CLASSIC, MODERN, AND POST-MODERN APPROACHES TO MAKING SECURITY STRATEGY

Todor Tagarev [1] and Petya Ivanova [2]

[1]*Centre for Security and Defence Management*
IPP - Bulgarian Academy of Sciences
e-mail: tagarev@bas.bg
[2] *Procon Ltd.*
e-mail: petya@procon.bg
Bulgaria

Abstract: In the recent past, security strategy has been oriented towards dealing with one or a few vital threats. The prevailing approach today—the 'modern approach'—is to develop a set of capabilities to meet a broad spectrum of security threats and challenges. The uncertainty and fluidity of the security environment, however, demand faster response to emerging threats, that can be provided only through a 'post-modern' approach to making security strategy – an approach focusing on flexibility and adaptiveness in the development of the security sector, and its interplay with other security instruments.
Key words: Security Sector Transformation, Uncertainty, Adaptiveness.

1. INTRODUCTION

Security strategy is the art and science of developing, applying, and coordinating the instruments of national power—diplomatic, economic, military, and others—to achieve national security objectives. It is often referred to as *national* security strategy or *grand strategy*. In the span of just a couple of decades scholars in the field of security studies, strategy and planning witness a momentous change in conceptual thinking and practical approaches towards

security strategy making. During the Cold war, the security strategies of many countries, in particular those in Europe and North America, were focused on the threat emanating from the opposing bloc. That focus by and far defined the complex of instruments of national power, as well as individual instruments, in particular major force structure parameters. Additional requirements were basically met through minor adjustments in the force structure. That approach— referred to here as 'classic' approach—is presented briefly in the next section of the paper.

With the end of the Cold war the defining nature of that threat to vital national interests was gone. The threat of state-organised military aggression against the territories of NATO and former Warsaw pact countries—even when still considered likely by policy makers and strategists—was turning to just one of many threats and challenges to be accounted for in strategy development. Respectively, strategy makers had to provide for a response to a spectrum of threats and challenges, often of similar importance. With time, capability-based planning emerged as the lead paradigm in defining the instruments of national power. Section 3 of the paper examines the respective 'modern' approach to strategy making.

Further we venture into the Twenty-first Century, more obvious it becomes that the complex interplay of evolving security threats and challenges, emerging technologies, and societal shifts make the environment for creating strategies uncertain and unpredictable in principle. And while state-of-the-art capability-based planning provides for dealing with some level of uncertainty, there is often a need to for flexibility and adaptability in the development of the security sector not witnessed before. Researchers have already presented early results of conceptualising this problem, as related to defence policy making and force planning (Nichiporuk, 2005; Tagarev and Ivanova, 2008). Main features of the respective approach to security strategy making, called here 'post-modern,' is examined in Section 4.

The concluding section enumerates the challenges of the transition to 'post-modern' strategy making.

2. CLASSIC APPROACH TO SECURITY STRATEGY

In the face of a considerable threat to vital national interests, security policy and strategy makers seek a combination of instruments of power that would effectively counter that threat. Authors often refer to this approach as 'threat-based' approach to strategy making (Handbook, 2003; Bartlett *et al.*, 2004). It involves identification of potential opponents and their capabilities, keeps the focus of strategists and planners on potential adversaries, provides a balance between the macro level of "balance of power" and the micro level of specific challenges, and requires rigorous assessment of capabilities in realistic scenarios (Bartlett *et al.*, 2004, p. 27).

In practice, the classic approach to strategy making combines threat-based planning with assessment of vulnerabilities to identified threats, proactive development of technologies and fielding of weapon systems, and account for resource constraints. The latter feature in particular necessitates to search for efficiency and is conducive to transparency and accountability of policy makers, strategists and planners to elected officials.

When resource constraints—and especially fiscal constraints—are not properly accounted for in strategy making, this approach may lead to strategies that are unsustainable. The collapse of the socialist bloc in the end of the 1980s and the dissolution of the Soviet Union soon afterwards serve as textbook examples in that respect.

Threat-based strategy making and planning are inherently reactive and dependent on quantitative data and trends that may be misleading. Furthermore, strategists do not always agree what constitutes a valid threat. Finally, the adaptation of threat-based strategies to sudden changes in the environment, as the experience after the end of the Cold war proves, may be notoriously difficult.

