"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XVIII – 2015 – Issue 1
Published by "Mircea cel Batran" Naval Academy Press, Constanta, Romania // The journal is indexed in: PROQUEST SciTech Journals, PROQUEST Engineering Journals, PROQUEST Illustrata: Technology, PROQUEST Technology Journals, PROQUEST Military Collection PROQUEST Advanced Technologies & Aerospace

THE ROLE OF THE BULGARIAN NAVY IN THE MARITIME CRITICAL INFRASTRUCTURE PROTECTION SYSTEM

Nedko DIMITROV[1]
Siyana LUTZKANOVA[2]
[1] PhD, Lecturer, Nikola Vaptsarov Naval Academy, Varna, Bulgaria, e-mail: n.dimitrov@nvna.eu
[2] Assistant Prof., Nikola Vaptsarov Naval Academy, Varna, Bulgaria, e-mail: s.lutzkanova@abv.bg

Abstract: *The security environment of the national maritime critical infrastructure is analyzed in the context of identification of and fight against the modern security threats. The contribution of the Navy is outlined based on its tasks and capacity. The Navy's role in the national maritime critical infrastructure protection system is figured out and some future development areas are mentioned.*
Keywords*: maritime security threats, critical infrastructures protection, Navy tasks.*

The process of globalization in the beginning of the 21st century has brought new challenges, both positive and negative. The prevailing trends in the sphere of international relations are positive. Confidence and cooperation are developed successfully; there is a sensible enhancement of European and Euro-Atlantic integration processes. Peace and security are getting stronger. Crisis management and prevention of conflicts are better dealt with. Along these positive global environment however, the factors causing internal crises and destabilization of certain countries and regions have grown in number. New non-traditional risks and asymmetric threats had appeared and their nature has been changed from initially potential to real.

The environment, where for the last 20 years the Bulgarian national security system (as well as the security system of many other countries) underwent deep transformation. The conceptual basis of the transformation processes of the Bulgarian national security system has been determined by the new - "civil security" approach. On a normative level it is defined as *a condition of society featuring the achievement of efficient protection of the population and national economy in case of calamities, accidents, catastrophes and other extraordinary situations in order to reduce vulnerability, minimize the harmful sequences and recover quickly*.

The establishment of the civil security system is aimed to fill the gap between the national security system (on a macro level) and the system for protection of population and infrastructure (on a micro level).

The civil security system includes: the system for protection of citizens and infrastructure during calamities, accidents and catastrophes as well as the liquidation of the sequences of other types of crises (terrorism, organized crime, etc.).

It should be established as an independent "column" of the security system that should be equally important to the other two main "columns" – the homeland security and public order (provided mainly by the Ministry of Interior) and the foreign security (provided mainly by Ministry of Defense).

To a very great extent, the establishment of the civil security system requires active civil participation and control, higher degree of transparency, accounting and democracy.

It is characterized with the changes in the security environment by focusing the defensive efforts on objects being potential targets of modern threats and at the same time - critical for the security of the country, its public life and population - namely the critical infrastructure.

The maritime security threats and their nature in the changing environment are object of the current security research. According to the direction of the „vector" of impact on the critical infrastrcture elements as well they are:

- External - terrorism, piracy, organized crime, amateur criminals, extremists, „stowaways";
- Internal - disgruntled employees or forced/recruited to cooperate with a criminal organization or rivals, representatives/helpers of the above groups, employees with criminal tendencies etc.
- Combined - a particularly danger option terrorists to get control of the other categories.

According to the reasons:

- Maritime terrorism - political reasons (opposition to the political system), ideological or religious, symbolic, inducing fear;
- Piracy and armed robbery - economic motives;
- Transnational organized crime - economic motives - smuggling, trafficking;
- Internal criminal conspiracies - economic motives, smuggling rivals;
- Inter-state hostilities - diversion;
- Riots or civil disobedience - sabotage or vandalism.

Today it is very difficult to trace a leading trend in the development of those threats. At the end of the 20th century the protection of the critical infrastructure was an essential element of the security policy of a lot of countries, especially of the NATO and EU member countries. On one hand that could be connected with the globalization processes, and on the other with countering the most concerning threat- the international terrorism. There is a direct link between the threat of terrorism and the critical infrastructure protection. Particular reasons for activation of the critical infrastructure protection policy were the 9/11 events in the United States and also the following terrorist acts. Another major reason is the development and control of large infrastructure projects for transfer of oil, petroleum, gas, raw staff of strategic importance etc.

