Shaping Bulgaria's Security and Defence R&T Policy

Stefan Hadjitodorov, Todor Tagarev and Nikolay Pavlov [1]

The main goal of this paper is to formulate fundamental principles in shaping an efficient security and defence R&T policy of the Republic of Bulgaria. Presently, due to a variety of reasons, there is no comprehensive, well-focused and sustainable security and defence R&T policy of the country that is clearly linked to its security and defence objectives. We see this as an important drawback in both the formulation and the implementation of the overall Bulgarian security policy.

The underlying premise of this study is that R&T policy has to be examined much more broadly than is currently the case. It is readily admitted that R&T policy ought to support the achievement of security objectives (although even in such case adequate management mechanisms are not readily available). On the other hand, and this is rarely understood, research can potentially support the formulation of an effective and efficient security and defence policy.

In support of the formulation of security policy, scientists analyse the security environment and support the definition of capability requirements, identification of capability gaps and possible solutions, accounting for novel threats and disruptive effects of emerging technologies. Analysts further support security and defence planning through generation and analysis of alternative solutions, assessment of costs and benefits, assessment of planning risks and support to risk management.

In support of the implementation of security policy scientists provide alternative solutions, emphasising capability development plans, concept development and experimentation (CDE), operations and maintenance, as well as the utilization of surplus and/or obsolete equipment and infrastructure.

Main principles of Security R&T Policy

First, we need to define properly the scope of security and defence R&T programs. Most important in this regard is to examine:

- o Capability orientation of security and defence R&T
- o The relationship among end product, systems, and enabling technologies
- o The contribution of variety of think-tanks and research organizations with primary focus on governmental R&T organisations, academia/ universities, and security and defence industries, as well as their interaction and cooperation with other players.

Secondly, security R&T policy supports both the formulation AND the implementation of security policy. It is very important that the most senior political leadership makes a clear declaration in that regard and, henceforth, provides definition of realistic ambitions for security R&T policy and formulates the precise roles of professional / expert entities in the planning process, the development of capability models and product development.

In order to devise an adequate and realistic security and defence R&T policy the political leadership should:

- o Set objectives and ambitions
- o Provide financing, adequate to these ambitions
- o Implement output- and outcome-oriented planning (and later - management) through program-based management.

The creation of such security and defence R&T policy should account for:

- o Common taxonomy of security technologies, systems, products, etc.
- o Common models of the life cycle of security and defence products
- o Assessment of technology readiness levels.

No less important would be a mechanism for prioritization that reflects areas of specialisation, e.g., in certain security and defence capabilities, available capacities, and competitive advantages sought.

In summary, a solid basis for effective R&T policy could be set through involvement of all major stakeholders in order to:

- o Define scope and requirements
- o Define realistic ambitions (at least three distinct levels)
- o Define ways to achieve the ambitions:
    - - on our own (national level)
    - - on a bi-lateral basis
    - - working within the framework of NATO Research and Technology Organisation
    - - working with the EU / European Defence Agency
    - - in other formats.

A good example for capabilities-based approach in R&T policy is the EU approach that is implemented in EU Framework Programme 7, Security theme. After an extensive capabilities-based study the European Security Research Advisory Board (ESRAB) developed in 2006 a detailed European Security Research Agenda. This Agenda underlies the EU Framework Programme 7, Security theme which has 7 main areas of research:

1. Security of Citizens
2. Security of Infrastructures and Utilities
3. Intelligent Surveillance and Border Security
4. Restoring Security and Safety in Case of Crisis
5. Security systems Integration, Interconnectivity and Interoperability
6. Security and Society
7. Security Research Coordination and Structuring

It should be noted that during the last years a number of EU countries – Germany, France, the United Kingdom, Austria, The Netherlands, Finland and Romania developed their own National security research programmes. These national programmes are based mainly on the Security theme of FP7.

On the road to a Bulgarian Security Research Programme

There is strong need for the development and implementation of a Bulgarian national Security Research Programme. Such a programme could be developed in close cooperation among governmental R&T organisations, academia / universities and the industry. The Centre for National Security and Defence Research (CNSDR) could contribute with its experience and know-how that was accumulated during the last five years within the Bulgarian Academy of Sciences.

