CAPABILITIES-BASED PLANNING FOR SECURITY SECTOR TRANSFORMATION

Todor TAGAREV

Abstract: Advanced approaches towards defense management, and the process of the ongoing force transformation in particular, rely to a great extent on Capabilities-Based Planning (CBP) to provide for robust response to a broad spectrum of threats and challenges. Our assumption is that CBP has considerable potential to enhance initiatives for security sector transformation. This paper outlines a planning framework, based on centralized planning and agency-based development of security sector capabilities. It links objectives, security ambitions, planning scenarios, tasks, required and affordable capabilities, and planning risks. The distribution of capabilities among security sector organizations accounts for their traditions, experience, and current roles, but focuses on cost effectiveness. The development of capabilities is subject to regular monitoring, assessment of gaps and risks, and coordinated decision making on corrective measures. Then, the paper presents possible levels of integration of the security sector. The conclusion is that coordinated capability development, with capabilities-based planning as its central feature, should be seen as the core process in security sector transformation.

Keywords: Scenario-based capability-oriented planning, comprehensive approach, cost-effectiveness, security sector reform, integration.

Introduction

The optimistic scenarios for world development after the end of the Cold war very quickly gave way to the dark effects of ethnic and tribal conflicts, religious extremism, climate change and rapid spread of contagious diseases. In a way, western societies today feel—and are—endangered by threats with much higher probability to materialize than the threat of nuclear annihilation during the Cold war. Terrorist attacks, hurricanes, major industrial accidents, proliferation of technologies, components and weapons of mass destruction, critical dependence of the functioning of society on infrastructure elements and other factors increase the level of insecurity. States are expected to protect societies against such ‘unconventional’ threats, but often find themselves in the trap of traditions, institutional culture, and bureaucratic fights. Countries with limited experience and capacity for security policy making and force planning find it especially difficult to escape this trap, being overwhelmed by the range of the threats, the speed of organizational and technological developments, and diverse requirements of international organizations and alliances they wish to join. Even countries with mature planning systems find it challenging to adapt, or transform, their security and defense establishments to the changing security environment.[1]

This essay looks at one particular aspect of security sector transformation, i.e. how to provide for an effective response to the spectrum of security challenges in a transparent and affordable manner. It is based on the assumption that capabilities-based planning (CBP)—a recent, but powerful approach to planning in defense—can bring substantial benefits if applied to the security sector as a whole. The essay presents a planning framework that links goals, strategy, security ambitions, planning scenarios, tasks, required and affordable capabilities, and planning risks. The framework assumes a degree of centralization in planning and agency-based development of security sector capabilities. Key is the step of distributing required capabilities among security sector organizations and the related allocation of resources. The respective decisions need to account for institutional traditions, experience, and current roles, but focus should be on cost effectiveness. Then, the development of capabilities is subject to regular monitoring, assessment of gaps and risks, and coordinated decision making on corrective measures. Finally, there are degrees of integration of the security sector and the introduction of security sector-wide CBP is powerful tool to increase both the degree of integration and the efficiency in spending public funds. The conclusion is that coordinated capability development, with CBP as its central feature, should be seen as the core process in transforming the security sector.

Framework for Planning and Developing the Capabilities of the Security Sector

In planning the capabilities of the national security sector, policy makers and planners need to define and to find a balance among four key components: objectives, strategy and respective distribution of roles among security and other organizations, means—or capabilities—to implement the strategy, and planning risks.[2]

The term "capability" is defined as

> *the capacity, provided by a set of resources and abilities, to achieve a measurable result in performing a task under specified conditions and to specific performance standards.*[3]

Therefore, in addition to the four main components, a more detailed "top-down" part of the planning process requires to define a set of plausible conditions (often design-