The matter of how to practically build the critical infrastructure protection in our country is still somewhat ambiguous and contradictory. By adopting the Crisis Management Law, specific governmental and regional authorities have been entrusted with particular responsibilities for the critical infrastructure protection; it is to be regretted however, that no mechanisms for their accomplishment have been introduced yet. There is a good practice of introducing the ISPS Code by IMO, but it concerns only the elements of the maritime transport scheme and they do not comprehend all the elements of the critical maritime infrastructures. The problems have to be deep analyzed in order to find principle approaches and concrete solutions based on the knowledge and experience gained worldwide, on researches carried out and on results interpretation.

The fact that there is no applied concrete model for the Bulgarian critical infrastructure protection means that the efforts of the scientists to develop the theoretical conception for the critical infrastructure protection have not been sufficient to satisfy the national requirements in this field. There are still problems, such as the proper place of the critical infrastructure protection within the national security system and the possibilities for integration with other security systems, which need to be clarified.

According to the assessments and analyses made in the Navy, threats for the critical infrastructure are classified as intentional and unintentional. Maritime critical infrastructure is associated with the sea, coastal routes and ports within the bounds of trans-European corridor No. 8, energy lines and dangerous goods routes as well as the crisis management systems and those of the sea-related institutions – the Navy, Maritime Administration and Border Police. We focused our efforts on the Navy contribution in fighting the intentional threats originated from the sea spaces.

International terrorism turned into the most difficult threat to be dealt with, as it globalizes, widens its relations with the organized crime, with no state groups with specific purposes, uses its accumulated financial resources and integrates with

the organizational structure and the ideas of different type of extremism (religious, ethnic etc.).

The asymmetric nature of the terrorist acts enables that a handful of people and means produce not only enormous material and physical damages but psychological impact as well, thus making a country's military power ineffective.

The first tide of international terrorism, which analysts assume to have occurred in 1968, affected mostly the air transport. In response to the enhanced safety measures, terrorists started to seek new and less protected targets. It is generally asserted that even today and in the near future as well, international terrorism is likely to concentrate its diversionary efforts on the more accessible ocean and sea communications.

Vulnerability of military and civil shipping from the terrorism at sea became plainly obvious during the attack of al-Qaeda men on the destroyer USS Cole on December 12, 2000. The success of the attack and the immediate public reaction has encouraged terrorist groups from Asia and the Near East to undertake similar suicidal acts. On October 23, 2000 kamikaze boats of the Liberation Tigers of Tamil Eelam destroyed one and damaged another Navy transport ship of the Sri Lanka. Later the same year on November 7, a Hammas kamikaze boat exploded ahead of time, slightly damaging an Israeli naval ship. On October 6, 2002 the French oil tanker Limburg was burst by means of an explosive-laden boat near the coast of Yemen. On June 14, 2006 the Israeli corvette Hanit was struck by a C-802 missile launched by soldiers of the Iranian group Hizbullah. The second missile hit an Egyptian merchant ship, which afterward sank.

About 90 per cent of the marine attacks address developing countries. The governments of the countries assaulted by terrorism at sea are quite often corrupted, inefficient, short of resources and knowledge how to counter the threat. Most of them are lacking the reconnaissance organization, legal tools and diplomatic influence needed to break and destroy the structures of terrorist and organized criminal groups. As a rule, should a government decisively repulse the threat, leave terrorists quickly the country seeking opportunities elsewhere.

What we think is that the real capabilities of marine terrorists at both tactical and strategic levels represent a multilateral and complex threat to the safety of navigation worldwide. Though the profound analysis of the tactical and technical characteristics of the international terrorism instruments cast away the distrust of many people in the real existence of "asymmetric" threats, the basic means for self-defense of ships remained focused, as before, on the traditional threats from the air, sea and coast (i.e. air defense, underwater defense, above water defense). Few maritime countries have included elite counterterrorist units in their navies: Special Boat Squadron (SBS) in Great Britain, SEAL teams (sea-air-land) in the United States and the Special Forces units in India. Most certainly, the funds that most countries invest in their navies in order to provide national maritime infrastructures defense and combat asymmetric threats at sea seem to be inadequate to the existing threat.

Marine targets are vulnerable to terrorist attacks from sea, coast and air. As we reckon, terrorist combat tactics varies from employment of land-based teams trained to place improvised explosive devices on board ships to employment of underwater swimmers, light aircraft, and hijacked ships from the legitimate traffic; mine lying. In a similar way, their equipment ranges from modern scuba outfit, sea scooters and speedboats to the most sophisticated navigation and communication systems. Sea terrorist activities against ships in naval bases and harbors differ from the ones against ships at sea. There are many factors that count when choosing one kind of tactics or another: motivation of the terrorist group and its operational experience, class and type of the ship to be attacked, significance and value of the target, existing security system at roadsteads or harbors. Employment of "kamikaze" tactics by terrorist groups greatly enhances their efficiency. Development and quick spread of remote control technologies also tend to be increasingly productive in diversionary activities.

