Journal scientific and applied research, vol. 3, 2013
Association Scientific and Applied Research
International Journal

Original Contribution

ISSN 1314-6289

RESEARCH OF THE OPPORTUNITIES FOR IMPLEMENETATION OF POLICES WHEN PLANNING THE POROTECTION OF CRITICAL INFRASTRUCTURE

Lyubomir I. Pashov

MUNICIPAL COUNCIL OF SHUMEN

ABSTRACT*: This work deals with the opportunities for implementation of policies when planning the protection of critical infrastructure in the framework of the national security system and the system for protection of the national sovereignty. A strategy is developed for the critical infrastructure protection at operational, regional and strategic level. A plan is outlined to address the relevant issues and requirements and set the activities and measures to protect the critical infrastructure.*

KEY WORDS*: critical infrastructure protection*

The policies used for planning of the critical infrastructure protection of a certain country clearly demonstrate the existence of a systematic approach. They usually follow a three-tier hierarchic model comprising national, regional and operational tiers (levels).

The geographical subdivision of the critical infrastructure is also used in the development of a protection system taking into account a number of factors, such as available security environment and possible terrorist threats. The protection system structure quite normally follows the critical infrastructure system structure, which is also hierarchic and three-tier and consist of three levels: national, regional and municipal (also called primary).

To be functional and reliable, such system will need the respective coordinators to manage and control the activities for protection system development and implementation, build the necessary intra-relations within the system as well as provide for the establishment of interrelations with other external systems.

The critical infrastructure protection system is developed and implemented by use of systematic approach within the scope of the national security system and the national sovereignty protection system, etc.[1]

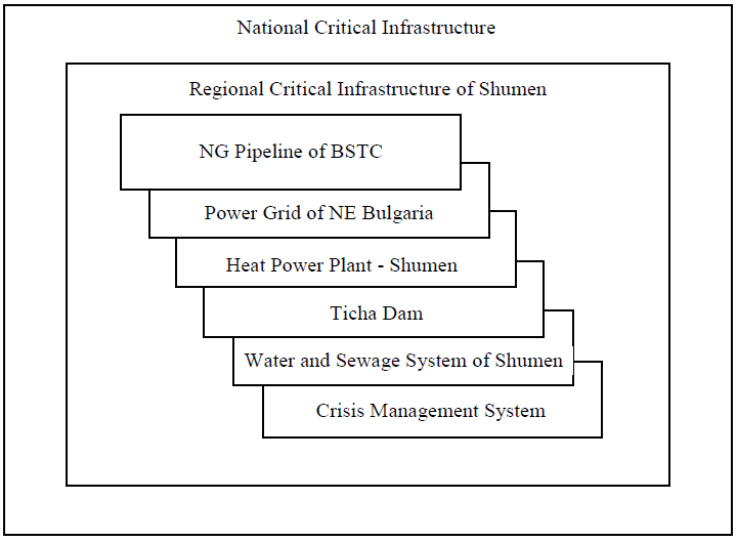

Figure 1 An Example for development of a critical infrastructure model for the Shumen Region

The system behavior will depend on the interactions among the separate components within the system structure. The feedback provides for the system stability and is carried out through the risk management at all three tiers: operational, regional and strategic. The system itself is established "from the bottom upwards".

The system functioning depends greatly on the information exchange

To be able to describe the system, we have to identify its levels:

1. Operational level. The system operation is performed at separate sectors which are further divided into their primary units. This allows performance of objective risk assessment and localization of the values of each risk category thus making them easily manageable in terms of planning and control. The accurate assessment at that level and processing. The used structure suggests that the information is communicated "from the bottom upwards". This facilitates the instructions giving process which takes place "from top downwards" and is based upon identification of all existing components at operational level, security risks assessment and planning. This ensures coordination of the risk management activities at all levels.

ensures preparation and undertaking of the correct measures to protect each component of the critical infrastructure.