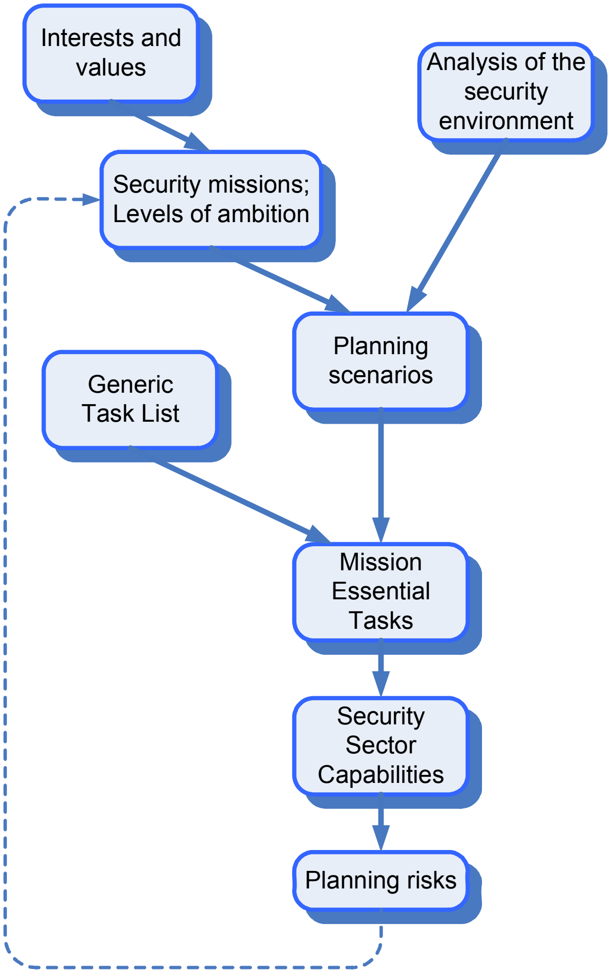
Interests and values
Analysis of the security environment
Security missions; Levels of ambition
Planning scenarios
Generic Task List
Mission Essential Tasks
Security Sector Capabilities
Planning risks

Figure 1: Conceptual Approach to Defining the Capabilities of the Security Sector.

nated as "planning scenarios"), as well as the set of tasks to be performed in these conditions. Thus, a rigorous planning process links:

- Objectives in the field of security, expressed in terms of missions and ambitions in guaranteeing security;
- Strategy for achieving the objectives;
- Roles of security sector organizations;
- Scenarios, describing plausible realization of risks and threats to national interests and security objectives;

- Essential tasks to be performed in neutralizing the plausible risks and threats (often extracted subset of structured catalogue of tasks, or 'generic task list'[4]);
- Capabilities required to perform the tasks;
- Ways to provide these capabilities (coordination of the development of the variety of capability components within a selected capability model);
- Estimates of planning risks.[5]

Relationships among components and the main feedback loop, intended to guarantee acceptability of planning risks, are presented graphically in Figure 1. Another feedback loop, not presented in Figure 1, serves to provide affordability of security ambitions and the respective capability levels.[6]

A more elaborated framework accounts also for the various horizons of the planning process, the possibility to act simultaneously to protect security interests across a number of scenarios, the centralized nature of capability planning and decentralized budgeting and execution of plans and programs, the distribution of decision-making authority for planning, implementation, and oversight, as well as a number of feedback loops. Figure 2 presents this framework with the assumption that a country applies program-based management of the resources for security or, equivalently, program-based development of the security sector organizations. Bulgaria, among others, applies such approach, with a particularly strong experience in program-based defense resource management. Other countries, e.g. The United Kingdom, use instead longer term—two to four years—budgets.

Of particular interest in this framework is the distribution of requisite capabilities among security sector organizations. Traditions and existing legal arrangements often drive the assignment of missions and tasks (and respectively – of capabilities) to organizations in the security sector. These are certainly important considerations; however, in the face of new security threats and the strife for efficiency there is a need for a broader rational and transparent framework that includes development and assessment of various cost-efficiency measures, e.g., specialization of security sector organizations in certain types of capabilities. As a start, there is a need to define lead and contributing organizations for each type of requisite capability and the sort of contribution each organization makes. Certain capabilities, i.e., management, command and control capabilities, do require interagency coordination and/or creation of centralized supra-agency bodies.