Though presently there have been no indications of threatening actions with large-scale and coordinated terrorist acts in the Black Sea, the spreading geography of international terrorism makes the region potentially dangerous. The ethnic contradictions in the Black Sea region have been generally overcome and the potential of the Islamic extremism is restricted, but the risk of terrorist acts induced by ethnic reasons or nationalism still exists. The interest of international terrorism in the Black Sea is due to the following reasons: consequences of regional conflicts; complicated interethnic and religious problems; powerful influence of organized crime; efforts of extremist organizations to establish their network in the region; presence of paramilitary groups supported by governmental or other hidden sources; nearness to unstable regions as the Near East and the Caucassus. Moreover, the Black Sea is the crossroad of the illegal drug traffic – one of the financial sources of illegal organizations.

Although the current processes in this area, danger of terrorist acts and the will of compact communities for self-determination impair the stability of the region, the risks do not represent a direct threat for the security of any of the Black Sea countries.

Our main conclusion is that the situation should be kept under close and continuous control through surveillance and readiness for adequate response to the dynamic changes; otherwise the regional stability could be seriously endangered. Against the current environment, an assessment of the national maritime critical infrastructure risk level is to be made and, if necessary, measures to manage the risk shall be undertaken.

If the aim of critical infrastructure protection is to "provide its normal operation under any environmental conditions" it can be inferred that, considering the naval tactics and operational art, building the protection system capable of functioning in peace time as well as in crisis is the best way of accomplishing the task of maritime critical infrastructure protection.

The elements of maritime critical infrastructure can be most effectively protected by making use of some general concepts, which are decisive for the development of the contemporary art of war. Some of the concepts are:

- Determination of the centers of gravity – the concept is built on the idea, that a system could depend critical on a group of its elements (even one element). The centers of gravity are those elements of maritime infrastructure, which are the most essential for the security of the country and the society. These elements have to focus all the defensive efforts of maritime power of the country. Thus the systems will be organized efficiently without wasting available ressources.
- Information superiority – the use of C4I-type systems provides integration of information that extremely improves the efficiency of utilization of the country's forces which ensure all aspects of security, including the security of the maritime critical infrastructure. To this end, in the Bulgarian Navy was developed the project "National Integrated Surveillance System for Shipping Control and Sea Border guard". Due to financial restraints, the execution of the military component of the system – named "EKRAN" was impossible before 2009, when financial means were provided through the Foreign Military Financing Program. The system is being improved acquiring and integrating new sensors and expert and decision support subsystems, in order to raise the ability to establish maximum adequate common operational picture and effectively to support planning and execution of the defense actions.
- Netcentric operations – providing maritime domain awareness and improving its level is an element of the required capabilities, necessary for building the efficient maritime critical infrastructure protection. Netcentric control of the security environment could raise the efficiency of the protection actions benefiting from the conception principles.
- Effect-based operations are in full compliance with the preventive nature of the strategy for maritime critical infrastructure protection. The essence of the strategy employment is to focus the efforts preliminary on particular systems in order to achieve a particular effect which, directly or indirectly, helps reaching the desired end result. In the process of planning the maritime critical infrastructure protective measures, the strategy contributes to use the effects of: coordination the efforts of the participating forces; minimization

the risks by reducing the threats, control of vulnerability, etc. The expected result is considerable cascade effects related to: restraint of intended hostile actions, breaking the will of potential opponents or diminishing the necessity of providing critical services, which has a direct influence on the maritime critical infrastructure protection, too, decreasing the probability of threats accomplishment.

- Combined joint task forces concept **–** maritime critical infrastructure protection involves coordinated participation of forces and assets of various national organizations (agencies). On the other hand, the membership in the North Atlantic Treaty Organization and in the regional security initiatives provide further opportunities to enhance the national security, one of them -using the combined joint task forces.

