical infrastructures are highly connected and highly interdependent. In the future, the big part of investments about researchers, have to be in this field.

The next problem in critical infrastructure protection is about the importance of critical infrastructure elements. Not every element of each critical infrastructure sector is of equal importance. Selection criteria are necessary to rank which critical infrastructure elements are of national importance.

After this analysis is obviously, that Canadian Government supports researchers for critical infrastructure protection. The Government understands that investing in science and technology is essential to protect and strengthening Canada’s economy.

References

1. Canadian Space Agency,
http://www.asc.csa.gc.ca/eng/newsletters/eo_express/2009/0213.asp
2. Defence Research and Development Canada, Centre for Security Science, <http://www.css.drds-rdds.gc.ca/index-eng.asp>
3. Public Safety Canada, <http://www.publicsafety.gc.ca/abt/index-eng.aspx>
4. Joint Infrastructure Interdependencies Research Program,
<http://www.ece.ubc.ca/~jiirp>
5. Public Safety Canada, <http://www.pablicsafety.gc.ca/prg/em/nciap/about-eng.aspx>
6. Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection
7. Dalhousie University,
http://www.spa.management.dal.ca/Research_and_Projects/2007/Critical_Infrastructure_Pr.....

INFORMATION SECURITY POLICIES IN R&D PROCESS

Mr. Nedko Tagarev, PhD Student
Department "National and Regional Security"
University of National and World Economy

For the beginning of such an article we have to get answers of two main questions:

What is "*information security*"(IS)?, and

What is "*Information security in R&D process*"?, are there any differences or are they the same.

To get answer to the first question we gen get in to the known understandings of the problem, or we can ask the professionals or just the ordinary people that are engaged with the problems of the security of information. There is no difference in methods of getting to the understanding of the asked question because in whatever direction we start to search we are going to get a thousand of different answers, which will not give us the theoretical paradigm of the "information security.

The only way to way to get to united understanding that can be used as main stone for the further analyses is to take that is common for the all definitions and to create our own, that will represent the answer of the early formulated questions.

"Information Security" represents a set of resources (technical and social) to protect information as an element of human socio-economic relations in order for it to remain unchanged and available all over, until the need to be used!

As we see from this definition of the „*information security*“ it gave us the answers of the two questions. The first one is clear as it's the definition of the IS, the explanation of the answer of the second one will be described in first two parts of this article.

After this explanation we will see by method of deduction, that this principles and this definition are general for all the problems related to the information security.

Part .I. Understanding of the information

The information is vital for every living organism, and can be used only from such ones. Nonliving organisms don't need and don't use information as such as we know it. As such the *information carriers of type I* - books, documents, computers, etc. have no interest in information they carry at all.

So we can classify the carriers of the information in two types:

- Type I – nonliving organisms;
- Type II – living organisms.

In the main interest of this article is the information that is carried by the living organisms. It can be classified also in two types:

- hereditary information;
- accumulated information.

Every living creature have hereditary information which make it to survive in the nature as we know it. Even the grass and the trees have such information, which bring it to the level of conditional reflex. This information, cannot be changed or interpreted in a different level than it is, so it's not in the interest of this article.

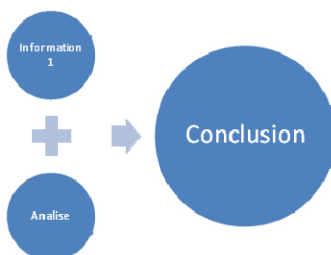
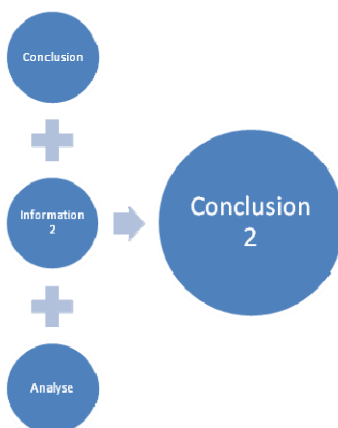
Accumulated information is also common for all biological species. For example the predators, get the information where are the water sources where their victims go to drink water. This kind of information helps them to survive the competitive world. For people is the same. The main difference is in the complex of the information, so the people need the tools to carry it or *type I information carriers*.

The process that complicated the information that we have in a moment of time and it's development in order to achieve some goal we call research and development process.

As the process of research and development is in connection with the information as it's mile stone we need the information security as such, and in accordance to this we need information security policies.

Part .II. Process of using the information

The basic theoretical scheme of R&D process can be presented in art mode in such way:

Step .1.**Step .2.****Etc.****Scheme .1. The simple look on the R&D process**

The explanation is simple. On the first step the man have the information. Analyze it with some methods and in the end get some conclusions. In the second step the man get the conclusions that already have, gain more information about the problem and perform further analyzes to achieve his goal. And so on.

So the question here is, where is the problem for *information security*?

The answer is simple if we get back to the definition where we

can see for the information that - ***in order for it to remain unchanged and available all over, until the need to be used.***

Every analyses change the information, every new gain information (information 2 in the scheme) change the information, so it's a problem for information security.

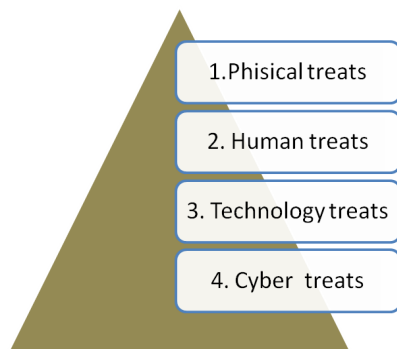
Based on logics we can define the treats to the information security during the process of analyses:

- Methods for analysis;
- True statement;
- Faithful findings;

The short diagnostic of the treats shows that the wrong analysis method, or intentional using of wrong method for analyze will bring false information. The false statement allays will bring to false information, but not all the true statements will bring us to true information if we don't use the right method. All the process if we don't use the right methods, or true statements will not bring us to faithful findings.

All this treats are related to human so in conclusion for this part of analyze and knowing already that the nonliving objects are not interested "directly" to harming the information we can put the human factor near the top of the pyramid of treats for information security. It must be noted that it's not even spoken about the intentional harm of the information.

On such scale we can create the pyramid of the treat factors (scheme 2):



Scheme 2. The pyramid of the treats.

Even we spoke till now for the human treat factor of =n the top of the pyramid stays the physical treats. The physical threats came from environment of the carriers of the information and are direly connected to the physical damages they can provide to the carrier.

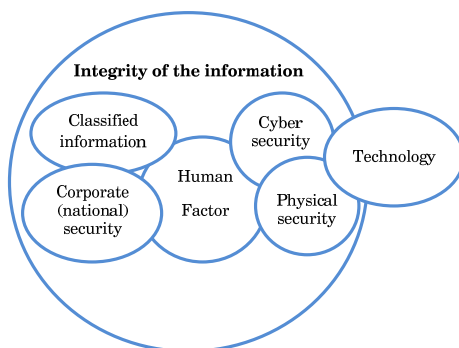
Technology treats are pretty same, but are related to the technology that man use to keep and provide the information.