Thus, 'good governance' requirements, and cost-benefit analysis in particular, are expected to play an increasing role in making decisions on distribution of required capabilities.[7] The next section of the essay shows how capabilities-based planning al-

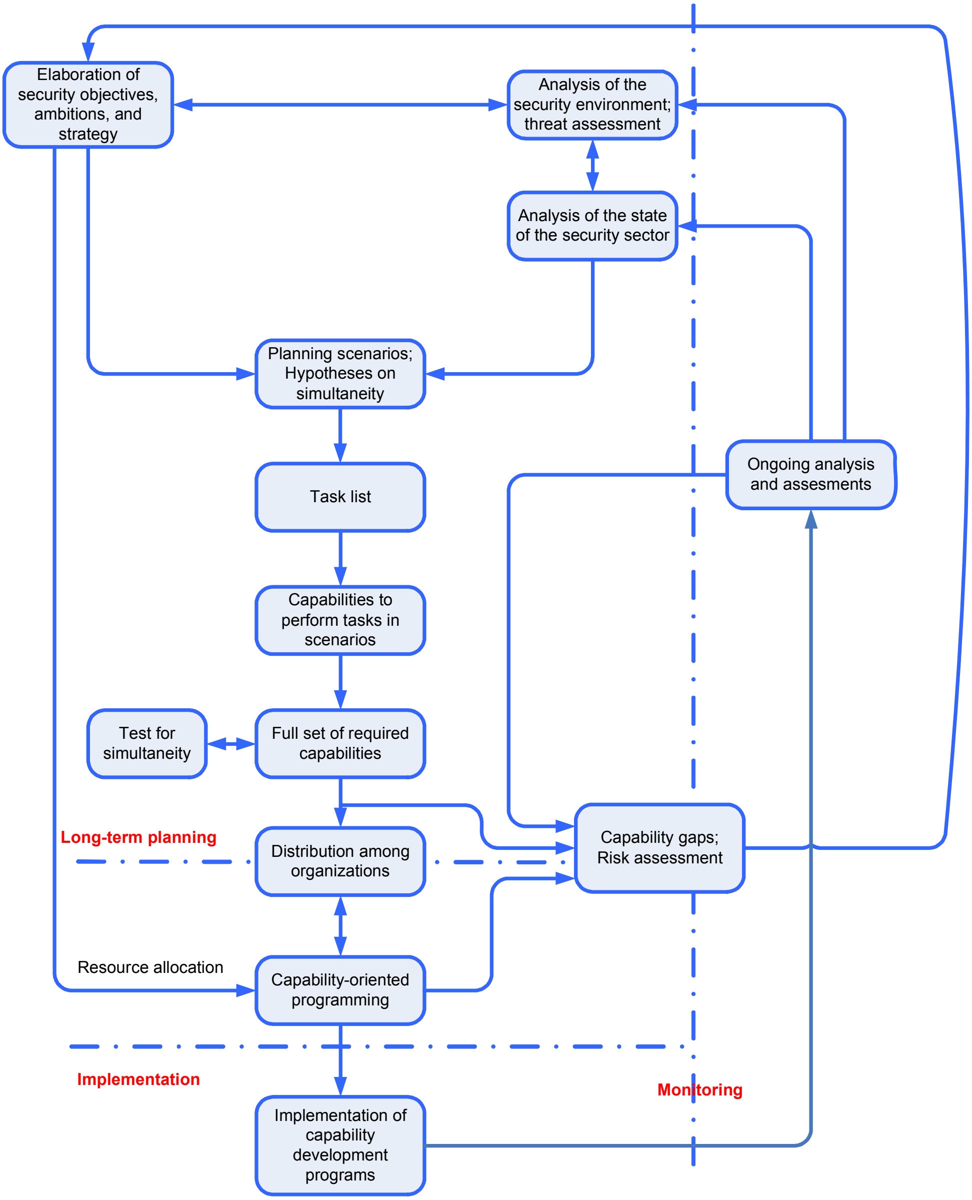
Elaboration of security objectives, ambitions, and strategy
Analysis of the security environment; threat assessment
Analysis of the state of the security sector
Planning scenarios; Hypotheses on simultaneity
Task list
Ongoing analysis and assesments
Capabilities to perform tasks in scenarios
Test for simultaneity
Full set of required capabilities
Long-term planning
Distribution among organizations
Capability gaps; Risk assessment
Resource allocation
Capability-oriented programming
Implementation
Monitoring
Implementation of capability development programs

Figure 2: Capabilities-based Planning for the Security Sector.

lows to permeate organizational boundaries and to seek higher levels of cost effectiveness.

What Makes the Security Sector a Distinct Whole?