In the absence of a valid, prevalent threat, strategy makers turn to other concepts. One such concept is capability-based planning, that emerged in its contemporary form in the defence planning of Australia during the 1980s (Young, 2006). The following section presents briefly this approach, expanded beyond the scope of defence planning.

3. MODERN APPROACH TO MAKING SECURITY STRATEGY

The prevailing current approach to making security strategy—called in this paper 'modern' approach—is focused on the capabilities of the security sector to be developed and, when necessary, applied in coordination with diplomatic, economic, and informational instruments to protect national and/or allied interests and achieve security objectives. This approach involves two distinct steps:

1. Definition of the capabilities, required to perform a number of tasks in implementing an intended strategy, and

2. Distribution of the requirements among security sector organisations and design of procedures and organisational structures providing the required capabilities.

These two steps are iterated in a feedback loop until strategists and planners find an acceptable balance among security objectives, strategy, capabilities, and planning risks within anticipated resource constraints.

A rigorous strategy making and planning calls for an elaborate definition of objectives in the field of security, often expressed in terms of missions and ambitions in guaranteeing security; design and selection of scenarios, describing plausible realisation of risks and threats to national interests and security objectives; and definition of essential tasks to be performed in neutralizing the plausible risks and threats, often extracted as a subset of structured catalogue of tasks, or 'generic task list' (Canton, 2007). Then required capabilities are defined *vis a vis* the tasks to be performed under conditions specified in the planning scenarios. The process, with some simplifications, is presented on Figure 1 (Tagarev, 2009), where the feedback loop is used to find a strategy and the respective set of instruments, including security sector capabilities, that are affordable and acceptable to decision makers.

In practice, more elaborated frameworks account for various horizons of the planning process, hypotheses for the need to act simultaneously across a number of planning scenarios, the centralised, 'top-down' nature of capability planning and decentralised budgeting and execution of sectoral strategies, plans and programs. Of critical importance for the elaboration of the strategy making approach is the level of coordination among security sector organisations. An

earlier work of the authors (Tagarev, 2009) distinguishes seven levels of interaction, presented in an order of increasing coordination:

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 organisations;

2. Formal points of contact among security sector organisations are established; there is experience of ad-hoc cooperation; key personnel of security sector organisations know each other;

3. There are instances of combined training and exercises and a level of trust among security sector organisations;

4. Deliberate and contingency operations planning processes are well coordinated; organisations and their units regularly train together; a common 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. The development of requisite capabilities is coordinated through centralised or well synchronized education, training, management of major procurements, development of infrastructure, shared operational concepts, etc.;