This three treats for *information security* we will call the **classical treats** because they are studied true the ages and the policies are all known, and probated by the laws, norms and standards.

The fort main treat is cyber treat and it is related with the tree classical ones, but in some new fashion. For the new time – the “Information age” the cyber technology is vital for keeping and providing information. The main advantage of the information technology is speed, which provide more time in no need of exact space. And if we go back to the definition it’s obvious that it’s object of the “information security”, that we call cyber security of computer security.

Part .III. Information security and the integrity of information

In this point of the article we must take a look at the all picture that is presented in abstract scheme, if we already know that the main goal of the information security is the integrity of the information:



Scheme 3. Abstract look at the integrity of the information

On this scheme we can see all the elements of the information security, as it's objects, contents, or as it treats. In the middle stays the human factor because only the humans are capable to understand, examine and use the complicity of the information. From the right are the main treats as a relation with the human, because the human is main source of the treat and defence, and is the only one that is related to technology for treat and defence.

From the left side is the most popular type of information that is protected. As through human factor it needs a protection from the treats, that can be provided again, only by human, and the usage of the information is only for human and their competitiveness for survival against other humans. In other cases the only treat will come only from physical treats in their natural disaster character and the treats from human usage of the information in order to its analyses.

Part .IV. Know popular policies for information security and models

The most popular models can be determined as:

- American government policy model (*Priority of the large objects*)
- European Union policy model (*Priority of the small users.*),
- as they are related to the cyber security at most.

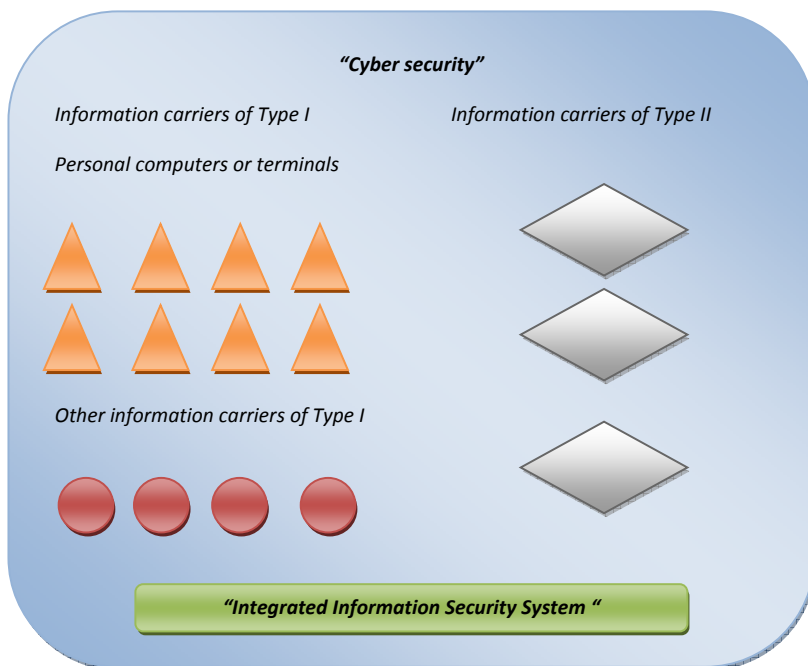
The main policies are related with the information security and the critical infrastructure, because the classic treats are eliminated in some stage, as if they can never be totally eliminated or such thing as absolute security does not exist. The only thing is to take some precautionary measures.

For the United States of America is obvious why the main security policy about information is cyber security. The level of the automation of processes is so big, and the level of the information society is so great that in every minute, and in every corner of being of the US economy are the computers.

On the other side is the private sector, and private-public relationship. Over 70% of the critical infrastructure in the US is in the private sector. According to that the government policy is concentrate on the cyber security of the large objects instead of their component,

which we will call the small once. So if we use the term system we will know that it means that it is the big object and its components.

This is shown on scheme 4:



Scheme.4. Large objects (system)

For such an "Integrated security systems" there are specific standards and requirements applied only for one big object. So there is no connection between two systems of such range. So the main problem is such type of cyber security, block the opportunities for cooperative work.

On the other side there is no protection on the lower level of security instead of the "head cyber security".

On the other side in context of the article this means that the smooth cooperative R&D process is impossible. On the other side it prevents the industrial espionage on the higher level, so the main

problems to solve for the information security are physical and technological treats.

The other type of known policy of cyber security is EU model, which is regulated, and for each country member of the union by laws or standards. The standards are directed to the small elements of the system, not for the huge systems as one.

This is a big tread as the standards are the same, and the treats methods are developing their resources faster than the defence ones. This means that the program management for such a problem as the information security is inadequate.

Conclusions

For conclusions we can list the main requirements treats for the information security in the R&D process:

- Information must be true;
- Methods of analyses must be exact;
- Conclusions based on previous information and analyses must be true, and if it's not we treat the information security system;
- Policies for information security must include security on the system as hole and security of the system as one;
- The systems with different standards and types of defence cannot provide cooperative R&D process.

Used literature

1. <http://www.sans.org/training/description.php?tid=877>
2. www.euractiv.com/en/security/critical-infrastructure/article-140597
3. European Programme for Critical Infrastructure Protection (EPCIP)
4. http://en.wikipedia.org/wiki/Critical_infrastructure
5. Critical Infrastructure Protection Program 1996r. CAIII
6. Patriot Act 2001r. CAIII
7. 97-71 <http://www.fas.org/sgp/crs/secrecy/>
8. RS20748 <http://www.fas.org/sgp/crs/secrecy/RS20748.pdf>
9. RL34120 <http://www.fas.org/sgp/crs/secrecy/RL34120.pdf>
10. the National Strategy to Secure Cyberspace, February 2003, USA
11. Cyber Security: A Crisis of Prioritization, February 2005, USA

12. department of defense Directive 8500/1, 24 October, 2002
13. establishing the European Network and Information Security Agency, COMMISSION OF THE EUROPEAN COMMUNITIES, 2005
14. <http://www.cesg.gov.uk/>
15. UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME, October 2008
16. INFOSEC ASSURED PRODUCTS
17. <http://www.bsi.bund.de/english/departement1.htm>
18. Annual Report 2005, Federal Office for Information Security (BSI) www.bsi.bund.de

AN APPROACH FOR CLASSIFIED INFORMATION LOCAL AREA NETWORK

Mrs. Darinka Nickolova, Mrs. Maya Bojilova

“G.S.Rakovski” National Defence Academy

Defence Advanced Research Institute (DARI)

Abstract

The purpose of this report is to present the results obtained during the process of realizing of a Local Area Network (LAN) with opportunity to manage sensitive and/or classified information using IPSec security tools. IPSec is described in the context of providing the ability to protect communication between local area network computers.

Key words: IPSec, IPSec Policy, Internet Security Protocol, IPSec Encryption and Integrity, Authentication Header (AH), Encapsulating Security Payload (ESP), OSI 7 Layer Reference Model

At present it is impossible to live and work without using information technology. One of the important problems is how to protect data integrity, confidentiality and accessibility transferring huge quality of information with networks. The security of information is a world problem of the present day not only for military but also for banking, economical research, firms' policy, marketing and many other area of human activity. 'Security is dynamic – people, process, and technology all change. all of these factors make managing security difficult'.