In the first part of the essay, the term ‘security sector’ was used without an attempt to define it with any degree of precision. There is a growing literature on security sector reform, or transformation, but the terminology in use depends on the main purpose, geographic focus, intended instruments, and country contexts.[8] Depending on the main purpose, different international organizations focus on development (e.g., World Bank), security (e.g., NATO) or democratic governance (e.g., Council of Europe).[9]

Our approach combines ‘security’ and ‘good governance’ perspectives. While democratic oversight is indispensable, the driver is the efficient use of limited societal resources, in a transparent and accountable manner, to provide highest degree of security.

Also, there is no agreement on what constitutes the security sector. A recent document, presented to the UN Security Council,[10] adheres to the definition of the Development Assistance Committee (DAC) of the Organization for Economic Cooperation and Development (OECD) and includes in the security sector [11]:

Core security actors	Armed forces; police; gendarmeries; paramilitary forces; presidential guards, intelligence and security services (both military and civilian); coast guards; border guards; customs authorities; reserve or local security units (civil defence forces, national guards, militias)
Security management and oversight bodies	The Executive; national security advisory bodies; legislature and legislative select committees; ministries of defence, internal affairs, foreign affairs; customary and traditional authorities; financial management bodies (finance ministries, budget offices, financial audit and planning units); and civil society organisations (civil review boards and public complaints commissions)
Justice and law enforcement institutions	Judiciary; justice ministries; prisons; criminal investigation and prosecution services; human rights commissions and ombudsmen; customary and traditional justice systems

The presumption of this study is that any organization that brings ‘essential’ capabilities to deal with plausible security threats and challenges should be considered part of the security sector. Thus, in addition to core security actors we include public or private entities that provide required capabilities. An example would be a private security company that provides protection of a critical infrastructure asset, e.g., a nuclear power station.

The term 'sector' itself is vaguely defined. It means 'a distinctive part,' e.g. the organizations authorized to use force or organizations financed through the 'security and defense budget' of the state.

The alternative term 'system' is more appropriate to our discourse. It denotes something more than a list of organizations, distinct from other organizations. System is 'a set of entities, comprising a whole, where each component interacts with or is related to at least one other component and they all serve a common objective,'[12] 'a regularly interacting or interdependent group of items forming a unified whole.'[13]

Thus, while there is no broad-based agreement, but nevertheless there is clarity what makes the security sector *distinct*, less attention has been paid to what makes it a system. Our thesis is that it is possible to define an open system of interacting and interdependent organizations. However, the level of interaction and interdependence may differ greatly among countries and in time. It is possible to distinguish seven levels, presented in order of increasing interaction:

1. Rivalry and lack of will to work together; strict decision making stovepipes, meeting only at the level of Cabinet, Head of State, or Parliament; limited communication among security sector organizations;
2. Key personnel know each other; formal contact points are established; there is experience of (ad-hoc) cooperation;
3. There are instances of combined training and exercises; a level of trust among security sector organizations exists;
4. Deliberate and contingency operations planning processes are well coordinated; organizations and their units regularly train together; a lessons learned mechanism is also in place;
5. Centralized or very closely coordinated capabilities-based planning is institutionalized up to and including related budget allocation and understanding of planning risks;
6. Coordinated development of requisite capabilities through centralized or closely coordinated education, training, major procurements, development of infrastructure, shared operational concepts, etc.;
7. Integrated organization.

Most countries, Bulgaria included, are currently at a level of interaction between two and three. The framework presented in this paper calls for integration among security sector organizations at levels five and six. These are the levels that provide best opportunity to increase cost-efficiency and, thus, the level of security of modern societies.

Conclusion

Countries greatly differ in terms of interaction and interdependence of security sector organizations. There are countries that do not have military, as well as countries where the armed forces, by default, perform law enforcement functions. But these are extreme examples. Full integration, or level 7 of security sector organization, is not to be recommended for variety of reasons – too high concentration of power and diverse requirements towards organizational culture being among the important ones.

Levels of interaction 5 – 'Centralized or closely coordinated security sector wide capabilities-based planning,' and 6 – 'Coordinated development of capabilities,' however, are both possible and desirable. At these levels the processes of making security policy, planning, and allocation of resources to security become transparent to decision-makers in Parliament and in Cabinet. These are also the levels of integration that create best opportunities to limit redundancies, seek most effective solutions, and increase efficiency of public spending. Thus, coordinated capability development, with CBP as its central feature, has the potential to turn into the core process in transforming the security sector in highly efficient distributed organization, adequate to the security challenges of the Twenty First century.

