

APPLYING THE SYSTEM APPROACH TO THE STUDY OF CRITICAL INFRASTRUCTURE

Boyan MEDNIKAROV, Nedko DIMITROV, and Kalin KALINOV

Abstract: Nowadays, in conditions of transformation in the maritime sector of the country, associated with changes of possession forms, establishment of new economic rules and overcoming the difficulties encountered in any period of changes, new types of relations for coordination of activities in the maritime domain are determined. They are established using a new type of civil-military cooperation in protection of the sea interests of the state, as well as in guaranteeing maritime security. The maritime critical infrastructure protection system is an instrument for adapting these relations to neutralization of modern threats, as well as for minimizing the damage effects during crises. This article proposes a register of the Bulgarian maritime critical infrastructure, which is elaborated taking into consideration principles from the modern civil security concept and the experience of leading nations in the area of maritime security.

Keywords: Maritime critical infrastructure, maritime security, maritime sector transformation, maritime critical infrastructure protection.

Being a sea state, Bulgaria endeavors to bind its national strategy to the sea spaces of the region, which, on one hand, holds substantial resources, but on the other hand is a constant generator of contradictions, which are most likely to cause future conflicts and crises. The following factors define the significance of the problem:

- Globalization of risks and threats resulting from or related to the sea – nowadays, the diversity of risks and threats is wider, they are more abstract, and the originators are no longer military units/ forces with predictable tactics and consistency in the pursuit of goals;
- The scope of threats has exceeded the armed forces framework – the risk targets ceased to be military ones only; more and more they address civilians and involve large groups of people with substantial social and cultural potential;

- Difficult control of the relationships between ethnic groups, difficulty in supporting ethnic peace, unresolved critical problems and presence of “frozen conflicts,” causing political instability in the region;
- The need for consistency in the maritime policy of the country through declaring, becoming aware of, and defending the national goals related to sea;
- Enhancing the role of Civil-Military Cooperation (CIMIC) relationships to fully employ the maritime power of the country;
- The need for adequate management of the maritime affairs of the country and establishment of an efficient national system for control in the maritime domain.

Bulgaria is facing new threats, which are more diverse, less visible, and less predictable. In particular, terrorism poses a growing strategic threat to the whole of Europe. Increasingly, terrorist movements are well-resourced, connected by electronic networks, and are willing to use unlimited violence to cause massive casualties.

In the maritime environment, illicit and violent activities, including drug trafficking, transporting of illegal immigrants and terrorism, are on the increase. The significant development of economic activity in the Bulgarian coastal waters also requires a higher risk control, and control over the risks to the environment in particular. Cargo and passenger ships need to get to their intended destination safely and on schedule. Ships in distress need to be found quickly and assisted. Commercial and naval ports need protection from terrorist attacks. Ships at sea need situational awareness of airborne, surface, and undersea threats.

Terrorist attack capabilities are using a variety of platforms, including explosives-laden suicide boats and light aircraft, merchant and cruise ships as kinetic weapons to ram another vessel, warship, port facility, or offshore platform, commercial vessels as launch platforms for missile attacks, underwater swimmers to infiltrate ports, and unmanned underwater explosive delivery vehicles. Mines are also an effective weapon because they are low-cost, readily available, easily deployed, difficult to counter, and require minimum training. Terrorists can also take advantage of a vessel's legitimate cargo, such as chemicals, petroleum, or liquefied natural gas, as explosive component of an attack. Vessels can be used to transport powerful conventional explosives or weapons of mass destruction for detonation in a port or alongside an offshore facility.

In this permanently more active, globalizing world of information technologies, intensive exchange of commodities, stocks, people, and traditionally more open societies, changes in thinking are necessary in terms of approaches and concepts that will

allow us to preserve our values and achievements by effectively reacting to the threats. This calls for transformation of our resources and capabilities that will permit us to react adequately to the new challenges.

As in other countries, the Bulgarian national security system undergoes deep transformation. The basis of transformation procedures has been formed by several new security concepts, such as the concept of homeland security, citizen security, civil and societal security. In Bulgaria, this new approach to security has commonly and increasingly been referred to by the term “civil security.” This term carries the impression of a newer, longer-range approach to security that goes beyond the traditional concepts of state security and national security.