The importance of the problem can be summaries as follow:

- the information in networks (networks data) can be subject to an attack;
- networks are susceptible to unauthorized monitoring and attacks;
- necessity of information management with different level of sensibility and classification

Essence of IPSec

IPSec, or Internet Protocol Security, is an encryption protocol which provides encrypted data transmission at the Network Layer (fig. 1) of OSI 7 Layer Reference Model across a public network such as the Internet. There are authors who assume that IPSec is the most powerful security tools available today.

IPSec is a suite of protocols that allow the secure exchange of packets at the IP layer. It defines how to provide data integrity, authenticity and confidentiality across a public network like the Internet. It accomplishes these goals through tunneling, encryption and authentication.

In IPSec, all protocols which sit upon the Network layer (according to Open System Interconnection (OSI) Model) are encrypted between the two communicating parties. TCP, UDP, SNMP, HTTP, POP, etc, are all encrypted regardless of their built in (or lack of built in) security and encryption.

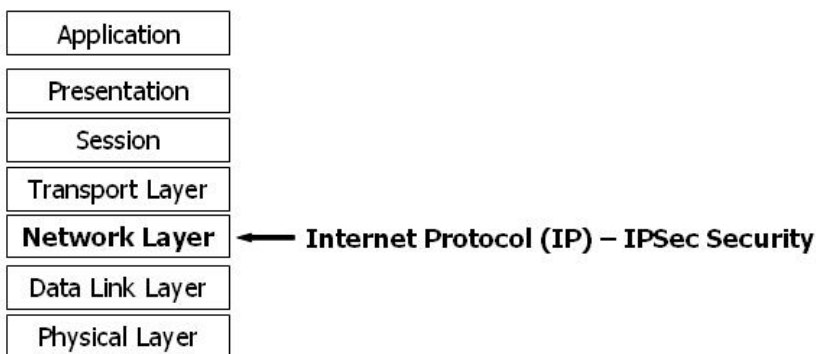


Fig. 1. OSI 7 Layer Reference Model

The form that a piece of data takes at any layer is called a Protocol Data Unit (PDU). Network Layer's PDU is called packet and is shown on Fig. 2. Implementing IPSec Policies encapsulates IP Packets to ensure their privacy and security.

IP Header	TCP	Data
-----------	-----	------

Fig.2. Form of the packet without IPSec

Encapsulating is a process of data wrapping in a particular protocol header. During encapsulation, each succeeding layer encapsulates the PDU that it receives from the layer above in accordance with the protocol being used.

In this paper we discuss defining and implementing IPSec with next network operation system:

- MS Windows Server 2003;
- MS Windows 2000;
- MS Windows XP.

Some features of the IPSec are available only in the Windows Server 2003 Family. If there are a servers or workstations running Windows 2000 or Windows XP it is important to test the policy thoroughly before deployment. To define the requirements for exactly IPSec Policy it is important to analyze the types of possible attacks that systems may be exposed. Network attacks might be a result of minimal or nonexistent intranet security.

IP Security Monitor is a tool to test and monitoring the effect of implementing IPSec Policies. IP Security Monitor was implemented as an executable program – IPsecmon.exe in Windows 2000, while in Windows XP and the Windows Server 2003 – like a Microsoft Management Console (MMC) with some enhancement as a feature.

The topology of the network that we have in mind is shown on (Fig. 3). The main goal is to ensure data integrity, confidentiality and accessibility of the traffic between different nodes.

IPSec is comprised of two protocols, which provide different services. It is possible the two protocols to be cooperated. The two protocols are:

- IPSec Authentication Header (AH) – provides packet integrity services
- IPSec Encapsulating Security Payload (ESP) - provides packet confidentiality services

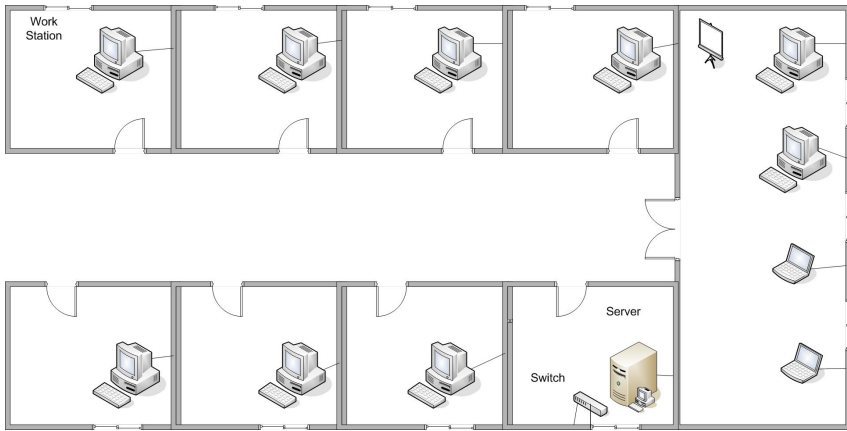


Fig.3. Enterprise Local Area Network

Both protocols provide authentication, integrity and anti-replay protection, but when packets are sent using ESP the payload (data) of the packet is encrypted and authenticated.

Encryption or security protocols

Security protocols and encryption are transmission protocols which are used to transmit high value data securely. Encryption, which is at the core of any security protocol, gives you three fundamental advantages over ‘clear-text’ or unencrypted data:

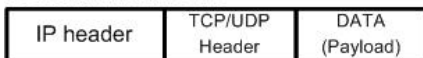
Data privacy - or the ability to hide the data which is being transmitted

Data authenticity and integrity – the mathematical algorithm of encryption give security protocols the ability to ensure data has not been modified or damaged during transferring.

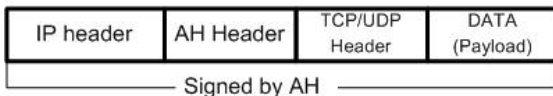
Non-repudiation - another feature of the math contained in encryption is the ability to prove an act occurred.

Comparison between form and size of the packet without IPSec, using AH and ESP IPSec are shown on Fig. 4.

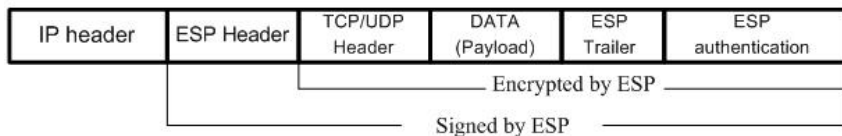
IP Packet without IPSec



IP Packet with AH modification (with IPSec)



IP Packet with ESP modification (with IPSec)

**Fig.4. IP Packet's form and size**

To create IPSec policies, you must configure rule that include the following settings - IP Filter List, Filter Action, Authentication Method, Connection Type and Tunnelling setting.

IP Filter List defines the type of network traffic that the IPSec applies to:

- Source address – specific IP address, specific IP subnet address or any address of the source host
- Destination address – IP address of the destination host, also can be specific IP address, specific IP subnet address or any address
- Protocols – it is possible to choose a specific protocol like TCP, UDP, etc. or use protocol ID number
- Source port – you should define source port if you choose TCP or UDP protocol
- Destination port – you should define destination port if you choose TCP or UDP protocol, for example for HTTP – TCP port is 80, for Telnet – TCP port 23.

