Click here to view PowerPoint presentation; Press Esc to exit

Harbor Protection Against Terrorist Threats: Difficulties and Possible Solutions

Ovidiu RADU, Georgică SLĂMNOIU, Liviu ZĂRNESCU
Naval Research Center
Constanta, Stefanita Voda Str., No. 4, 900402
ROMANIA
Tel: +40-241-671022; Fax: +40-241-641368

staff@ccstm.ro

Liviu COŞEREANU
Military Equipment and Technologies Research Agency
P.O. BOX 51-16, 053070, Bucharest
ROMANIA
Tel: +40-21-4231483; Fax: +40-21-4231030

rsi@acttm.ro

ABSTRACT

Ships play an important part on the scene of current conflicts. This is why they must be protected both in their home port and in other operating harbors. Also, because they are a symbol, an extension of a state's territory, they are a potential target for terrorists, fact that was demonstrated in 2000 by the action against USS Cole in Yemen, or in 1995 against the Sri Lanka Navy.

An integrated harbor protection system must be prepared early on so that it permanently supplies information that will lead to reducing adverse actions effects, and increasing the global performance of the reaction force. A complex of detection technologies is needed so that the information is redundant and it ensures a false alarm rate as low as possible, and target tracking to be done accurately and automatically. From this point of view, designing such a system implies conducting studies about threat and sensor characteristics, data fusion, complex systems architecture, etc.

1.0 GENERAL SITUATION

Overlaying the globalization process with the regionalization tendencies and, mostly, with the emergence of non-state players, will determine the appearance of a broad spectrum of risks and asymmetric threats.

The international relations and the security environment are irreversibly marked by the terrorist attacks on the US, Spain and United Kingdom, attacks that have modified the geopolitical stage, enhancing its unpredictable character, and which have led to amplifying the existing instability sources, and to the appearance of new types of them. On this background, the risk of large scale military conflict will decrease, but will grow and diversify the political, economical, social and military risks, at regional, zonal and local scale.

Radu, O.; Slămnoiu, G.; Zărnescu, L.; Coşereanu, L. (2006) Harbor Protection Against Terrorist Threats: Difficulties and Possible Solutions. In *Force Protection in the Littorals* (pp. 3-1 – 3-10). Meeting Proceedings RTO-MP-SCI-180, Paper 3. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

Starting from the transnational and asymmetric characters of terrorism, the main threats terrorist in nature (as considered by this paper), are considered to be the following [1]:

- The possibility of usage by terrorist organizations, groups or persons of weapons of mass destruction.
- The proliferation of punitive or retaliatory actions against those that started the antiterrorist campaign and against the countries that take part in the antiterrorist coalition. In this sense, more than likely ate the actions that target:
  - Conducting attacks on environmental protection systems, water dams, and using toxic and radioactive waste to cause ecologic disasters;
  - Attacking research institutes, laboratories and national or international importance companies, to produce panic and terror;
  - Continuing and intensifying attacks with bombs, explosives and other improvised devices against the population, in crowded place and, if possible, when the media reporters are present.
- Terrorist actions in cyberspace, to create grave perturbations in the communication systems, destruction of command and control systems, banking systems, database infections and creating a state of generalized chaos in the informational and information systems.

But the specter of terrorist threats is much wider, and practically we cannot build a complete index of terrorist threats and risks, due to their diversity but also to the rapidity of emergence of others. We can easily conclude that, without forgetting the classical terrorist devices, particular to the cold war era (car bomb attacks, assassinates, kidnappings, aircraft hijacking or embassy takeovers) the terrorism has became 'super terrorism' in the last decade, through adopting in their arsenal of weapons of mass destruction: nuclear, biological and chemical.

We have to notice that attacks with explosives are the most used method by terrorist organizations, and this is based on the wide knowledge spread about producing explosive substances (books, Internet, etc) and the large number of modalities in which it can be done[2]. Terrorist groups use a very diversified gamut of explosives, and explosive devices can have hundreds of different shapes, and these depend on a lot of factors like: target, terrorist's training, available materials, target's environment constraints, and so on.

At present, we have re-started to consider the vulnerability of commercial and military ships, of naval bases, commercial harbors, oil platforms and terminals, and of other similar coastal emplacements to terrorist attacks. In March 2004 Hamas divers have attacked an Israeli coastal surveillance installation, and in April, oil installations on the Iraqi coast have been targeted by similar terrorist attacks. The US Navy has list 17 sailors as a result of the terrorist action in the port of Yemen against USS Cole in 2000, and the Sri Lanka Navy has lost a few ships in 1995 when the Tamil Tigers used suicide divers to attack them.