Civil security does not revoke national security, but complements it and expands its scope in terms of aims to achieve a higher degree of security for the individual citizen. Building the civil security system of Bulgaria attempts to fill the gap between the system of national security and the system of population and infrastructure protection in the context of an integrated security sector.

Building a modern civil security system, the following principles should be respected:

- *Decentralization.* The importance of the regional components (controlled by the regional authority) of civil security is essential. They are expected to react first to the emerging threats to citizens and infrastructure.
- *Critical Infrastructure Protection.* Special attention should be paid to the protection of critical infrastructure because it is an important new component of the civil security system. In Bulgaria, a scientific study was conducted on the issues of critical infrastructure protection, but there is still lack of an officially tested and accepted methodology for evaluation of critical infrastructure, as well as a register of the national critical infrastructure.
- *Enhanced Involvement of the Citizens.* In the American and various European civil security models, the citizens play central role in providing civil (public) security. Civil security is specified as a general term for the efforts to cope with the new security threats to society. The civil security policy is determined by mobilization of all public sectors with the goal of security protection.
- *Recognition of the Problems Associated with Migration.* Illegal migration became one of the most serious security threats on national, regional, and international level in the beginning of 21st century.

In this article, one of the main principles of civil security—the protection of critical infrastructure—will be analyzed in detail.

As a concept, the maritime critical infrastructure is determined as a critical infrastructure exploited in the maritime domain. The maritime domain includes all zones and elements from, over, under, relevant to, attached to, or bordering the sea, the ocean or others, provide for navigation, including all sea related activities and the respective infrastructure, people, cargo, ships, and other transportation means. The studies performed already and the experience of leading nations in the area of security identify the following main components of the maritime critical infrastructure ¹:

- Ports (as part of national transportation plan);
- Roads (littoral and sea) and bridges;
- Energy sources and energy transfer means, coastally placed (electricity, gas, petrol);
- Infrastructure related to dangerous substances (chemical, biological, explosive) – terminals, pipes, carriers, manufactories;
- Critical infrastructure designed for emergency situations:
 - Emergency assistance (search and rescue, law enforcement);
 - Safety of shipping and economic activities.

If we assume that the critical infrastructure and its protection could be described as a complex system, it could be expected that the result would be an improved critical infrastructure protection system based on the principles of complex systems theory. Using system structural methods, one can achieve deduction, verification, and integration of the results reached by analytical methods and models, and shaped by broader hypotheses. During development, the system structural approach is crucial for obtaining knowledge about the systems, their structural details, relations, and interactions. Thus, system self-regulation features can be used, their self-organization respectively, achieved during system transition from one to another stable state. Furthermore, the stochastic system is a useful concept, located between chaos and organized state of the systems (when a system attains a particular type of frequency function, it can be viewed as deterministic instead of stochastic). That may happen also by aggregation of components of the considered system.

A system is a group or combination of interrelated, interdependent, or interacting elements (physical, behavioral, or symbolic entities) that form a collective entity. The characteristics of the systems are:

- Existence of links and relationships between system components.
- Tight link with the environment. The interdependence between the system and the environment explains system's "integrated whole."

- Each system can be viewed as a component of a higher level system, while its components can be systems from a lower level class. Or, every system is composed of subsystems nested within larger systems.
- System behavior is directed towards achieving the determined goal.
- The systems are able to change their organization and structure during operation (functioning).
- Individual components of the system determine certain aspects of its behavior, while the complete operation is a consequence of the interaction of all components.

If the entire maritime critical infrastructure of the country is analyzed, it is not difficult to prove that it represents a complex system, considering the following facts:

A. Analyzing the data about the elements of the sea transportation system, the maritime infrastructure associated with outputting and transferring energy and dangerous goods, the system of crisis management and the supporting activities related to safety of shipping, military and civil security, the following critical infrastructure components are identified:

- A1. Ports “Varna–East,” “Varna–West,” “Bourgas–East,” “Bourgas–West;” terminals “Nephtochim–Bourgas,” “Kraymorie;” petrol terminal of port “Varna,” power plant “Varna,” military/ border police ports Varna and Bourgas.
- A2. Transport arteries: bridge “Asparuchov,” sea area and approaches to Varna and Burgas ports;
- A3. Control system of the NAVY, Border Police, and Maritime Administration.