Acknowledgement

This paper reflects research results of the project "From National to Societal Security: Scientific Support to Security Sector Transformation," sponsored by Bulgaria's National Science Fund at the Ministry of Education and Science under contract VU-MI-103/2005.

Notes:

[1] An example would be the enduring debate on the efficiency of the recently created Department of Homeland Security in the United States.

[2] This is an extension of the "Bartlett model" presented in Henry Bartlett, G. Paul Holman, and Timothy E. Somes, "The Art of Strategy and Force Planning," in *Strategy and Force Planning*, 4th ed. (Newport, R.I.: Naval War College Press, 2004), 17–33.

[3] Todor Tagarev, "The Art of Shaping Defense Policy: Scope, Components, Relationships (but no Algorithms)," *Connections: The Quarterly Journal* 5, no. 1 (Spring-Summer 2006): 15–34, <https://consortium.pims.org/the-art-of-shaping-defense-policy-scope-components-relationships-but-no-algorithms>.

[4] For a recent example see *Universal Task List*, Version 2.1 (Washington, D.C.: U.S. Department of Homeland Security, Office of State and Local Government Coordination and Preparedness, May 2005).

[5] The 2005 U.S. defense strategy refers to these risks as 'future challenges risk.' See *The National Defense Strategy of the United States of America* (Washington, D.C.: Department of Defense, March 2005), 11, <www.defenselink.mil/news/Mar2005/d20050318nds1.pdf>.

[6] For more information refer to Tagarev, "The Art of Shaping Defense Policy" and the references therein.

[7] On cost-benefit analysis with emphasis on public spending the reader may refer to Diana Fuguitt and Shanton J. Wilcox, *Cost-Benefit Analysis for Public Sector Decision Makers* (Westport, Connecticut: Quorum Books, 1999).

[8] David Law, "Who's Who Intergovernmentally in SSR?" in *Developing a Security Sector Reform (SSR) Concept for the United Nations* (Bratislava: Ministry of Foreign Affairs of the Slovak Republic and DCAF, July 2006), pp. 23–25, <www.dcaf.ch/unssr/security-sector-reform-concept-united-nations.pdf>.

[9] Ibid., 23.

[10] Security Sector Reform, *Security Council Update Report* 1 (14 February 2007), available at www.securitycouncilreport.org.

[11] Ibid., 3–4. For other definitions of the scope, depending of perspective (narrow or broader) and focus (state-centric or human-centric) see Heiner Hänggi, "Conceptualising Security Sector Reform and Reconstruction," in *Reform and Reconstruction of the Security Sector*, ed. Alan Bryden and Heiner Hänggi (Münster, LIT Verlag, 2004), 3–18, <www.dcaf.ch/_docs/bm_ssr_yearbook2004_1.pdf> (12 Apr. 2007).

[12] Modified from *Wikipedia*, <http://en.wikipedia.org/wiki/System>.

[13] *Webster's Ninth Collegiate Dictionary* (Springfield, Mass.: Merriam Webster, 1991).

TODOR TAGAREV is 'Strategic Management' Adviser to the Minister of Defense of Republic of Bulgaria and Head of the Centre for Security and Defense Management at the Bulgarian Academy of Sciences. He was the first Director of the Defense Planning Directorate since its establishment in early 1999. From May until late 2001, he served as Director for Armaments Policy in the Bulgarian Ministry of Defense and National Armaments Director. Among other duties, he coordinated all defense modernization and R&D programs in support of defense reform and NATO integration. From 2005 till 2008 he was Head of the Defense and Force Management Department of "G.S. Rakovski" Defense and Staff College in Sofia Bulgaria and member of NATO's Research and Technology Board. He graduated from the Bulgarian Air Force Academy in 1982 and received a PhD degree in systems and control from Zhukovsky Air Force Engineering Academy, Moscow, in 1989. Dr. Tagarev is a 1994 Distinguished Graduate of the US Air Command and Staff College at Maxwell Air Force Base, Ala. *E-mail:* tagarev@gmail.com.