7. Integrated organisation.

Theoretically, higher levels of cooperation create opportunities to examine comprehensively threats and potential responses in terms of strategy and capabilities and to seek solutions that are optimal in some sense (Tagarev *et al.*, 2008). Utmost efficiency from that theoretical perspective can be achieved when the decision making process is fully centralized. That rationale is strengthened by the emergence of new threats that cannot be assigned to existing security sector organisations but require instead very close coordination among two or more existing organisations. Likewise, there are novel strategies and operational concepts that also demand increased cooperation. For that reason most countries with mature strategy making and planning mechanisms move up the ladder of increasing cooperation (Rademaker, 2008), and some are in the process of integrating a considerable part of their security sectors.
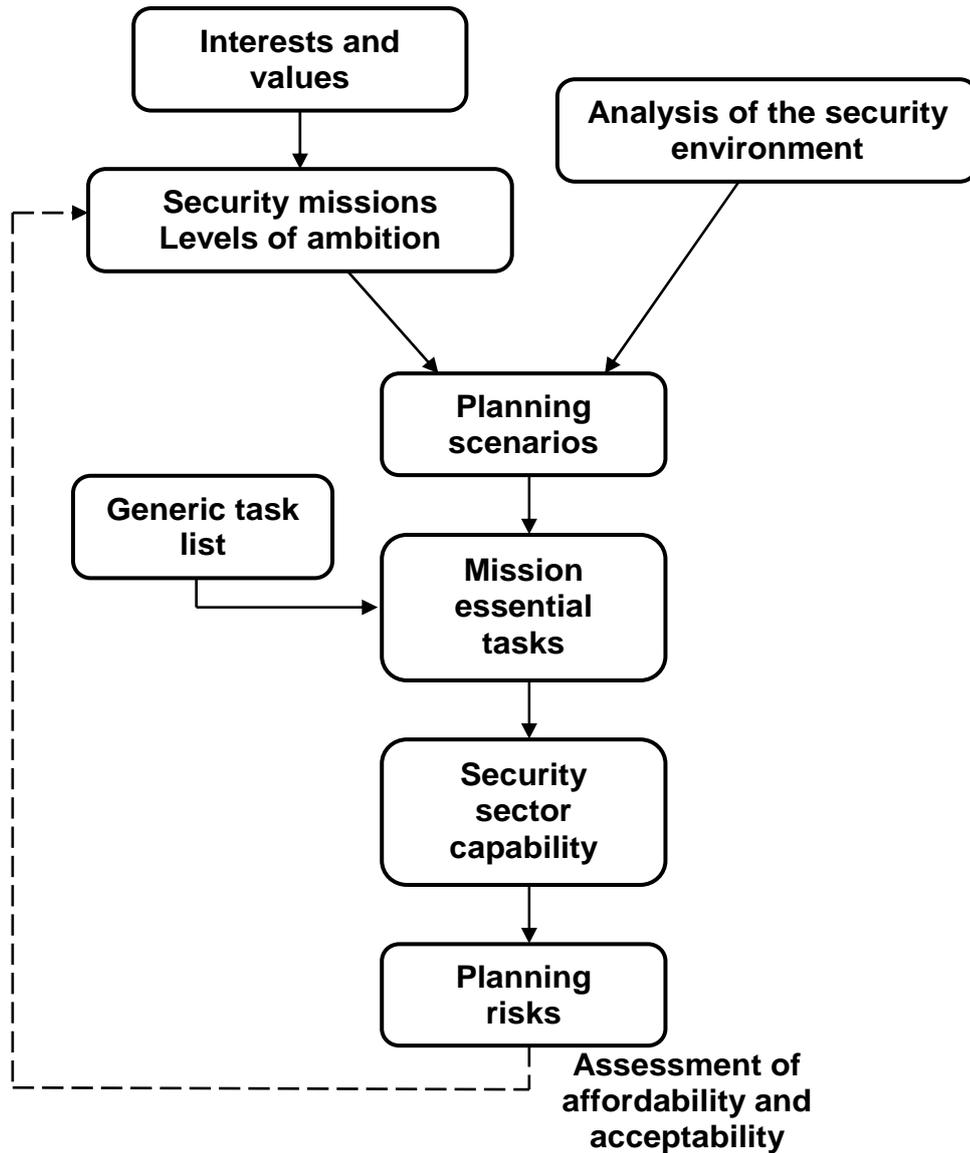
```
                    ┌─────────────────┐
                    │  Interests and  │
                    │     values      │
                    └─────────────────┘
                             │
                             ▼              ┌──────────────────────┐
    ┌ ─ ─ ─ ▶ ┌─────────────────────┐      │ Analysis of the security │
    ┊         │  Security missions  │      │     environment      │
    ┊         │  Levels of ambition │      └──────────────────────┘
    ┊         └─────────────────────┘              │
    ┊                    │                         ▼
    ┊                    └──────────┐    ┌─────────────────┐
    ┊                               ▼    │    Planning     │
    ┊                               │    │   scenarios     │
    ┊    ┌─────────────┐            └────└─────────────────┘
    ┊    │ Generic task│                       │
    ┊    │    list     │                       ▼
    ┊    └─────────────┘            ┌─────────────────┐
    ┊           │                   │    Mission      │
    ┊           └──────────────────▶│    essential    │
    ┊                               │    tasks        │
    ┊                               └─────────────────┘
    ┊                                       │
    ┊                                       ▼
    ┊                               ┌─────────────────┐
    ┊                               │    Security     │
    ┊                               │     sector      │
    ┊                               │   capability    │
    ┊                               └─────────────────┘
    ┊                                       │
    ┊                                       ▼
    ┊                               ┌─────────────────┐
    ┊                               │    Planning     │
    ┊                               │     risks       │
    ┊                               └─────────────────┘
    ┊                                                 Assessment of
    └ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─    affordability and
                                                      acceptability
```