In general, these components form a list (a register) of the maritime critical infrastructure of the country. The following relationships exist between these critical elements:

- According to *geographical location*. The critical components of a physical type can be combined in two groups: those placed in the Varna region and those located in the Bourgas region. The items inside each group are connected and related through the integrity with the maritime domain as well and within the neighborhood (to a different extent) of the location of the critical elements. These links and interrelations form two subsystems of the system “maritime critical infrastructure” that can be explained with conditional system integration (“organized whole”) and can be named “Varna” and “Bourgas.”

- According to *crisis management*. The management systems of the three departments—NAVY, Border Police, and Maritime Administration—are subsystems of the national crisis management system due to the fact that these three departments are the three main pillars that guarantee the maritime security of the country. Furthermore, security in the current environment can be guaranteed only by a good coordination of planning as well as interaction during management in the national maritime domain. This interaction is already a fact, confirmed by the signed interdepartmental documents.

B. Each of the systems described above can be viewed as a component of a higher level system, such as the national critical infrastructure system and correspondingly the national critical infrastructure protection system, the maritime (air) sovereignty protection system, the crises response system, etc. At the same time, the systems “Varna” and “Bourgas” include elements that can be arranged as lower level systems. For example, each seaport or a separate management (command) system can be viewed as an independent system due to the existence of organized aggregation of related as well as functionally-related entities and courses that form a complex unity.

C. The defined systems “Varna” and “Bourgas” exist in a specific environment (physical, public, national, risky), characterized by common nature; that means similar potential outside and inside influences. In these consistent conditions, the behavior of the systems is obviously deterministic and predictable, too. It is directed towards the protection of the physical integrity (wholeness) and normal functioning of the elements, despite changes in environmental conditions. That means that the systems are goal-oriented and their functioning is directed towards the achievement of system’s goal(s).

D. The systems “Varna” and “Bourgas” are in a position to change their organization and structure during operation. Risk studies (performed on a periodical basis or after a security incident) provide the ground for initiating changes of system organization and/or structure in order to improve its functionality. System organization could be changed also during real operation. For example, when certain threats appear, extra security measures can be initiated.

All these facts confirm that the critical infrastructure and respectively its protection can be described as a complex system (see Figure 1).

The system described here as a complex system is an open system. It is characterized by:

- “Integrated Whole” – as a result of the links and relationships between system components.

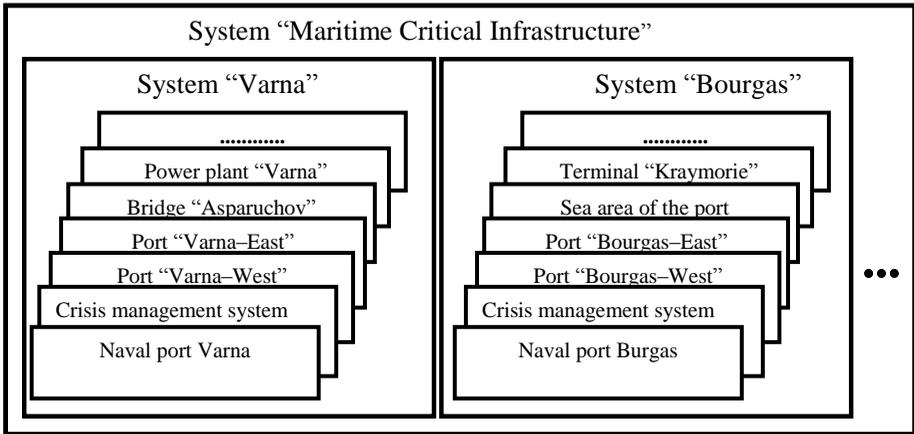


Figure 1: Illustration of the Maritime Critical Infrastructure System.

- Behavior of the system. It shows how the state of the set of system variables on the input is transformed to a new state on the output. A crucial role here plays the change of system structure, more precisely – the network of feed-forward and feedback connections between the elements of the system.
- Mode of operation of the system. It determines the control of its progress.
- Feedback loops. They determine the stability of the system through balancing the difference between its old and new state (having an offset character).

The feedback loops play the role of means for self-regulation of the system during its transition to a new stable state.