CNSDR was established in 2002 as a specialized coordination body within BAS on the basis of a Framework Agreement for Cooperation between the Ministry of Defense and BAS. The Centre facilitates security and defence research throughout the Academy through provision of timely and accurate information to BAS institutes, research teams and individual scientists on user needs and programs, opportunities for bilateral and multilateral cooperation, in particular within the framework of NATO and EU research and technology activities. To this effect CNSDR maintains close exchange with all main users within Bulgaria – the Ministry of Defence, the Ministry of Interior, the Ministry of State Policy for Disasters and Accidents, "G.S. Rakovski" Defence and Staff College, and others. CNSDR maintains a database of available technologies and the capacity of research units, teams and scientists, informs potential users and facilitates contacts and cooperation between researchers and users.

In 2002 CNSDR conducted a major study on Research Support for Planning the Modernization of the Bulgarian Army: an Inventory of security research capabilities in BAS. This study was conducted in close cooperation with Department "National and Regional Security" at the University of National and World Economy. The study was used by its end-user – the Ministry of Defence in the Bulgarian Armed Forces Modernization Plan.

During the last years very active Security R&T Policy is conducted by the Standing Governmental Committee for Protection of the Population against Natural Disasters and Accidents (SGCPPNDA). In 2003 a Scientific Coordination Council was established within SGCPPNDA. The Centre for National Security and Defence Research (CNSDR-BAS) is the administrative Secretariat of the Scientific Council. The Centre coordinates the applied research of 7 Expert Councils dealing with radiological, chemical, medical, seismic, meteorological, biological protection and the

protection of the population and critical infrastructure. The Centre organized two national research conferences on emergency management and critical infrastructure protection in 2005 and 2007. In 2006 CNSDR co-organized the TACOM (Terrorist Act Consequences Management) exercise which is part of the National Crisis Management Exercise "Protection – 2006".

For five years of its existence CNSDR's main achievement is better coordination and priority setting in the sphere of security research within BAS. Therefore CNSDR strongly supports the development and implementation of a comprehensive Bulgarian security and defence R&T programme. On the road to such a programme a number of steps have to be done:

- o Political will for the development of a Bulgarian security research programme
- o Survey of existing institution-focussed security R&T quasi-programmes in Bulgaria – especially in the Ministry of Defence, Ministry of the Interior and the Ministry of State Policy for Disasters and Accidents
- o Strengthening the network within the academic sector and among business, academic sector, NGO-s and governmental institutions
- o Participation at the Technology Watch project under FP7, Security theme
- o Application of the Technology Watch taxonomy as a basis for a Bulgarian taxonomy of security technologies, systems and products
- o Special focus on young scientists dealing with security research. The PhD policy should be considered as one of the important elements of Bulgaria's security R&T programme

Bibliography

1. *2006 Annual Research & Technology Report: Defence Research for the German Armed Forces in the Process of Transformation* (Bonn: Federal Ministry of Defence, Division Rü IV, December 2006).

2. Defence S&T Strategy: Science and Technology for a Secure Canada (Ottawa: Department of National Defence, December 2006).

3. *Guide to Capability-Based Planning*, TR-JSA-TP3-2-2004 (The Technical Cooperation Program, Joint Systems and Analysis Group, Technical Panel 3, MORS Workshop, October 2004), <www.mors.org/meetings/cbp/read/TP-3_CBP.pdf>.

4. *Handbook on Long Term Defence Planning*, RTO Technical Report 69 (Paris: NATO Research and Technology Organization, April 2003), <www.rta.nato.int/Pubs/RDP.asp?RDP=RTO-TR-069>.

5. Joint DPA/DLO Technology Management Strategy, Summary Paper FBG /36/08 (July 2006).

6. *The Management of Defence Research and Technology*, Report by the Comptroller and Auditor General (London: National Audit Office, March 2004).

7. Todor Tagarev, "The Art of Shaping Defense Policy: Scope, Components, Relationships (but no Algorithms)," *Connections: The Quarterly Journal* 5:1 (Spring-Summer 2006): 15-34.