PLANNING MEASURES AND CAPABILITIES FOR PROTECTION OF CRITICAL INFRASTRUCTURES

Todor TAGAREV and Nickolay PAVLOV

Abstract: The paper presents a framework methodology and process for planning and developing capabilities and measures for protection of critical infrastructure and presents major methodological and organizational challenges of effective and efficient protection. The authors emphasize the need for comprehensive approach, based on much better communication and greater coordination among governmental organizations, security services, owners and operators of critical infrastructure.

Keywords: Critical Infrastructure Protection, CIP, Capabilities-Based Planning, CBP, Security Sector Transformation, Counterterrorism, Comprehensive Approach.

Introduction

There is no need to look much back in time in order to recognize the threats for the normal functioning of societies, arising from deliberate attacks, malignant behavior, natural disasters or other kind of harmful impact on key elements of the infrastructure.[1] In their attempts to limit possible damage and enhance societal security, governments adhere to one or a specific mix of two main approaches:

- Formulation and application of rules, mandatory for critical infrastructure owners and operators;
- Provision of public funds in order to increase the protection of infrastructure elements.

In the first approach, the main responsibility for the normal functioning of infrastructure elements is transferred from the state to other entities, primarily private actors. In such cases, the companies will add to the price of their products the costs, arising from the fulfillment of security-related obligations. Thus, the infrastructure protection measures will be paid indirectly by the customer, e.g. the population. Another disadvantage of this approach relates to the process of globalization of businesses. If overregulated, the national economy may lose its competitive advantages

INFORMATION & SECURITY. An International Journal, Vol.22, 2007, 38-48.

and thus the business environment in the country may deteriorate considerably, leading at the extreme to bankrupts and unemployment.

In the second approach, central or local governments will carry the financial burden of measures to decrease the vulnerability of infrastructure elements. While enhancing security, such investment of public funds may have an unintended side effect in enhancing the competitiveness of particular companies.

While state authorities try to increase the security for the citizens, such effects might be unavoidable, but their impact should be clearly understood and limited to the extent possible. Therefore, for a state with a market economy and democratic governance, it is crucial to ensure due decision making procedures – a process which is transparent, rules are fair and the public is well informed on the relevant criteria. This process should be monitored by an independent body and subject to audits when necessary.

This article presents the main steps of such a process. First, it looks at how decision on the "criticality" of certain infrastructure element is made. Next, it presents a framework process for planning and developing capabilities and measures for protection of critical infrastructure. The final part presents major methodological and organizational challenges, emphasizing the necessity for much greater coordination among governmental organizations, security services, owners and operators of critical infrastructure. In the conclusion, the authors briefly address the applicability of the approach to other security-related issues.

Defining Criticality of Infrastructure Elements

According to Bulgaria's Law on Crisis Management, critical infrastructure is

> a set of assets, services and information systems, whose failure, impediment or destruction would have a grave and harmful impact on public health and safety, environment, national economy or the proper functioning of government.[2]

Though logical, this definition does not provide for a comparative evaluation of the criticality of a particular infrastructure element. It is not even sufficient to determine whether a particular asset, system or service can potentially be examined as "critical" or not. Therefore, the definition can not be very helpful in the process of identifying and analyzing the effectiveness of measures for protection of infrastructure. It can not be used for setting priorities either. Generally speaking, the current legislation does not provide a proper basis for reasonable distribution of public and private resources in order to enhance the security of critical infrastructures. The approach outlined in this article does provide such a basis. It also entails a model of decision making on public and private investment in security-related measures, thus enabling the achievement of highest possible impact within limited resources.

As member of the European Union (EU) since the beginning of 2007, Bulgaria looks at the respective EU regulations. A proposed EU Directive defines critical infrastructure as "those assets or parts thereof which are essential for the maintenance of critical societal functions, including the supply chain, health, safety, security, economic or social well-being of people."[3] It further delineates the critical infrastructure 'sectors' from the 2005 'Green Paper,' into eleven sectors:

- Energy;
- Nuclear Industry;
- Information and Communication Technologies;
- Water;
- Food;
- Health;
- Financial;
- Transport;
- Chemical Industry;
- Space;
- Research Facilities.

In the ongoing national and European debate on what type of infrastructure can be considered a candidate for "critical" and, thus, subject to public investment for higher degree of protection, our analysis [4] identifies three additional candidate types of "critical infrastructure:"

- Waste and Waste Management;
- Public Crisis Management Services and their key assets;
- National Symbols.