The processes of development—the transition to a new stable state of the system—are possible in a deterministic framework, dependent on system productivity. For the system "Varna" and "Bourgas," these boundaries can be determined by the change of security level of the components (from the register of the maritime critical infrastructure) as well; more precisely, from the difference between existing and surplus security in a spatial-temporal framework. The outlined basic characteristics of these open systems determine their non-stationary character and a development connected with synergistic, multiplicative, and acceleratory consequences that are results from the change of the network of links and interactions between system elements.

The increased productivity of the system designates its stability in time, respectively the rate of change from one to another dynamic state. This process depends on the intensification or loss of offsetting feedback connections. These characteristics of systems development are determined by:

- Changes in the quantitative ratios of the elements – as a result of their qualitative productive changes;
- Variety of functional role of individual elements at various stages of development.

The resulting expression for accumulation of system productivity, as a result of structural changes, is determined by the changing level of security between the individual critical infrastructure sectors.

In the context of these fundamental characteristics of open (complex) systems, this means to apply adequate model instruments in terms of use of the system structural approach for elaboration of the strategies for critical infrastructure system development.

The required legal basis that sets the policy and strategy for national critical infrastructure protection has already been provided by the national legislation. According to the Law on Crises Management it is required to approve and accomplish a “National Plan for Critical Infrastructure Protection,” “Annual National Plan of Action for Critical Infrastructure Protection,” as well as ministries’ and departmental plans for protection of the critical infrastructure.² This requirement can be performed only when:

- The owners and operators of critical infrastructure (in the private and public sectors) determine the specific elements that can be assumed “critical” in national dimension;
- These items are assessed in terms of vulnerability to potential hazards, which the country may face, in order to determine their level of risk;
- Measures for reducing risk are chosen when necessary.

In order to be able to conduct and manage this process, it is necessary to perform research where applied scientific methods would reveal relations, interdependencies, the nature of events, and possibilities for control. Considering the structure of the system “National Critical Infrastructure” (see Figure 1), analysis and respectively risk management of the system have to be performed at three levels – operational, regional, and strategic.

Operational Level

That is the level of the individual elements of a critical infrastructure system. Decomposing the system into separate sectors, and further into their constituents, permits detailed and precise risk assessment. Decreasing the size of each assessment makes it easier than in planning and execution. Limiting the number of required estimations by means of segmenting into separate objects allows partition of the entire maritime

critical infrastructure system into individual sections, belonging to individual organizations and departments. So, if each organization conducts risk assessment for the exploited critical infrastructure that would limit the number of individual estimations and thus facilitate the process in general. Furthermore, the responsibilities of the organizations will be realized.

With this objective, a scientific method for risk management adapted to the specifics of security of maritime critical infrastructure has been developed. The general hypotheses of risk management,³ such as the main phases of critical infrastructure assessment procedure,⁴ the critical factors for success in risk management of activities in military⁵ and civil (ISPS-code, petroleum, fiscal and computer Companies)⁶ domains, are taken into consideration in method development.

The method for risk management of the maritime critical infrastructure has been used in a study conducted in the Bulgarian Navy, taking advantage of the available knowledge and expertise of Navy's experts in all areas related to analysis of infrastructure and threats related to its security. The object of this study has been the maritime infrastructure of the country, Navy's infrastructure in particular, and the subject – the criticality and the capabilities for maritime critical infrastructure protection.

It is harder to achieve a high level of accuracy of assessment of the maritime critical infrastructure security risk in comparison with the other types of risks owing to the fact that the data for probabilities and costs associated with the risk factors for this type of security are limited and constantly varying as well. For example:

- Limited information about risk factors such as probability of realization of terrorist attacks in Bulgarian conditions; size of the damage, digression or violation of the normal work, exploitation of faults in the infrastructure security system;
- The risk factors are not easily foreseeable due to their realization probability in the different mediums—air, land, water—with different physical characteristics and properties. For example, the hydrology of the sea water changes in different seasons; the heterogeneity in the sea water produces jamming, that worsens surveillance conditions and facilitates the movement and penetration in security zones without necessary reaction;
- Part of the maritime critical infrastructure, including the sea routes, has a unique nature and properties as well as specific security requirements;
- Factors such as confidentiality of information and the need to disclose classified data cannot easily be quantified;

- Even the existing physical and information security systems and the organization of their use get older quickly due to the active development of technologies and advance of the devices used for access control.