Fig. 1. Iterative process of making strategy, with focus on security sector capabilities

4. POST-MODERN APPROACH TO MAKING SECURITY STRATEGY

Even though state-of-the-art capability-based planning provides solutions that are considered robust against some level of uncertainty in the environment and the trends in its evolution (The Technical Cooperation Program, 2004), resulting strategies consume most of the resources that might be made available to security. Furthermore, it is assumed that security objectives are well defined,

based on consensus, and stable (Jobbagy, 2007). Once strategy decisions are made, the respective capability and organisational development plans cannot be easily redirected. At the same time, practice teaches us that assumptions underlying strategy development, e.g. the ones related to key threats, economic trends, societal preferences and others, are bound to change well within the capability development horizon. For example, current strategy thinking is heavily oriented towards the threat of international terrorism, but seasoned analysts predict that the terrorist threat will not be among the major concerns by 2020 (Friedman, 2009).

Hence, strategy making must respond to a level of uncertainty higher than the one assumed in the 'modern' approach – uncertainty that is deep, massive and ubiquitous (Davis, 2007). Strategists must assume that a qualitative change will occur within their planning horizon. It may be caused by the emergence of a new threat, geostrategic shifts, shifts in the political and/or societal agendas, significant change in the economic environment, the emergence of a new technology with a disruptive impact, or another reason that cannot be anticipated. Such a qualitative change would likely make the strategy and the security sector organisation, designed under one set of scenarios and/or constraints, inadequate to the changed circumstances (Tagarev and Ivanova, 2008). Security strategists and planners must provide for adaptation of the strategy and the respective security capabilities to the changing environment, in due time.

The conceptual basis for responding to such level of uncertainty—called in this paper 'post-modern' approach to strategy making—is still in the making. It seems that this approach is bound to combine at least two strands of recent thinking on strategy. The first one envisions further elaboration of rigorous planning methodologies to accommodate for higher levels of uncertainty. It builds on state-of-the-art capability-based planning, which assumes however that the future is generally known, and reflects uncertainty through a set of planning situations, or scenarios, describing the realisation of likely threats or missions. Its 'post-modern' upgrade calls for examination of several qualitatively different, alternative futures (Nichiporuk, 2005), or context scenarios (Ratchev, 2008), and expansion of the notion of capability to incorporate strategic concepts such as 'shaping the environment' and adaptability (Tagarev and Ivanova, 2008).

In the first strand, strategy making is an inherently a top-down process, and scholars assume a decision making that is centralised to the extreme. The second strand also addresses the issues of uncertainty, ambiguity, and unpredictability, but from the bottom up. It is based on the understanding that living systems are complex, they adapt to changes in the environment and, at the same time co-evolve with other complementary and competing systems and change that environment in the process (Smith, 2006). Scholars admit that interactions in military, social, political, diplomatic, or economic spheres cannot be examined in separation, and draw insights from the theory of complex adaptive systems (Holland, 1995; Bar-Yam, 2005). Quick response to emerging challenges and opportunities is provided through agility of organisations and management processes (Atkinson and Moffat, 2005), delegation of resources and responsibilities, networking and self-organisation.

5. CONCLUSION

In less than twenty years the conceptual basis for strategy making made the transition from threat-based to capability-based planning and now shifts to a new, still emerging approach, referred to as 'post-modern.' The informed reader may find the use of the terms 'classic,' 'modern,' and 'post-modern' to identify respective approaches questionable. It is not questionable, however, that scholars and strategy makers need to explore and implement novel ways to deal with the challenges of complex dynamics, uncertainty and unpredictability.

This paper distinguishes two different venues of exploration – one focusing on a rigorous top-down and centralised decision making process, and the other – on local responsibility and initiative, networking and self-organisation. Most likely, applicable 'post-modern' strategy making will combine features of the two approaches, e.g. focus on agility both as a core competency in operations and as a value metric for policy and investment decisions (Alberts, 2005).