The interactions at operational level are organized by the head of the respective administration or institution which operates the respective critical infrastructure component. It includes coordination of the available resources in terms of object, place, time and protection measures.

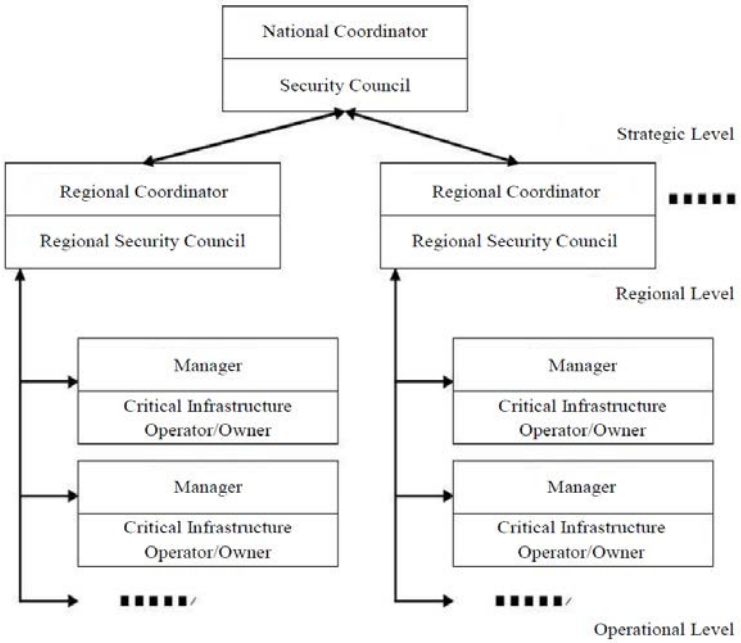

Figure 2 Critical Infrastructure Protection System

During the operative interactions, decisions are suggested and taken to mitigate the possible damages caused by an accident affecting the security, and subsequently actions are taken to restore the infrastructure's working capacity. As a result of the decision-making process a work plan is developed to protect the critical infrastructure component.

2. Regional level. At this level the critical infrastructure available in a specific region is subjected to risk assessment. A Regional Program for Critical Infrastructure Protection is developed and approved (the Municipal Program is approved by the respective Municipal Council). All systems and components comprising the critical infrastructure are entered into a Regional Register.

The interactions at regional level are organized by a specially appointed regional coordinator. They include coordination of the measures to protect the system components available or operating in a specific environment within the region boundaries in compliance with the approved Critical Infrastructure Protection Program and the developed Register of the Critical Infrastructure Components and Systems. Thus, the coordinator establishes the necessary connections among the separate infrastructure components to ensure their interaction. The interactions at regional level follow the interaction principles for management and mutual assistance of the actions intended to protect the critical infrastructure.

3. Strategic level. The risk assessments of the critical

infrastructure nationwide are summarized at the highest national (strategic) level. A National Program and Annual National Plans for protection of the critical infrastructure are developed on grounds of the data available in the critical infrastructure registers. At this level, the critical infrastructure protection system is composed in its entirety.

The interactions at national level are organized by a national coordinator. They include harmonization of the internal efforts to protect the critical infrastructure and coordination of the aid provided by other national security systems to ensure the critical infrastructure protection. At this level the protective measures and actions to be taken by the ministries and organizations involved in the provision of the national security are agreed. At strategic (national) level, the separate regional critical infrastructure systems establish connections with each other and with the national critical infrastructure system. Connections are built also between the national critical infrastructure system and the other systems ensuring the national security. Where necessary plans are developed to implement new approaches for protection of the critical infrastructure components subjected to an increased risk.

The system established in the above way provides feedback among all levels and ensures its reliability in general. Substantially, the feedback in all three levels of the critical infrastructure protection system is carried out periodically through risk assessments which cover certain periods of time. The risk assessment results are used for adjustment of the system to make it compliant with the existing environment and the selected strategy.

The system is directed towards protection of specific components against certain threats to achieve acceptable levels of the risks for these elements. Establishment of horizontal and vertical interconnections aims to maintain and coordinate the preventive actions and avoid omissions or repetition of functions or responsibilities.