2.0 PARTICULAR SITUATION

Generally, harbors are vulnerable to terrorist attacks because of their dimensions, general accessibility from water and land, intense traffic of materials and people, their emplacement in densely populated areas, and so on. Because harbors represent a great density of transport ways (roads, railways, navigation channels), they are much more vulnerable to terrorist attacks than other areas. The concentration of passengers, merchandise, properties and business in harbor areas represent just as many potential targets.

Ships and drilling platforms represent a symbol. A ship belonging to ROMLINE represents Romania itself. More than the company, the state itself is targeted by a terrorist attack[2]. Also, not without importance, is the crew or passenger's nationalities, or the destination of the ship.

The main threat categories against port facilities are:

- Thefts from ships and from harbor installations;
- Terrorism: bomb attacks, hostage situations;
- Traffic of forbidden substances;
- Sabotages: intentional damage or destruction of harbor installations, of the communications network, of the data communication network, of a part of a ship, equipment or cargo, vandalism;
- Piracy and armed robbery;
- Threats against the environment: accidental spillage or intentional drainage of pollutants; and
- Proliferation and development of terrorist networks, of transnational organized crime, illegal traffic pf persons, etc.

Any location comprised in the harbor category implies the existence of a large surface area, difficult to administer and protect, which has a diversified economic activity, a complex administrative and control structure, and a diversified topography of property boundaries, and these make this structure difficult to manage and protect from the threats and risks to which it is permanently exposed. The existence of diversity of activities of harbor operators implies a large flow of merchandise, persons, transport vehicles that have to be monitored and managed in order to insure the safety and security of the installations to protect. Generally, the harbor surface is physically characterized by:

- Perimeter boundary fences;
- Access control points;
- Infrastructure (transport, communications, public utilities, maritime flow command and control installations, etc.);
- Harbor basin;
- Berths (operative and technical) providing the ship-port interface (with a maximum admitted Tonnage at berths, maximum depth at berth determines a certain operation capacity, which in turn determines which ship types are admitted);
- Banks protecting the berths against sea waves;
- Port operators providing various services (pilot, towing, berthing and releasing ships, supply, operation); and
- Merchandise storage.

As it is well known, in London, between 9 and 13 December 2002, during the IMO Conference, have been adopted amendments to the Annex to the International Convention for Preserving Human Life at Sea from 1974 and amended, and to the International Ship and Port Security (the ISPS code). In addition to the requirements imposed on companies by the A section (compulsory) of the ISPS code, it is also mandated that port security is of such a nature so that it does now allow unauthorized access to the ships, including the mobile drilling platforms at sea, but at the same time that all protection activities conducted must not cause major disturbance or delays to passengers, crew, merchandise, ships and services. Also, in the B section (recommended) of the ISPS code, it is stated that, in the process of identifying the weak spots from a security point of view to a ship or port installation, it has to be considered the possibility of the threat being initiated from the open sea, from surface.

We find that there is no particular mention concerning the protection of port installations from terrorist or diversionist attacks launched from underwater. Also, harbor and ship protection against attack launched from open sea (even those originating from surface), at present is still lacking. At the same time we can remark that ship arrivals are much more supervised than ship departures.

3.0 DIFFICULTIES IN DESIGNING A HARBOR PROTECTION SYSTEM

An integrated harbor security system is always a mix of human, technical and procedural measures, meant to achieve the deterrence, delay, detection, assessment and intervention in cases of unauthorized access attempts in regard to harbor perimeter and port facilities used by port operators. From recent years' experience we have found that protection measures that use only humans are totally inefficient in harbor area conditions, being impossible even to assure the integrity of perimeter boundary fences, without even considering the problem of preventing unauthorized access.

An objective analysis of the crime situation in harbor areas shows that the frequency of unauthorized perimeter crossing events for various purposes is extremely high. This fact makes even more difficult the early detection of unauthorized harbor perimeter entry attempts using only the administrative measures and guarding measures using humans exclusively.

Across the years, various checklists have been compiled (and these must be permanently analyzed and updated) regarding various problems that appear in designing and implementing integrated harbor protection systems [4]. Some difficulties that, in author's opinion, maintain their current status, and have a major influence upon the global performance of the protection system are:

- Not knowing exactly all the data that characterizes completely the threat (availability, specific 'fingerprints', behavior parameters – speed, autonomy, etc-, destructive potential, etc.) with direct implications on the determination method for operational and technical characteristics: surveillance area dimensions, type of used sensors, angle and distance resolutions, etc.
- Difficulty in estimating the characteristics of the resources used in combating the threat: type of counter-action, effectives, reaction time (depending on layout, vehicle types, etc), reaction attack devices (lethal or non-lethal).
- Necessity of estimating as precise as possible of the general environment parameters, and of those specific to a certain location, in order to determine the type of sensors deployed, detection performances, necessity of using redundant systems, etc.
- Necessity of automating processes of surveillance, detection, pursuit and identification imposed by the permanent character of this activity and its importance.