Filter Action defines how will be handled traffic in the IP filter List by the filter rule. The possible three Filter Actions are listed below:

- Permit – allow receiving or sending packets in plaintext (for example, without encryption). Security will not be requested for these packets
- Block – discard packets. If the associated IPSec filter is match (between two computers), all packets will be discarded if the choose is Block action
- Negotiate security – the administrator defines the desired integrity and encryption algorithms to secure data transmissions if an IPSec filter is match.

Integrity and encryption algorithm

Integrity algorithm:

- MD5 – Message Digest Algorithm 5 was designed by Ron Rivest in 1991 and widely applied to check the integrity of files. The MD5 algorithm takes as input a message of arbitrary length and produces as output a 128-bit "message digest" of the input.
- SHA1 – stands for Secure Hash Algorithm and was designed by the National Security Agency and published by the NIST as a U.S. Federal Information Processing Standard. When a message of any length, smaller then 2^{64} bits is input, the SHA-1 produces a 160-bit output called a message digest.

Encryption algorithm:

- DES – Data Encryption Standard (block cipher is a symmetric key cipher). Used when the high security and overhead of 3DES are not necessary
- 3DES – common name for the Triple Data Encryption Algorithm. Used when high security is required. 3DES processes each packet three times, using a unique 56-bit key each time. It is important to take in mind that computers running Windows 2000 must have the High Encryption Pack or Service Pack 2 (or later) installed in order to use the 3DES algorithm.

Authentication Method must be chosen for each filter rule. You can enable multiple Authentication Methods for each rule and determine their order of precedence. The Authentication Methods can

be Kerberos V5 authentication, public key certificate for authentication services and Preshared key – defined own key on both nodes that will be used for authentication.

For **Connection Type** you must specify what type of interfaces each filter rule applies to. It is possible to choose:

- All Network Connection
- Local Area Network Connections
- Remote access Connections

Tunneling setting. IPSec operates in two modes:

- Transport mode – host to host communication. In transport mode, only the payload (the data you transfer) of the IP packet is encrypted and/or authenticated.
- Tunnel mode – network to network, host to network communication. In tunnel mode, the entire IP packet (data and IP header) is encrypted and/or authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is used to create Virtual Private Networks for network-to-network communications (IPSec tunnel between routers) or host to network communication (IPSec tunnel between a host and a router)

IPSec technology is very complex and flexible, for that reason IPSec policies are widely used to protect inbound and outbound Internet and Intranet traffic. IPSec policies are manually configured to individual nodes and this process is very critical for policies to be specified and configured correctly.

Conclusion

Using IPSec protocols enable to transfer classified information across the network.

To implement IPSec policies it is necessary to have following in mind:

- Defining Security policy for the LAN is a very important process, which must be very carefully planned.
- Two parties who wish to create an IPSec must first negotiate on a standard way to communicate.

- Configure the same IPSec policy for each node of the LAN. Since IPSec supports several modes of operation, both sides must first decide which security policy and mode to use, which encryption algorithms they wish to communicate with and what type of authentication method to use.
- IPSec policies can make one computer functionally invisible to another
- It is obligatory to assign static IP address for each node – do not use DHCP (Dynamic Host Configuring Protocol)
- It is important to assess security and performance requirements because of using IPSec increases network traffic due to IP packet size augmentation and decreases network throughput [**Error! Reference source not found.**].

References

1. <http://www.ibm.com/developerworks/library/s-ipsec.html>, 07.05.2009
2. <http://seclab.cs.ucdavis.edu/papers/policydsom.pdf>, 07.04.2009
3. http://securitytechnet.com/resource/rsc-center/vendor-wp/openreach/IPSec_vs_SSL.pdf, 07.05.2009, IPSec vs. SSL: Why Choose? Remote VPN Access from Anywhere, An OpenReach Backgrounder Comparing VPN Technologies
4. <http://www.arraynetworks.net/ufiles/File/SSLVPNvsIPSecWhitePaper021006.pdf>, 01.05.2009
5. <http://technet.microsoft.com/en-us/network/cc987611.aspx>, 26.04.2009
6. <http://bg.wikipedia.org/wiki/IPsec>, 01.05.2009
7. Николова Д., М. Божилова, И. Христов, IPSec политики за сигурност, 24.02.2009, конференция, факултет „Командно-щабен”, катедра „Комуникационни и информационни системи”, ВА „Г. С. Раковски”
8. Смит Б., Б.Комар, Microsoft Windows Security resource Kit, Софтпрес

HIGH-TECH OUTSOURCING SERVICES IN BULGARIA: SURVEY RESULTS

Assoc. Prof. Matilda Alexandrova, PhD⁶²

Chief Assist. Prof. Svetla Boneva, PhD⁶³

1. Introduction

At the current stage of applied research in the area of high technology services outsourcing it is found that business organizations decide to transfer such kind of services to other firms (identified as “vendors”) mainly because of cost-related advantages. It is still not clear whether vendors are able to provide comparative advantages from the point of view of economizing costs of the production of these services. It is valid predominantly for the large organizations having the capacity to organize their own provision of such services on the bases of a particular costs minimization strategy. The contradictory success of outsourcing practices during the last few decades requires a more comprehensive study of the actual value added by vendor organizations through the provision of the transferred services.

As far as outsourcing decisions of a particular business organization and its relations with the vendor organization have been extensively studied in the specialized literature, the point of view of the vendor organization is still not analyzed in adequate extent. It is particularly valid for such organizations in Bulgaria that are positioned on this global market and endeavor to develop their own competitive advantages.

The paper hereafter presents some selected results from a study⁶⁴ of

⁶² Associate Professor, Department of Management, UNWE – Sofia; e-mail: matil-daa@unwe.acad.bg.

⁶³ Chief Assistant Professor, Department of International Economic Relations and Business, UNWE – Sofia; e-mail: svetla_bogdanova@yahoo.com.

⁶⁴ The study is supported by a research grant № NID 21.03-3/2007 of the UNWE Research Program.

the outsourcing relations between Bulgarian vendor organizations and their client organizations (outsourcers) considering the issues of the development of successful strategic partnerships in outsourcing practices.

As a main hypothesis of the study was raised the existence of an interrelation between the efficiency of business activity of vendor organizations originating from the economic gains achieved on the basis of developing a system of key competences. They appear to be “complementary” in respect of the competences of client organization. This can be explained by the fact that the vendor organization makes efforts to build own technologic infrastructure, know-how, and capacity by which to substantially increase the efficiency of realization of a set of similar high technology services. A strategic partnership assumes sharing of the value added between the vendor and the client generated through the attainment of the comparative advantages. This is realized by a complex of both formal and informal relations between units of the organizational structures of partner organizations.

Thus, the object of the study are the partner relations between Bulgarian vendor organizations and client organizations (which currently are from USA and EC). The main research thesis is focusing on the assertion that an outsourcing partnership provides benefits for client organizations which they otherwise could not achieve within their own organizational context at the same level of economic, organizational, and technological efficiency. The main risks associated with the realization of outsourcing partnerships as well as the strategic perspectives of these partnerships are identified.