The lack of up-to-date and reliable information causes often inaccurate evaluation of security risks and respectively, incorrect selection of relevant measures. Due to these limitations, models that by means of risk assessment achieve objectivity of analysis and effectiveness of solutions are used, such as the rational-analytic framework model. The model proposes to explore the entire aggregation of maritime critical infrastructure components and to use various optimization methods.

During this study, a register of the threats to the maritime critical infrastructure and a list of the entities of the maritime critical infrastructure of the NAVY were compiled. Based on these two documents, sixteen scenarios were developed. Each of them represented the impact of a concrete threat on a concrete entity. Further, by playing the scenarios, risk assessment for each one was performed. The risk was ranked using four-level grades. Two levels (level 3 and level 4) were acceptable and the other two (level 1 and level 2) – unacceptable. Measures for reducing risk were chosen for the scenarios with unacceptable risk.

Regional Level

It is required at this level to have:

- Integration of the risk assessments of the critical infrastructure according to a regional factor;
- A program for critical infrastructure protection developed for the area (municipality);
- An area register issued for the entities of the critical infrastructure.

Here is the place for application of a behavioral model for determining the effectiveness to the benefits from risk assessment. This model is based on the condition that the decision and respectively the action plan are a result of achieved compromise between the different departments and organizations having particular interests and responsibilities in the critical infrastructure protection process. The consensus is needed to assure a full vote of the decisions made and to guarantee the engagement that the plans will be realized.

Risk management at regional level is associated with a cyclic application of analysis and deduction methods. They are based on decomposition and aggregation. While the decomposition is typical for analysis at operational level, the aggregation is typical for regional level. It means that a few components of an object (a whole) are brought together. That whole is interpreted externally, in the framework of the environment, and internally – in the context of the structure and organization of the system. In the

aggregation process, the feature emergence can be witnessed, which is a new quality that could not have been observed only from the qualities of the involved elements, but would have been impossible without aggregation.

Aggregation plays the role of a system-built factor that determines the degree of internal connection and integration of the system. The result from emergence is the synergetic effect – qualitatively new capabilities of the systems as a whole. The synergy is based on the understanding that the whole is bigger than the sum of its parts. The synergy arises in a united system, where the integral effect is bigger than the differential.

At this level, relationships between the individual elements are established in order the interaction and constitutional effect to be guaranteed. These links are established on the basis of military (naval) tactic as well military (naval) art. A circle echelon-observation in order to achieve in-time detection of threats and their neutralization is established by means of the practices “a static secured zone” and “a circle zone of immediate defense.” Using the principles of interaction in control and mutual support in action contributes to achieving the goals of critical infrastructure protection at regional level (through sharing the existing capability of one department to protect critical infrastructure’s vulnerabilities of others).

Strategic Level

At the highest (strategic) level, where the risk assessments of the entire national critical infrastructure are integrated, a National Program and Annual National Plans of Action for Critical Infrastructure Protection are developed. At this level, running the behavioral model is performed on the critical infrastructure protection system at national level. The protection measures for the national critical infrastructure are agreed at this level, joining the efforts of the ministries and the departments guaranteeing national sovereignty.⁷ In this way, the relationships between the individual regional critical infrastructure protection systems (in the framework of the national critical infrastructure system) and the other systems related to national security are established. Also at this level, if a need arises, acquisition of new capabilities for critical infrastructure protection in the regions for the elements with unacceptable level of risk is scheduled.

In relation to the maritime critical infrastructure system at strategic level, a common warning zone has to be determined, agreed between the different departments, under the framework of which (based on the air and maritime sovereignty defense systems) to create a possibility for early detection and warning for potential threats to security.

To guarantee system stability it is required to incorporate feedback connections at all levels. The state of the system is monitored through those offsetting mechanisms that

determine the need for transition to a new stable state as well as balance the transition. Risk assessment (as main part of the risk management cycle) has to be initiated prior to major changes of the infrastructure or structure of the system; after a serious incident, associated with security; when a new risk factor is determined; or on a periodical basis. The result of this assessment is used for:

- Adaptation/ modification of system's goals, its "fitness" to the environmental conditions, and
- Evaluation of the structure of the strategy.