Conducting general purpose analyses of these problems can not be considered a productive and pertinent activity. Thus, we will try to outline a type of these activities, concerning a single type of threat (underwater one) in order to underline the importance of approaching them under the most intimate aspects.

Table 1 shows the capabilities of various attackers against targets on the littoral (ships, harbors, etc) from the point of view of availability, probability of use of such a method, and of the destructive potential[3].

Table 1: Capabilities of possible attackers

Attacker / weapon	Availability	Probability of attack	Destructive potential
Diver	High	High	High
Torpedo	Low	Low	High
Fast ship	High	High	Medium
Mine	Medium	Medium	High
AUV / ROV	Medium	Low	High
Mini submarine	Low	Medium	Medium
Unforeseen attackers (e.g. dolphins)	Medium	Low	Unknown

To be possible to define operational characteristics of a protection system against such attackers, in addition to a good knowledge of environmental parameters (propagation, position of natural obstacles, statistical properties of the clutter) we have to also consider those characteristics of the threat that refer to movement and the 'fingerprint' of this, from the point of view of the sensor used in the detection and identification process. In Table 2 we present this data from the point of view of hydro-acoustic detection (passive or active) [3].

Table 2: Characteristics of targets from the point of view of detection using sonar systems

Attacker / weapon	Speed [knots]	Action depth [m]	Target strength [dB/1 µPa/1 m]	Generated noise level
Diver	0,5 - 1	1 - 20	-25	Low
Torpedo	10 - 50	> 20	-20	High
Fast ship	5 - 40	0,1 – 0,5	?	High, but fluctuating widely
Mine	-	5 - 10	-15	-
AUV / ROV	2 - 5	5 – maximum zone depth	-20	Low
Mini submarine	2 - 5	5 - 30	-10	Low
Unforeseen attackers (e.g. dolphins)	1 - 35	1 - 50	-15 to -30	High

We can notice that potential attackers that have a high availability (supported by a destructive potential that is also high) have evolutive and specific characteristics from the point of view of detection with sonar-type systems, characteristics that are spread on quite a large gamut of values, so that the process of determining technical and operational requirements becomes extremely difficult.

Let’s consider, for example, the case of divers:

- Equipments can be purchased relatively easily.
- Manufacturing explosive devices, or purchasing these via obscure channels must not be considered a difficulty.

- Can be deployed from any boats, from beaches near the objective, from commercial ships, etc.
- Specific characteristics (for example target strength) varies significantly depending of the sonar systems (working frequency, modulation type, etc) breathing apparatus used (closed or open circuit), and so on.
- They act in an environment which has characteristics that affect detection capabilities: noise generated by high volume traffic, shallow waters, high masking possibilities, etc.

At a speed of 1 knot (≈ 0.5 m/s) the diver can cover a distance of 500 meters in about 17 minutes. These 500 meters are (currently) the detection distance for sonar systems designed for diver detection, for a target strength of -25 dB and ensuring a detection probability greater than 90%. If we also consider the time needed for attacker detection, identification and classification, determination of trajectory, estimating the danger factor of this (by determining possible targets) and so on, we can observe that the time needed for a counter-action intervention team remains at around 8 to 10 minutes, which implies using ultra rapid transport vehicles, localization and 'instantaneous' neutralization of the aggressor. If we are dealing with the attack of a terrorist team, coordinated in time and space, this situation becomes critical. This situation can aggravate if we keep in mind that the target strength for a diver using an open air circuit system can reach – 27 dB (at 100 kHz) [5], the air bubbles left in the wake of a ship are masking for a significant period of time the target (figure 1), and the presence of various objects in the surveillance area (figure 2), besides providing cover for the divers, also makes the operator's activity significantly more difficult [6].