2. Literature review

The main orientation of the research in the area of outsourcing of high technology services are the various aspects of vendor-client interrelations. Various studies find a relative parity between the importance of the informal aspects of these relations (e.g. personal trust) and the formal aspects formulated in the outsourcing contract (Poppo, 2002). In order to achieve a strategic partnership however it is necessary that both aspects of these relations are emphasized (Kern & Willcocks, 2001). According to the study of Kern & Willcocks the strategic

vision and the technical capacity shape not only the formal structuring of contract relations but also the development of inter-personal relations. As factors influencing the success of the outsourcing partnerships can be highlighted: the high degree of synchronization between the client and the vendor; team working; balance of control function; clear responsibilities of the partners; the degree of flexibility and intensity of the transferred processes (Goles, 2001).

For example, the interrelations based on the orientation to the utilization of advantages originating from *technological leadership of vendor organization* (regarding the contracted service) for increasing the efficiency of IT operations of the client organization could provide a higher value added only if *sustainable partnership relations have been established*. For the development of such kind of partnership relations various successfully applied approaches are known, e.g. realization of pilot projects for cooperation; contracts with multiphase realization and evaluation of intermediate results; precise choice between flexible contracting and contracting at fixed conditions; contracting mechanisms with a bilateral risk sharing; establishment and bilateral promotion of partners reputation, etc. (McDonnell & Lichtenstein, 2002).

In another case the increase of IT operations efficiency could be achieved by the establishment of another type of relations with the vendor organization, namely the “pay-per-service” scheme, when the vendor offers a wide range of services and accessible capacity of resources, but is not a technological leader in the branch. From the point of view of developing partnerships of that type, the preferred principles of the negotiations are: short-term contracting; simultaneous provision by few vendors (i.e. maintaining a competitive environment), clear criteria for stimulation / sanctioning, etc. (Lacity & Willcocks, 1998; Currie, 1998).

Relatively little attention in research literature is paid on the characteristics of the vendor organization having significant relation to the process of value adding by the outsourcing partnership. For example, on the basis of theoretical hypotheses Goles (2001) derives several important factors characterizing the vendor organization: techni-

cal competencies; knowledge of the subject area and the specifics of client's operations; competences for coordination and management of partner relations. Albeit the interest about these characteristics is growing there is a scarcity of empirical evidence for the specifics and the degree of their impact on the success of the partnership.

3. Questionnaire survey of high-tech outsourcing services partnerships

In year 2008 an empirical survey of outsourcing partnerships in the area of high technology services has been conducted based on cases of Bulgarian vendor organizations. The subject of the study was the analysis of the key determinants influencing the formation and development of strategic outsourcing partnerships between Bulgarian vendor organizations and their clients (foreign companies).

The model of determinants facilitating the success of the partnership between a client and vendor organization (in the process of outsourcing of high technology services) assumes a clarification of the interrelations between a complex of determinants and a response variable capturing the level of success of the outsourcing partnership. The model incorporates the following key determinants:

1) Bidirectional transfer of knowledge /BTK/

BTK emerges when optimal (as a quantity and quality) information necessary for the realization of the service is provided through the channels of effective communication between the partners. The knowledge could have two forms: implicit /informal, tacit/ and explicit /formal/ (Nonaka & Takeuchi, 1995). Special attention should be put on the way which organizations "learn" from their partners as this appears to be one of the means for development of key competences. The following research hypothesis is raised in respect of this determinant:

H1. The degree of success of outsourcing partnership is positively related to the degree of effectiveness of BTK.

The operationalization of the BTK in the framework of the study is realized on the basis of four primary measures that capture the extent of:

1.1. the exchange of organizational knowledge about key business processes;

1.2. the exchange of information about the impact of business environment factors;

1.3. incorporation of bilateral information exchange in the business planning of organizations;

1.4. incorporation of bilateral information exchange in the technological development of organizations.

2) Achievement of the contracted goals as results of outsourcing partnership

Another key determinant in the model is the degree of achievement of results set as contract goals in the outsourcing agreement. This degree should reflect the divergence between actual benefits and relative costs that client organization would have to spend without the realization of the particular partnership (Anderson & Narus, 1990). A research hypothesis regarding this determinant is also raised:

H2. The degree of success of outsourcing partnership is positively related to the degree of achievement of contracted goals.

3) Mutual trust

The third key determinant reflects the intensity of the informal relations between partner organizations having in great extent a psychological dimension. The degree of trust between the partners compensates any eventual drawbacks of the formal contracting and the lack of strong defence clauses in outsourcing agreement (Lee & Kim, 1999). This determinant reflects the flexibility of the cooperation and the orientation to mutual correctness based on the understanding that the interests of the partner organization should be respected (as far as “the success of the partner works for our own success”). The following research hypothesis is raised in respect of this determinant:

H3. The degree of success of outsourcing partnership is positively related to the degree of mutual trust between the partners.

4) Security assurance of outsourcing partnership

The existence of security assurance is an important determinant of the success and sustainability of outsourcing partnership that is

likely to provide strategic nature of the partnership. Unlike the mutual trust (that is of informal nature) the availability of security assurance has entirely formal character as far as it is incorporated in the outsourcing agreement. These warranties should be provided by special clauses in the contract. As a base precondition for the provision of reliable assurance is a targeted negotiation process before the finalization of the contract (i.e. the decision to form the outsourcing partnership). The following research hypothesis regarding this determinant is raised:

H4. The degree of success of outsourcing partnership is positively related to the degree of security provided in the agreement.

5) Interdependence between client and vendor organization

This determinant reflects the degree of dependency of the activities of client organization from the operations of the vendor organization supplying a high technology service as a subject of the outsourcing agreement. This interdependence has a clear bidirectional nature – often in practice the vendor organization is strongly dependent on the realization of contracted service. It is particularly valid in cases when the vendor is serving one key client or diversification of the vendor services/client was not achieved.

The model assumes that the impact of this determinant is moderated by the effect of the levels of mutual trust and security assurance (warranted by the outsourcing agreement). It is hypothesized that if there is a positive impact of at least one of these (conditionally defined as “moderating”) determinants, a positive relation can be observed between the success of partnership and the level of vendor-client interdependence. In the same time, having a situation characterized by a lack of trust and low security guarantees, the effect of the mutual interdependence should be negative. Thus, the research hypothesis regarding this determinant is raised as follows:

H5. The degree of success of outsourcing partnership is positively related to the degree of interdependence between the operation of the client and the vendor organization, with a moderating effect of the determinants “mutual trust” and “security assurance of the agreement”.

6) Shared values within the outsourcing partnership

The sustainability and the strategic nature of outsourcing partnerships are expected to reflect the sharing of common values, principles, and cooperation ideas as elements of the organizational cultures of partner organizations. As a result of the formation of the outsourcing partnership transformations of organizational cultures have often taken place in both client and vendor organizations. Along with the direct net benefit of the agreement having immediate effect on the economic status of the partner organizations, the sharing of common values and the exchange of organizational and managerial know-how has a significant (although indirect) long-term effect on the operation of the organizations. The research hypothesis regarding this potential determinant states that:

H6. The degree of success of outsourcing partnership is positively related to the degree of sharing of common values between the partner organizations.