Shared understanding and decision on which are the 'sectors' of critical infrastructure is a necessary condition for the elaboration of a transparent process of defining the criticality of particular infrastructures and elements. Such process incorporates the following assessments:

1. Identification of the main sectors, sub-sectors and assets of critical infrastructure and determination of the most critical among them (*sector analysis*). Criticality is measured by the anticipated negative impact resulting from failure or impediment of an asset. The more severe the impact, the more 'critical' is the asset. Among the criteria for assessing the potential magnitude of an incident are its /a/ "public impact" (number of citizens affected: loss of life, injuries or illness that require long-term treatment, evacuation); /b/ economic impact (effect on GDP, economic loss, degradation of products and services);

/c/ environmental impact; and /d/ political and psychological impact, e.g., the confidence in the ability of government to cope with the incident. In addition, the time aspect of the impact should be accounted for, i.e., immediate, within one or two days, one week, over longer term.[5]

2. Identification, description (characterization) and evaluation of *threats* to the critical infrastructure. These threats can arise from deliberate attack, natural disaster or human error. In the course of threat assessment, we need to consider the capabilities of the possible intruders to carry out a successful attack, as well as their intentions, accounting for existing vulnerabilities of critical infrastructures. The exploitation of the vulnerabilities could aim at incurring damage to economy, defense or other aspects of national security.
3. *Vulnerability* assessment for the main sectors of critical infrastructure in respect to specific threats. Vulnerability can be defined as a weak point, exposed to malignant actions, performed in order to destroy or damage certain assets of critical infrastructure.
4. Assessment of *interdependencies* among subsystems and infrastructures, with focus on identifying those that potentially lead to cascading effects or other similar processes. Interdependencies may play a crucial role in decisions on measures to protect critical infrastructures, since often damage to one sector has a derivative, sometimes even more destructive impact on other sectors, dependent on the first one.
5. *Risk* assessment (the consequences to be expected of certain attacks against particular sectors, accounting for all types of negative impact: loss of human life, economic losses over time, etc.). The risk estimate is integral, i.e. across threats, and accounts for the likelihood of related incidents.

The results of these assessments are then used to identify and prioritize risk mitigation strategies and measures:

6. Elaboration of a critical infrastructure protection *strategy*. Normally, this would be a strategy for risk mitigation and risk management.
7. Elaboration of a set of *measures and capabilities* for critical infrastructure protection and risk mitigation in the framework of the strategy.

The activities in the course of analysis and planning of critical infrastructure protection (CIP) shall be performed step by step in the framework of an integrated process, as shown in Figure 1, which further involves a number of feedback loops.

CIP policy-making involves decisions on the scope of critical infrastructure, setting objectives, identifying and prioritizing measures, and allocating resources for