The policies connected with the planning of critical infrastructure protection represent a recurring process which assesses the actions and measures to be taken with reference to the assets, or against the treats, vulnerabilities or the various categories of risk. The planning aims to define the actions for prevention of vulnerabilities and mitigation of risks.

The planning process results in development of a plan for protection of the critical infrastructure components at regional and national level. The plans should take into account and provide instructions, protective measures and actions to cope with the expected threats. Any such instructions shall be based upon the analysis of the former experience and further expanded, modified and integrated in such a way to adequately address and mitigate the modern threats. The instructions and measures shall be introduced via rules

of behavior and procedures for coordination the critical infrastructure protection.

Planning and coordination of the critical infrastructure protection shall be done simultaneously at all three system levels to achieve improved efficiency of the decision-taking process based upon the correct identification of the risks concerning a specific critical infrastructure component.

Based upon the risk assessment results and the devised risk management activities, an Action Plan is developed (Critical Infrastructure Protection Plan, National Program and Annual Action Plans for Protection of the Critical Infrastructure).

An action plan contents will depend on the level concerned. To harmonize the plans at all levels, they have to address the following general matters and requirements to be able to facilitate the adequate management and control of the activities connected with the critical infrastructure protection:

1. Getting acquainted with the situation:

- Threat analysis and expected occurrence;
- Type and location of the critical infrastructure components which are taken from the Critical Infrastructure Register.
- Objects and organizations located in close vicinity to the components of the critical infrastructure.

2. Organization of the critical infrastructure protection depending on the level of management:

- Development of a protection concept depending on the decision making level;
- Definition of the measures and resources depending on the critical infrastructure level;
- Dislocation of the measures and resources, definition of the scope of responsibilities, development of action plans for the different protection levels.

3. Provision of the means and resources necessary to maintain the critical infrastructure working capacity and ensure the workability of the protective measures.

4. Management. It includes the order of notification and reporting of the situation; the decision taking according to the action plan; the procedures to be followed and the security measures to be applied and consecutively, the actions to be taken.

By application of the critical infrastructure protection plan the specific conditions concerning the critical infrastructure are addressed.

For that purpose, the following measures and activities can be taken depending on the level of protection of the critical infrastructure:

1. Definition of the security zones. The plan may foresee various measures, procedures or actions for the different zones. These will depend

on the risk assessment, zones location and the interrelations between them.

2. Coordination of the measures introduced in zones with various specifications in terms of vulnerability and security.

3. Definition of the organizational structure at different levels which must ensure the critical infrastructure protection.

As a result of the analysis of the above basic parameters, it is recommendable the protection plan for the single components of the critical infrastructure to define the interactions between the separate structures and their scope of responsibility in compliance with the legislative requirements for the specific institution. The plan should specify the interaction mechanisms between the separate authorities involved in the access control, including building of data links between the information and security systems of these authorities to provide complete check-up prior to granting of access. The critical infrastructure protection plan should be accompanied by an action plan to be activated in case of accidents The action plan should contain different scenarios based upon the results from the risk assessment analysis and should stipulate the actions to be taken by the various resources in case of an accident. It should also define the recovery measures which will be needed to restore the critical infrastructure component's normal operation.

In conclusion we should note that the policies for critical infrastructure protection planning should be compliant with the requirements of the complex systems theory and the management theory. The correct application of the policies must provide for the establishment of an effective protection system through optimal use of the protective means and mechanisms of the government, the critical infrastructure owners and operators organized in a complex system at one hand and the application of the Crisis Management Act requirements on the other, which regulate the horizontal and vertical interactions of the governmental authorities (with their central and local structures).

References:

[1] Mednikarov D., Dimitrov N., Second Scientific and Practical Conference on the Emergency Management and Civil Protection – Approaches in Planning of the Maritime Critical Infrastructure, Sofia, Bulgarian Academy of Science, 2007.