Based on the accomplished analysis of the considered critical infrastructure system, the authors propose the following recommendations:

1. To initiate risk assessment for other elements of the critical infrastructure using the applied in the NAVY method "Maritime critical infrastructure analysis." In this way, unification of assessment criteria standards and comparison of the results will be achieved, as well as an initiated cycle of risk management for the maritime critical infrastructure at an element level of the system will be performed.
2. To develop a procedure for integration according to geography specification of risk management actions for the elements of the critical infrastructure. The results from its application are supposed to have a system-constituted character in order to give the main elements of the developed "Plan for Critical Infrastructure Protection" in the Varna and Bourgas regions.
3. To develop procedure for the integration at national level of the actions for critical infrastructure risk management in order to establish a mechanism for concerting the efforts of the ministries and the departments in guaranteeing civil security and national sovereignty in the context of national security. As a result of this procedure, the documents required by the Law of Crises Management at national level will be created.

Nowadays, in conditions of transformation in the maritime sector of the country, associated with changes of possession forms, establishment of new economic rules and overcoming the difficulties encountered in any period of changes, new types of relations for coordination of activities in the maritime domain are determined. They are established using a new type of civil-military cooperation in protection of the sea interests of the state, as well as in guaranteeing maritime security. The maritime critical infrastructure protection system is an instrument for adapting these relations to neutralization of modern threats, as well as for minimizing the damage effects during crises.

Notes:

- ¹ John D. Moteff, *Critical Infrastructures: Background, Policy, and Implementation*, Report for US Congress (Washington, DC: Congressional Research Service and Library of Congress, updated 13 March 2007), <www.fas.org/sgp/crs/homesecc/RL30153.pdf> (27 October 2007).
- ² *Law on Crises Management*, <lex.bg/laws/ldoc.php?IDNA=2135499555> (23 May 2007).
- ³ Gueorgui Tsvetkov, “Risk Management,” *Military Journal* 113, no. 5 (Sofia, 2006): 29–36.
- ⁴ Todor Tagarev and Nickolay Pavlov, “Critical Infrastructure Analysis and Protection – Key Issues and Relationships,” *Military Journal* 113, no. 1 (2006): 84–96.
- ⁵ “Practical Application of Assessing Environmental-Related Risk,” in *Environmental Considerations in Military Operations*, FM 3-100.4/ MCRP 4-11B (Washington, DC: Headquarters, United States Marine Corps, 15 June 2000), <www.globalsecurity.org/military/library/policy/army/fm/3-100-4/appg.htm> (23 May 2007); Venelin Georgiev, “Implementing the Defence Programs of the Ministry of Defence for the 2006-2011 Period – Risk Assessment,” *Military Journal* 112, no. 6 (Sofia, 2005): 14–19; Dimitar Tashkov, “Assessing and Managing Risk in Operations Planning,” *Military Journal* 112, no. 4 (Sofia, 2005): 63–66.
- ⁶ International Maritime Organization, “International Code for the Security of Ships and of Port Facilities,” (London, 12 December 2002), <www.admiraltylawguide.com/conven/amendsolas2002.pdf> (15 June 2007).
- ⁷ Boyan Mednikarov, “Maritime Sovereignty Protection as a Specific Function of the System for State Government,” *Military Journal* 114, no. 1 (Sofia, 2007): 73–86.

BOYAN MEDNIKAROV – Information about the author is available on page 122 of this volume.

NEDKO DIMITROV is Senior Assistant in the Maritime Sovereignty and Surveillance Centre in the Bulgarian NAVY HQ, Varna, with main responsibilities for control of shipping and Maritime Sovereignty execution. He has experience as an engineering and commanding officer of onboard and shore based surveillance units and operational officer in the Navy HQ. His current rank is Commander in the Navy. Mr. Dimitrov graduated from the Naval Academy with a major in radio electronics in 1989 and from the “G.S. Rakovski” Command and Staff College in Sofia in 2003. He is pursuing his doctoral degree now and his research interests are studies of maritime critical infrastructure protection and information and warning system integration.

KALIN KALINOV – Information about the author is available on page 122 of this volume.