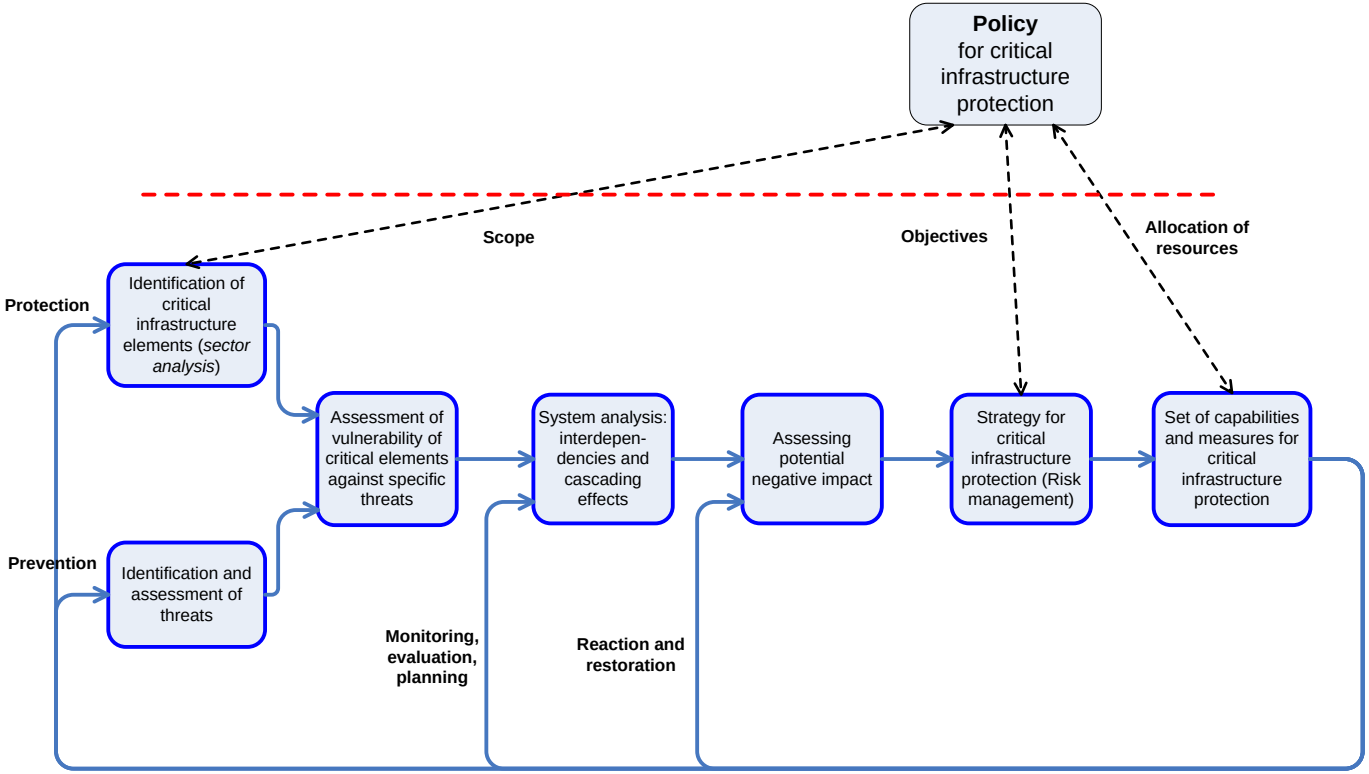

Figure 1: Critical Infrastructure Protection Process.

protection of critical infrastructure. Thus, it both informs the implementation of the seven steps outlined above and feeds on their results in an interactive manner.

Framework Process for Planning CIP Capabilities

In planning the capabilities for protection of critical infrastructure, policy makers and planners need to define and find a balance among four key components: goals, strategy and respective distribution of roles among variety of public and private organizations, means—or capabilities—to implement the strategy, and planning risks.[6]

The term "capability" here 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.[7]

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

- Objectives in the area of critical infrastructure protection;
- Ambitions in terms of the protection of critical infrastructures;
- Strategy for achieving the objectives and respective roles of public and private organizations engaged in CIP;
- Scenarios describing plausible risks and threats to critical infrastructures;
- Tasks to be performed in preventing and responding to the plausible risks and threats, and to manage the consequences of an incident;
- Measures and capabilities required to perform the tasks for protection of critical infrastructures;
- Ways to provide these capabilities (coordination of the development of the variety of capability components—human, materiel, training, etc.—within a selected capability model, often described through *programs*) within resource constraints.

The framework accounts also for the various horizons of the planning process, the possibility to act simultaneously for protection of critical infrastructures 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 output-oriented, e.g. program-based, management of the resources for protection