Whatever the final shape of such approach, its application will demand a level of transparency, distribution of decision-making authority, understanding and acceptance of ownership and responsibility uncommon for the strategic cultures in many countries. The importance of these requirements cannot be overestimated. The lack of the respective culture will be—and maybe already

is—a threat not only to the efficiency, but also to the effectiveness of security policy and strategy.

ACKNOWLEDGEMENT

REFERENCES

Alberts, D. (2005). Foreword. In: *The Agile Organization: From Informal Networks to Complex Effects and Agility*, S.R. Atkinson, J. Moffat, eds., p. xix. DOD CCRP Information Age Transformation Series, Washington, D.C.

Atkinson, S. R., J. Moffat (2005). *The Agile Organization: From Informal Networks to Complex Effects and Agility*. DoD Command and Control Research Program, Washington, D.C.

Bartlett, H. C., G.P. Holman, T.E. Somes (2004). The Art of Strategy and Force Planning. In: *Strategy and Force Planning*, 4th ed., 17-33. Naval War College Press, Newport, R.I.

Canton, L. G. (2007). *Emergency management: Concepts and Strategies for Effective Programs*. Wiley-Interscience, Hoboken, NJ.

Davis, P. K. (2007). *Lessons from Defense Planning and Analysis for Thinking About Systems of Systems*, WR-459-OSD. RAND Corporation, Santa Monica, CA.

Friedman, G. (2009). *The Next 100 Years, A Forecast For The Twenty-First Century*. Doubleday, New York, NY.

The Technical Cooperation Program, Joint Systems and Analysis Group, Technical Panel 3 (2004). *Guide to Capability-Based Planning*, TR-JSA-

TP3-2-2004. Available at www.mors.org/meetings/cbp/read/TP-3_CBP.pdf.

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

Nichiporuk, B. (2005). *Alternative Futures and Army Force Planning: Implications for the Future Force Era*. RAND Arroyo Center, Santa Monica, CA. Available at www.rand.org/pubs/monographs/2005/RAND_MG219.pdf.

Rademaker, J. G. M. (2008). From stove pipes to interagency policy and capabilities: The new Dutch security strategy. Presentation to the *Workshop on Development of the Security Sector of Bulgaria* (22 April 2008), Sofia.

Jobbagy, Z. (2007). Developing Strategy: On Effects-Based Operations, Complex Adaptive Systems, and the Importance of Biological Connotations. *Militaire Spectator*, 6 (**176**), 251-259. Available at http://hcss.nl/en/download/176/file/ MilitaireSpectator2007June.pdf.

Ratchev, V. (2008). Context Scenarios in Long-Term Defense Planning. *Information & Security: An International Journal* (**23**), 62-72. Available at http://infosec.procon.bg/v23/Ratchev.pdf.

Smith, E. A. (2006). *Complexity, Networking, and Effects-Based Approaches to Operations*. DoD Command and Control Research Program, Washington, D.C. Available at www.dodccrp.org/files/Smith_Complexity.pdf.

Tagarev, T. (2009). Capabilities-Based Planning for Security Sector Transformation. *Information & Security: An International Journal* (**24**), under print. Available at http://infosec.procon.bg.

Tagarev, T., P. Ivanova (2008). Expanded Capability Portfolios to Steer Force Development under Strategic Uncertainty. In: *Proceedings of the RTO SAS-072 Specialist Meeting on Capability-Based Long Term Planning* (Oslo, 18-19 November 2008), 5-1 – 5-10. NATO Research and Technology Agency, Paris.

Tagarev, T., Ts. Tsachev, N. Zhivkov (2008). Formalizing the Optimization Problem in Long-Term Capability Planning. *Information & Security: An International Journal* (**23**), 99-114. Available at http://infosec.procon.bg/v23/Tagarev_ Jivkov.pdf.

Young, T.-D. (2006). Capabilities-Based Defense Planning: Techniques Applicable to NATO and Partnership for Peace Countries. *Connections: The Quarterly Journal*, 1 (**5**), 35-54.

Bar-Yam, Y. (2005). *Making Things Work: Solving Complex Problems in a Complex World*. NECSI, Cambridge, MA.

Holland, J. H. (1995). *Hidden Order: How Adaptation Builds Complexity*. Helix, New York, NY.