Based on these conceptions, the most effective protection of the maritime infrastructure elements can be provided by building an integrated system of organizational and technical instruments capable to respond adequately and timely to contemporary threats, to work continuously and to be able to early detect and fully counter all potential threats for the defended targets security. The integrity of the system could be explained with the connectivity of the protection of every single critical infrastructure element in a common protection system, which is integrated to other security subsystems of the country.
If we try to find the roles of the different maritime institutions in such a protection system, we can outline and stress the role of the Navy. They play the leading role in crises management, in scenarios, related with asymmetric threats, because they own some advantages, such as mobility, exterritoriality, privilege of their ships acting in open sea, high level of interoperability and cooperation. They can participate in antiterrorist and counter-terrorist operations both as an independent force and as a component of a national or a coalition force, accomplishing the following major tasks:

- Execution of surveillance and reconnaissance in wide sea areas for the early warning purpose;
- escort the floating facilities of especial importance;
- protection of port facilities and coastal objects, providing safety of navigation;
- search and rescue at sea and evacuation of people in distress / in danger;
- providing humanitarian aid to people in distress;
- exercise of regional shipping control;
- using of special forces and antiterrorist groups;
- Participation in maritime embargo operations in order to isolate the terrorist groups in the operation areas.

To enhance the maritime domain awareness, up to now the Navy has established and maintain the following network links for information exchange:

- at an institutional level – within the framework of the army command and control C4ISR system – with the rest services of the armed forces, with the superior and subordinate command levels;
- at a national level – within the Vessel Traffic Management Information System maintained by the State Enterprise "Port Infrastructure", where the Navy and the Border Police are users. The extension of the system is already executed. The connection with the similar information system owned by the Bulgarian Fishery Agency is planned.
- at a coalition level – within the frameworks of the NATO Maritime Safety and Security Information System (MSSIS) for exchange of unclassified information, and within the Italian Trans-Regional Maritime Network. The integration to the NATO Maritime Command and Control Information System (MCCIS), supporting the classified information exchange up to NATO-Secret, is under way.

Additionally, new responsibilities for the Naval Forces may occur regarding the security of the future gas and oil offshore installations in the Bulgarian and Romanian offshore zone. The types of threats to offshore installations should be identified, the potential links and overlaps between different types of offshore security threats should be analyzed and a framework for a consistent approach to the assessment of these threats should be proposed. The international legal responses and security measures adopted by governments and industry to safeguard offshore oil and gas installations should be also reviewed in this concept.
In this context, the Navy appears to be the link between external and civil security in the model of national security. It can be concluded that building of capable and combat-ready Navy is crucial for the maritime security and is a factor in the fight against risks and intended threats in the maritime critical infrastructure protection system.
Several major practical fields and subjects of decisive importance for the planning and building of an adequate system for national maritime critical infrastructure protection would be specified as:

1. Development of unified methods of threat assessment to benefit the analysis of maritime critical infrastructure protection;
2. The phenomenon "criticality" study – its aspects, types, interdependences, behavior under impact;
3. Development of strategies and measures for maritime critical infrastructure protection: prevention, protection, recover actions;
4. Maritime critical infrastructure protection capabilities building: study of the structural, organizational, information and technical factors; protection planning;
5. Definition of the maritime critical infrastructure protection in the context of the maritime crisis management system.

The studies carried out, final scientific results, proposed scientific solutions and applications along with modern approaches, will favor further the establishment of a maritime security system in which frame the maritime critical infrastructure protection will be built most effectively and efficiently.
The role of the Naval Forces should be prioritised and considered as decisive. They have the biggest practical expertise in performance of control over the national marine territories and they still posses great potential in ships and an excellently deployed coastal surveillance system (CSS) with big capacities. A great extent of operational interoperability with the forces and means of Naval Forces of NATO' and Black Sea countries is achieved. They still possess also the biggest experience in organization of the interaction among different forces as well as in their most efficient management.

Bibliography:

[1] Analyse Kritischer Infrastrukturen (Die Methode AKIS), http//www.bsi.de/fachthem/ kritis/acis_paper_d.pdf, 11.09.2014.
[2] Kolev K., Management of Maritime Security, Varna 2014.
[3] Mednikarov B., Defense of the Maritime Sovereignty, Varna 2008
[4] Mednikarov B., K. Kolev, S. Lutzkanova, Problems of Security of Offshore Oil and Gas Installations, in: International Scientific-Applied Conference „New Technologies in the Offshore Industry", 3-5 October 2013 г., Varna.
[5] Moteff J., Critical Infrastructures: Background, Policy, and Implementation, Updated February 17, 2005, Report for US Congress, http://www.fas.org/sgp/crs/homesec/RL32531.pdf.
[6] Moffat J., Complexity theory and network centric warfare, ISBN 1-893723-11-9
[7] Концепция за защита при природни бедствия и аварии (Concept for protection from natural disasters and accidents), <http://www.mdpba.government.bg/documenti/ drugi/koncepciya-za-zaschita-pri-prirodni-bedstviya-i-avarii>.