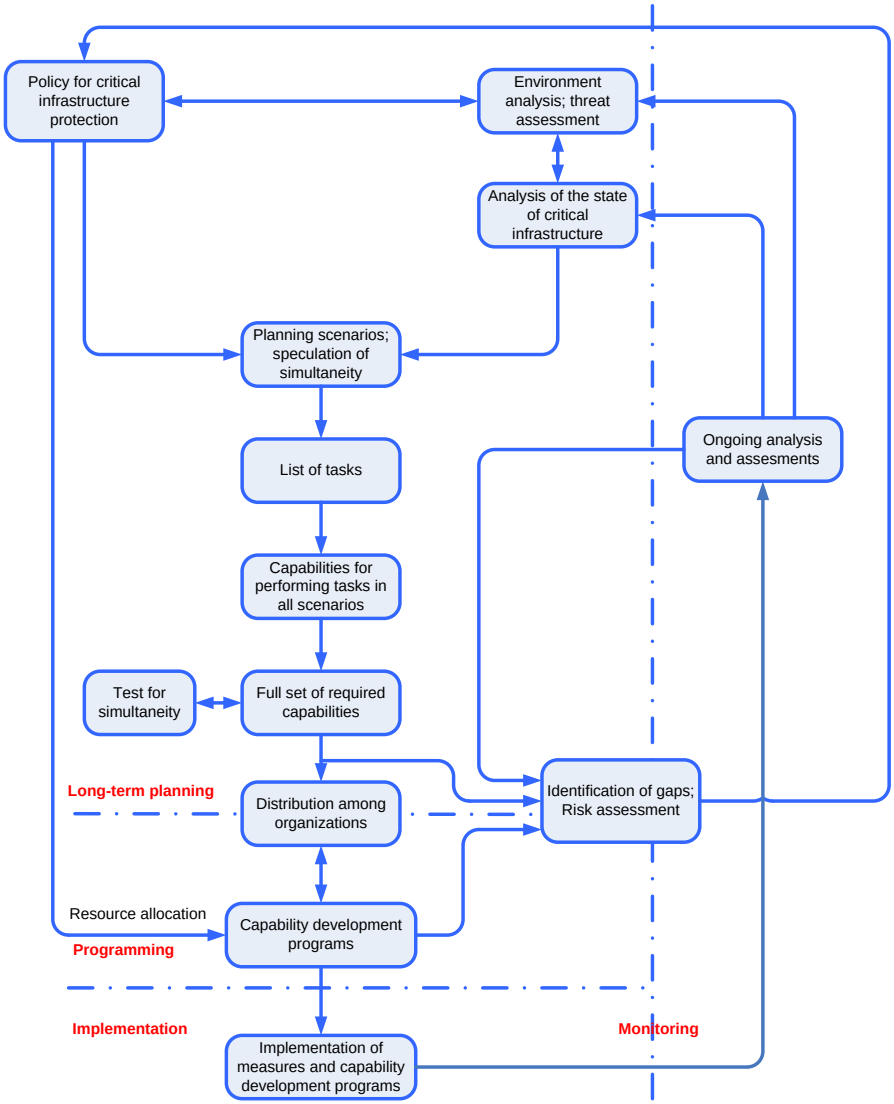

Figure 2: Planning and Development of Capabilities for Protection of Critical Infrastructure.

of critical infrastructures, and, equivalently, program-based implementation of measures and development of the respective capabilities.

Methodological and Organizational Challenges

Our expectation is that in the foreseeable future Bulgaria will develop and adopt an "official methodology" to guide the assessment of criticality of infrastructure assets, the planning of protective measures and capabilities and the respective allocation of public and private resources.[8] In all probability, it will be based on a risk management strategy.

This strategy will be implemented through a set of measures and capabilities for critical infrastructure protection. However, it is not recommended to create the respective plans and programs independently of other security-related requirements. Since a considerable number of the organizations, contributing to the protection of critical infrastructures, maintains a wide spectrum of capabilities, many of which are "multi-purpose," our recommendation is to set the CIP planning process in the context of "*protection of population and critical infrastructure against terrorist threats, natural disasters, industrial accidents and catastrophes*."

It is possible, but not advisable at this stage,[9] to use an even broader planning context, for example:

- CIP capability planning in the context of "protection of population and the *national economy* against terrorist attacks, natural disasters, industrial accidents and catastrophes"[10]
- CIP capability planning in the context of capability planning for the *national security sector* (which, in addition, needs to account for NATO and EU planning requirements).

From analytical point of view, in further development and implementation of methods, tools and analysis techniques, it is recommended:

1. To treat critical infrastructure as a complex adaptive system. All typical features of this type of systems are to be taken into account, including inherent uncertainty and rather limited predictability within such systems.
2. The most promising—and competing—methodologies for exploration of complex adaptive systems are based on the creation of two very different critical infrastructure models:
    - Architectural model (tools for structural and object-oriented modeling can be integrated in the course of its elaboration);
    - Agent-based model.
3. The implementation of these models shall be complemented by integration of expert assessments, for example in defining integral criteria, defining ob-

jectives and ambition levels (in the course of the development of a CIP policy), in generating and assessing alternative solutions, etc.

4. In certain cases, as expert estimates we can consider group decisions, i.e. the ones made by participants in computer-assisted exercises and simulations.
5. A broad variety of methods and approaches is available to support the performance of specific tasks. It is important, however, to integrate the latter in the overall planning framework for critical infrastructure protection.

From an organizational point of view, the key challenge is to break organizational stovepipes. Otherwise, the state administration will not be able to get the 'whole picture,' i.e. to assess interdependencies and, respectively, impact of infrastructure-related incidents, to seek cost-efficient distribution of CIP capabilities among the organizations involved, etc. That was one of the reasons for the recent creation of the Ministry of State Policy for Disasters and Accidents. At this stage though it is not clear whether the new Ministry breaks stovepipes or creates new ones.