7) Level of risk

A key determinant of the success of the outsourcing partnership is the level of risk associated with the process of realization of the contracted high technology service. This risk has a complex character with various sources, e.g.:

- possible deviation of the actual from planned results;
- possible delay in the deadlines and contracted schedule;
- possible overspending of resources (and the budget respectively);
- possible changes in the operational procedures contracted in outsourcing agreement;
- possible technical problems emerging during the realization of the service;
- possible conflicts of interests between the partners at various levels (management, experts, other staff), etc.

The contracted relations in the outsourcing partnership assume identification, evaluation, and comprehensive analysis of the potential sources of risks that can lead to obstruction and blockage of the service itself, considerable financial losses, worsening of the reputation of the partners, and even to failure of the business (DeLoach, 2000). As a

key aspect related to the normal existence and the survival of the organization is considered the adequate assessment and monitoring of the risks, and on that basis, the capability of the organization to react *ad-hoc* when risky situations emerge.

During the realization of outsourcing partnerships in the area of high technology services some specific risky situations can emerge, e.g.:

- related to the security of the information exchange between the partners (possible leakage of insider information);
- originating from difficulties with maintaining the loyalty of the personnel after the realization of the organizational changes being a result of the outsourcing agreement;
- problems with the motivation of client organization's personnel due to the fact that important ICT functions become a responsibility of the vendor;
- problems originating from the low likelihood of the vendor organization to transfer knowledge about ICT functions back to the client organization;
- problems related to the transfer of responsibility between the partners with not enough clear formulation of the clauses of outsourcing agreement.

H7. The degree of success of outsourcing partnership is negatively related to the degree of risk associated to the outsourcing partnership.

8) Other characteristics of the organizations that should be controlled for in the analysis of the interrelations (as key features of the outsourcing partnership) are embraced in the profile of the respondent organizations. Such variables are:

- total duration of the activities of the organization (year of establishment);
- size of the organization (number of employees);
- sector / branch of the main activity;
- experience in outsourcing (duration);
- type of outsourced services / ICT functions.

B. Success of outsourcing partnership

The degree of success of outsourcing partnership is the main *dependent (response) variable* in the model. It is however commonly considered as quite difficult for operationalization and empirical measurement as far as it is of multidimensional nature. For example, Lee & Kim (2003) define the success of partnership as the degree of satisfaction of the needs of client organization from the services provided by the vendor organization. Other points of view are also applicable, e.g. that which characterizes the outsourcing partnership success by the degree of achievement of overall (pan-organizational) comparative advantage through outsourcing of all or part of ICT functions of the client organization.

In the specialized literature two dimension of the success are considered – “net benefit” and “service quality” (Lee & Kim, 2003). Generally, the outsourcing decision is motivated by the endeavour to realize strategic, economic, and technologic benefits (Grover et al., 1996). In the same time, of considerable importance for this success is the level of quality of the service supplied (DeLone & McLean, 2003). Here one should have in mind that the evaluation of the quality level might diverge from the different points of view of the vendor and client organization, where different operational measures could be adopted for capturing the service quality level (Jiang et al., 2003).

II.2. Methodology of the study

The provision of the information for the pilot study of outsourcing partnerships in Bulgaria, and about the determinants that are expected to influence the success and its strategic dimensions, is conducted by the method of personal interview. Object of the pilot study were 28 Bulgarian vendor organizations in the branch of high technology services having two or more outsourcing projects realized (or currently working for 2+ international client organizations). Because of the specific character of these organizations the sample was selected by the purposive sampling method⁶⁵ where the potential of the Internet, information and communication network of Bulgarian Investments Agency was utilized.

⁶⁵ For more details see: www.socialresearchmethods.net.

The respondents in respective organizations have key managerial positions at various levels and are directly responsible for the realization of the outsourcing partnerships. Most of the questionnaires (21) are filled by the “face-to-face” interview method and the rest by self-interviewing using electronic questionnaire form. For this purpose, a specialized instrument for empirical study of outsourcing partnerships (realized by Bulgarian vendor organizations) was developed as a questionnaire for structured interview. The emphasis is put mainly on *the characteristics of the partnership itself* rather than on the characteristics of these organizations. The questionnaire was used to record the individual information and contains 20 questions directed to the respondents. These questions are targeted in the operationalization of the response variable and the determinants of outsourcing partnership as defined in the model. The concept indicators extracted by specific sets of items (taken from the questionnaire) have been verified and prepared for further data processing and analysis of results.

The operationalization of the concept indicators is performed through a multivariate (multi-item) method where for each determinant 1 to 4 questions are utilized. For the standardization of primary data a unified 7-rank Likert scale for the answers was adopted which allows the summarization of the answers on the items to extract one empirical measure (variable) for each concept indicator. Rank 7 codes the opinion expressed at the maximum of the scale (e.g. maximum degree of agreement with the respective statement) and with rank 1 respectively at the minimum of the scale.

The current pilot survey can be treated as a first step in the probation of a methodology through which a reliable and justified evaluation of the characteristics of outsourcing partnerships in Bulgaria can be obtained. Along with the evaluation of the status of these partnerships, the development and application of this methodology could support the identification of the perspectives for development of the outsourcing of high technology services in the country as well as to provide a basis for comparison of Bulgarian practices with the world experience in this area.

4. Main results from the survey

A) Main characteristics of respondents

For each of the organizations interviewed a set of characteristics is obtained in order to describe their profile – legal status (type of firm), size, type of the main activity, foreign participation in the capital, etc. According to their legal status, shareholding and limited responsibility companies prevail (almost 40% for each of them) and about one fifth are the single-owner limited responsibility companies.

A variety is observed also about the size of organizations captured by the number of the employees – almost one third (32%) are big enterprises (over 250 persons according to Bulgarian Law on SMEs) and only 11% are micro-enterprises (up to 10). The rest of respondents are from the category “Small and Medium Sized” enterprises. However, about two thirds of the respondents declare that they regularly hire part-time personnel.

According to the presence of foreign shareholders about one fourth of the firms involved in the pilot survey are mixed enterprises and about 11% are companies entirely owned by a foreign investor. This undoubtedly provides these organizations with options for transfer of contemporary managerial and technological know-how in the area of high-tech business. And almost two thirds of the interviewed are fully domestic companies. About 40% of the organizations classify their main activity as being in the software industry (software development and/or implementation-at-client) and almost 30% are providing Internet-based communication services. Several organizations identify as their main activity: telecommunications, database management services, call centres as well as financial services.

B) Results on the success of outsourcing partnerships

In this pilot study the success of an outsourcing partnership is evaluated by the degree of matching between goals planned and results actually achieved. This evaluation is required in respect of four key dimensions: the realization of expected financial benefits; complying with the deadlines; successful execution of the tasks; provision of the required service quality.

Table 1

Dimensions of outsourcing partnership success

	B10. Degree of matching:			
	1. financial results	2. deadlines fixed	3. tasks executed	4. service quality
1) very low	–	–	–	–
2) low	–	–	–	–
3) moderate (–)	–	14.3	–	–
4) moderate	32.1	17.9	7.1	–
5) moderate (+)	50.0	57.1	28.6	10.7
6) high	17.9	7.1	39.3	60.7
7) very high	–	3.6	25.0	28.6
Total:	100.0	100.0	100.0	100.0

A already mentioned above, caution should be put here since the evaluation of the results achieved may diverge from the points of view of the vendor and client organizations. In our case the evaluation results obtained by the pilot survey reflect the position of the vendor organizations (it would be of major interest to obtain also the evaluation of the representatives of client organizations). As a whole, the results achieved are favourably evaluated by the representatives of the vendor organizations where we do not observe any “low” and “very low” degree of achievement evaluations.

The degree of realization of the financial goals is found to be “moderately high” and “high” for over two thirds of the vendor companies and the almost the same share is observed in respect of the degree of completion of the tasks. Moreover, regarding the latter item about one fourth declare that the degree of achievement of the goals is very high which is comparable with the result on the “service quality” dimension. The lowest level of achievement is evaluated about the compliance with the contracted deadlines where almost two thirds of respondents define the degree as “moderately low” (14%) и “moderate” (19%).

C) Model of the determinants of outsourcing partnership success

The model of the determinants is depicted on fig.1 where the preliminary results for the correlations between the variables are presented. They are obtained as Pearson correlation coefficients measured for the summarized (composite) success variable and the composite variable for each determinant. Considering the hypotheses raised about the potential interrelation between each determinant in the model and the level of success of outsourcing partnership, the following results were obtained.

H1. The hypothesis for the presence of a positive relation with the effectiveness of the bidirectional transfer of knowledge is confirmed by the observation of a moderate positive correlation (0.57).

H2. The hypothesis for any positive interaction with the degree of achievement of contracted goals is also confirmed, however, at the higher estimated correlation (over 0.8) which provides evidence for the strongest effect of this determinant on the level of partnership success.

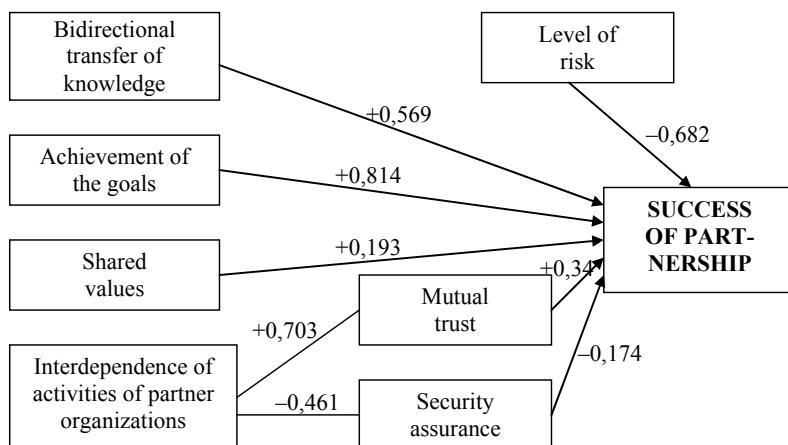


Figure 1. Estimated correlation coefficients in the model of determinants of outsourcing partnership success

H3. As assumed, the degree of success of outsourcing partnership is also positively related to the degree of mutual trust, albeit confirmed by a relatively low correlation (0.34) possibly due to the simultaneous influence and moderating effect of several variables. These effects should be further analyzed by specific multivariate method.

H4. The hypothesis about the relation with formal security assurance is not confirmed – the correlation is not significant and its negative sign (-0.17) could be ignored. At that stage we can conclude that the formal warranties included in the outsourcing agreement do not directly contribute to the level of success of the partnership. The results show that other factors (e.g. informal relations and trust) have strongest impact on the response variable.

H5. The evaluation of the interrelation between the degree of success of outsourcing partnership and the interdependence of the operation of vendor and client organizations is influenced by the moderating effects of two determinants causing a strong multicollinearity. A strong positive correlation is observed between the degree of interdependence and the level of mutual trust (0.7) as well as moderate negative correlation with the level of formal security assurance (-0.46). Here the analysis is to be further clarified in order to derive the net effects of each determinant on the response variable (the level of partnership success).

H6. On the basis of the low correlation (0.19) it can be concluded that the degree of success of outsourcing partnership is not substantially related to the degree of sharing of common values between partner organizations – this aspect of high technology services outsourcing is to be developed still in the process of integration of Bulgarian organizations in the global economy.

H7. The hypothesis about the effect of the level of risk is confirmed in light of one of the highest correlations estimated (-0.68). The degree of success of outsourcing partnership is negatively related to the level of risk associated with the partnership – as it was expected, lower levels of success are evaluated (on average) with highest levels of risk generating an unhealthy environment for the operation of the outsourcing agreement.

5. Final remarks

The development of high technology services outsourcing in Bulgaria is oriented to the options for solving intra-organizational problems, e.g. the improvement of internal business processes through formation of managerial competencies and transfer of managerial know-how from developed business organizations having strategic interests to transfer their own processes in Bulgaria as a new EU member state. The influence of outsourcing on the development of human resources in the area of high technology services is undoubtedly *a basis for improvement of professional qualifications, narrowing of labor specialization, and finally an increase of the efficiency of the business processes*. Such a process presumes sustaining the tendency for outsourcing to evolve from a purely tactical and short-term managerial tool to its formation as a long-term perspective assuming the establishment of strategic partnerships between domestic organizations and foreign companies.

6. Literature

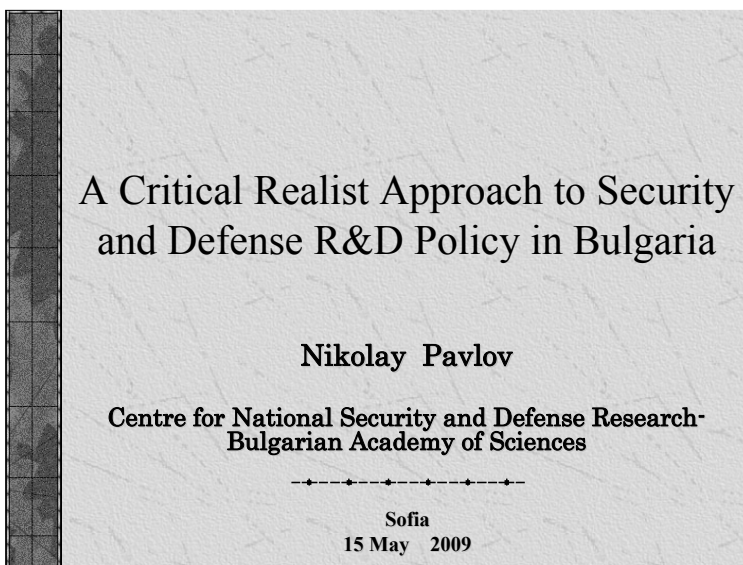
1. Anderson, J., Narus, J., 1990. A Model of Distributor Firm and Manufacturer Firm Working Partnerships. *Journal of Marketing* 54 (Jan), 42-58.
2. Currie, W. 1998. Using multiple suppliers to mitigate the risks of IT outsourcing in two UK companies: ICI and Wessex Water, *Journal of Information Technology*, 13: 169-180.
3. DeLoach Jr., J.W. 2000. *Enterprise-wide risk management: Strategies for linking risk and opportunity*. London: Financial Times.
4. DeLone, W.H., McLean, E.R. 2003. *The DeLone and McLean Model of Information Systems Success: A Ten-Year Update*. *Journal of Management Information Systems*. Vol. 19. No4: pp9-30.
5. Goles, T. 2001. *The Impact of Client-Vendor Relationship on Outsourcing Success*. Houston, TX: University of Houston.
6. Grover, V., Cheon, M.J., Teng, J.T.C. 1996. *The effect of service quality and partnership on the outsourcing of information systems functions*. *Journal of Management Information Systems*. Vol.12.Issue4:pp 89-116.
7. Jiang, J.J., Klien, G., Tesch, D. and Chen, H-G. 2003. *Closing the User and Provider Service QUALITY GAP: A method for measuring service*