Conclusion

The dependence of businesses, government and societal services on critical elements of the infrastructure creates vulnerabilities that can cause considerable losses in cases of malevolent behavior, human error, or extreme forces of nature. Societies are willing to pay a price to limit the vulnerabilities and, respectively, the losses, knowing at the same why and how much to invest in particular measures and capabilities for protection of critical infrastructure. That means *transparency* – clear rules and decisions on which assets are critical, what could be done to increase the robustness of these assets, which measures to implement within resource constraints, what would be the overall impact of one measure or another.

This paper outlines a methodological approach to assuring such transparency. With all methodological, procedural and analytical challenges in place, the major obstacle to effectiveness and efficiency is the culture of centralized decision-making within strict hierarchies that limits interagency coordination, and often even communication.

Being a relatively novel challenge that enjoys highest interest on the European Union agenda, the protection of critical infrastructure has the chance to turn into a 'Trojan horse' breaking organizational stovepipes, enhancing transparency of decision-making and accountability of central and local governments of Bulgaria—a newcomer to the European Union—and to provide a new, much higher level of coordination among governmental organizations, security services, owners and operators of critical infrastructure.

Utmost challenge in itself, the protection of critical infrastructure is just one of the 21st Century security challenges that require comprehensive approach, sound coordination among and, at times, integration of governmental agencies. Countering the terrorist threats and their origins, conducting stabilization operations, dealing with the consequences of pandemics, catastrophic terrorism, and major disasters are other missions that require such comprehensive approach. A methodology of the kind presented herein may contribute to finding effective and efficient solutions in the best interest of society.

Acknowledgement

This paper reflects results of two research projects: "Methodology for Modeling, Vulnerability Analysis and Risk Assessment of Critical Infrastructure," conducted by the Center for National Security and Defense Research at the Bulgarian Academy of Sciences in 2005, and "From National to Societal Security: Scientific Support to Security Sector Transformation," sponsored by Bulgaria's National Scientific Fund under contract VU-MI-103/2005.

Notes:

[1] See for example *Green Paper on a European Programme for Critical Infrastructure Protection* (COM(2005)576 final), (Brussels: Commission of the European Communities, 17 November 2005).

[2] *Law on Crisis Management*, State Gazette 19 (1 March 2005), amended State Gazette 102 (19 December 2006).

[3] Proposal for a Directive of the Council on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve their Protection, Commission proposal COM (2006) 787 final, December 2006.

[4] Greatly assisted by previous work of the ETH Center for Conflict Studies, published in Myriam Dunn and Victor Mauer, eds., *International Critical Information Infrastructure Protection Handbook 2006*, vol. I (Zurich: Center for Security Studies, 2006) and previous editions of the Handbook.

[5] See Dunn and Mauer, *International Critical Information Infrastructure Protection Handbook 2006*, p. 347.

[6] This composition is based on 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.

[7] 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>.

[8] In the spring of 2007 Bulgaria's Ministry of State Policy for Disasters and Accidents launched an ambitions project, part of which is to develop a methodology for assessment of critical infrastructure assets at municipal level.

[9] A comprehensive, tested methodology is not yet available, and planners would be easily overwhelmed by the complexities involved.

[10] This seems to be the current preference of law-makers and the executives in Bulgaria. See *Concept for Protection during Natural Disasters and Industrial Accidents* (Sofia, Ministry of State Policy for Disasters and Accidents, n.d.), available in Bulgarian at <www.mdpba.government.bg>.

TODOR TAGAREV is Head of the Defense and Force Management Department of "G.S. Rakovski" Defense and Staff College, Sofia, Bulgaria. 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 member of NATO Research and Technology Board and national representative at the RTO System Analysis and Studies panel. He has authored or co-authored six books and more than 50 papers published in refereed journals. His current research is focused on defense management processes and systems, process improvement, policies for and methodologies in support of security sector transformation. In these areas he currently leads three international research projects. Dr. Tagarev is Managing Editor of Information & Security: An International Journal, <http://infosec.procon.bg>, and member of the Editorial Board of Connections: The Quarterly Journal, <www.pfpconsortium.org>. *E-mail:* tagarev@gmail.com.

NIKOLAY PAVLOV (b.1976, Sofia, Bulgaria) holds a MA in International Relations and Security from Sofia University "St.Kliment Ohridski." He has been working at NGOs dealing with security research. Since 2005, he is Coordinator at the Center for National Security and Defense Research at the Bulgarian Academy of Sciences. In addition, since December 2006 he serves as Bulgaria's national contact person (NCP) for security research under EU Seventh Framework Programme. *E-mail:* nikolay_pavlov@abv.bg.