- quality that includes both the user and IS service provider perspectives. Communications of the ACM. Vol.46, No.2, pp.72-76.
8. Kern, T., and Willcocks, L. 2001. *The Relationship Advantage: Information Technologies, Sourcing, and Management*. Oxford, New York: Oxford University Press.
 9. Lacity, M.C., and Willcocks, L.P. 1998. An Empirical Investigation of Information Technology Sourcing Practices: Lessons From Experience. *MIS Quarterly*, September 1998, pp. 363-408.
 10. Lee, J.N., and Kim, Y.G. 1999. The Impact of Knowledge Sharing, Organizational Capability and Partnership Quality on IS Outsourcing Success. *Journal of Management Information Systems*, 15: 29-61.
 11. Lee, J.N. and Kim, Y.G. 2003. *Exploring a Casual Model for the Understanding of Outsourcing Partnership*. Proceedings of the 36th Hawaii International Conference on System Science, p. 268.
 12. McDonnell, A., and Lichtenstein, Y. 2003. Pricing Software Development Services 2002. (<http://mis.ucd.ie/staff/YLichtenstein/alan.doc>; March 10, 2003).
 13. Nonaka, I. and Takeuchi, H. 1995. *The Knowledge-Creating Company*. Oxford University Press, New York.
 14. Poppo, L. 2002. Do formal contracts and relational governance function as substitutes or complements? *Strategic Management Journal*, 23: 707-722.

A CRITICAL REALIST APPROACH TO SECURITY AND DEFENSE R&D POLICY IN BULGARIA

Mr. Nikolay Pavlov

Centre for National Security and Defense Research -
Bulgarian Academy of Sciences



Purpose of the study

- ✧ Critical Assessment of the Defense R&D "Policy" in Bulgaria. The need for critical realist approach.
- ✧ To present an academic survey of the Defense R&D "Policy" in the context of the specialized R&D data base in Bulgarian Academy of Sciences.
- ✧ A prototype of a knowledge management system - is it worth? Where are the end-users?

General Framework of Security and Defense R&D in Bulgaria

- ✧ Security and Defense R&D in Bulgaria is not institutionalized as a separate scientific field
- ✧ Interdisciplinary studies that fall in various scientific domains
- ✧ EU 7-th Framework Programme - 1,4 billion EUR for Security theme
- ✧ The wider context of scientific research in Bulgaria – poor prospects as a whole. Lack of state policy and political will – underfunded, fragmented and ageing scientific community.

Defense R&D Policy in Bulgaria from the BAS perspective

- ✱ 1999 – Framework Contract between MoD and BAS – the establishment of a specialized coordination body within the Academy in 2001
- ✱ Years of active cooperation – 2000-2003
- ✱ The main R&D players in BAS – Institute of Metal Science, Institute of Space Research, Institute of Parallel Processing, CNSDR и Institute of Hydro- and Aero-dynamics
- ✱ The need for Security and Defense R&D Strategy (Programme) in Bulgaria

Current State of Defense R&D

- ✱ Major shortcomings and “mazes” in the defense R&D system
- ✱ Lack of will and efforts in the higher political ranks of MoD to realize effective R&D policy
- ✱ Defense R&D funding - 0,1-0,18 % from MoD budget (500 000 EUR) – it is spent for Bulgaria’s annual participation in NATO *Alliance Ground Surveillance* - AGS
- ✱ Ministry of Emergency Situations takes the initiative – the draft National Programme for protection against natural disasters

A Survey of Bulgarian Security R&D projects for the last decade (1999-2008)



Conclusions

- ✱ The relations between public authorities (MoD) and research organizations (such as BAS) are dependent on the state political leadership. The constitutional sovereign of the state – the nation (and civil society) is excluded from this equation.
- ✱ A possible solution of the democratic deficit in this respect is active civil-military cooperation in defense R&D policy implementation, that is cooperation between civil and military research organizations.

PRESENTATION OF GAMA PROEKT 99 Ltd

Mr. Hristo Georgiev
Mr. Dobromir Georgiev



ГАМА ПРОЕКТ 99 АД



5300 ГАБРОВО, ул. "Орловска" 164, Тел.: 066 803303, 807177, Факс: 066 809099

E-mail: gp99_marketing@mbox.contact.bg, www.gama-proekt99.bgcatalog.com

BASIC PRODUCTS AND SERVICES:

1. TOOLING EQUIPMENT (designing and manufacturing to customer's order)

- **Stamping tools** (cutting, drawing and multiple, bending, fine and combined action)
- **Dies**
- **Injection moulds**
- **Blow moulds**
- **Moulds for blow-moulding of polyethylene parts**
- **Pressure casting moulds and other tools**
- **Benders**
- **Forms for casting of aluminium and zinc-aluminium alloy**
- **Measuring tools:** gauges for checking holes, internal threads, external threads, smooth shafts; height gauges, depth gauges, horseshoe gauges, and layout gauges. Minimum quantity for the order to be manufactured for all tools is 10 pieces.
- **Non-standard cutting tools:** taps, milling cutters, thread milling cutters, counter-bores, straight and helical fluted reamers, profile turning cutters, thread rollers

2. MANUFACTURING OF SPECIALIZED MACHINES AND EQUIPMENT

3. AUTOMATION DEVICES

4. PRODUCTION OF ARMAMENT AND DEFENSE APPLIANCES

- **Gun locks KO 1**
- **Portable metal detectors**
- **Plug-detonators for accoutrements for grenade launcher**

5. DESIGNING AND PRODUCTION OF NON-STANDARD MECHANICAL, ELECTROMECHANICAL AND ELECTRONIC DEVICES (TO CUSTOMER'S ORDER OR DOCUMENTATION PRESENTED)

6. MANUFACTURING AS WELL AS OTHER SERVICES TO CUSTOMER'S ORDER

- **Cutting and bending parts**

BUSINESS AND SCIENCE FOR SECURITY
AND DEFENCE INDUSTRIAL R&D

Tilcho Ivanov and contributors

First Edition

Editors:

Prof. Tilcho Ivanov, PhD

Assoc. Prof. Dimitar Dimitrov, PhD

Assist. Prof. Konstantin Poudin, PhD

Size 60x84/16

Quires 18,25

AVANGARD PRIMA
ISBN 978-954-323-579-7

Sofia, 2009