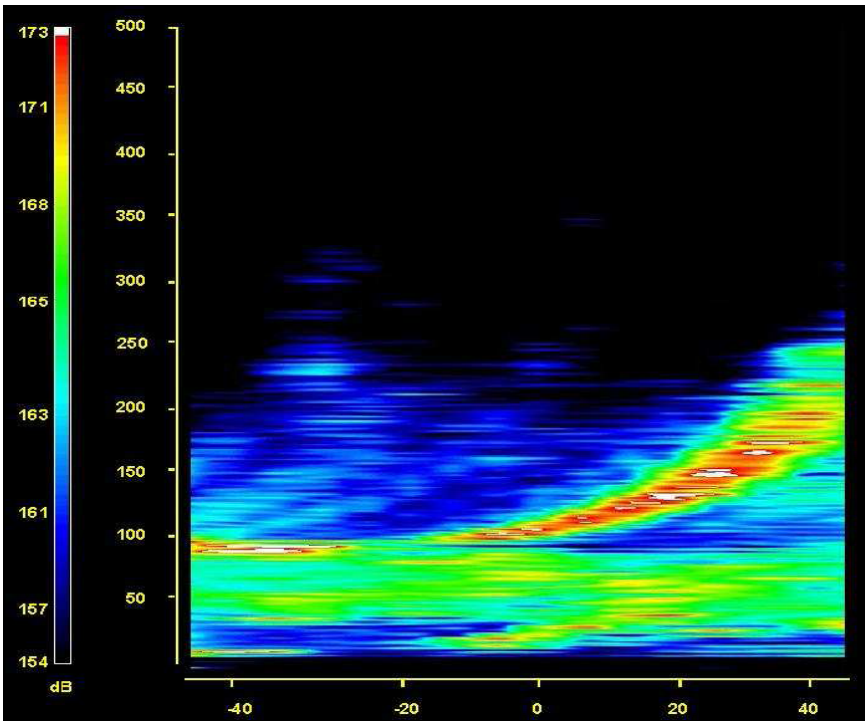

Figure 1: Noise generated by traffic

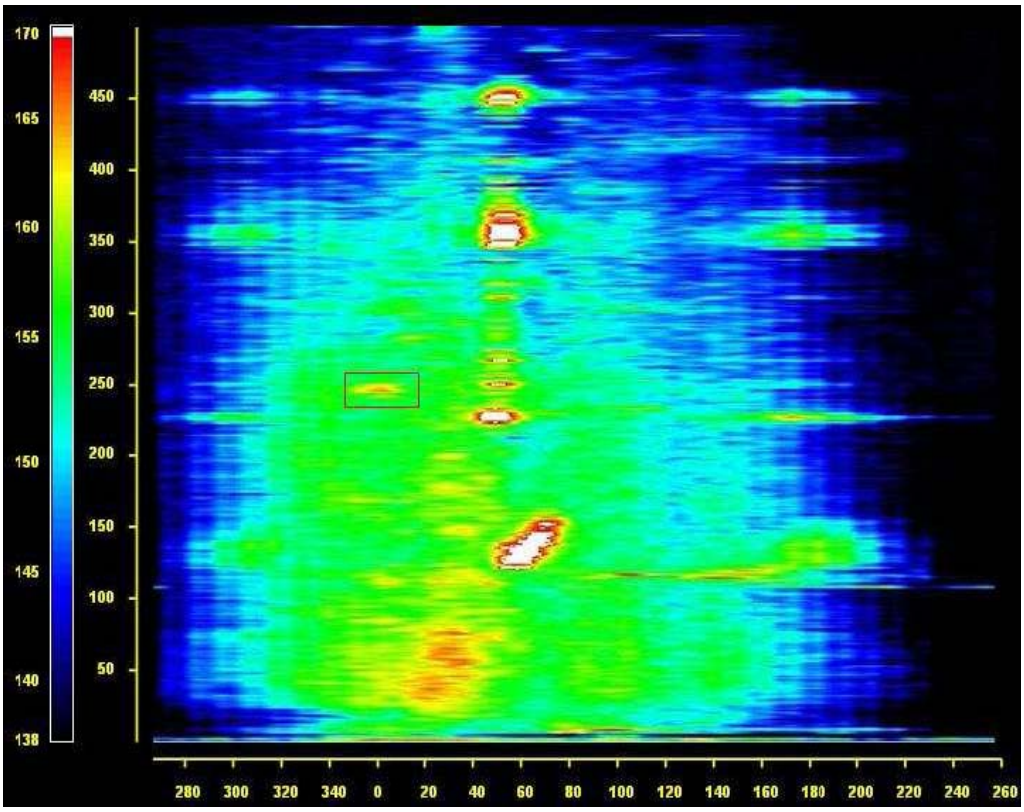

Figure 2: Open circuit diver located at 250 meters

Conducting a similar analysis for an AUV/ROV that moves at a speed of 4 knots we can remark that this one can travel a distance of 1600 meters (common discovery range by sonar systems of this type of target) in about 13 minutes. Also, if we account for the time needed for detection, identification and classification, determining the trajectory, estimating the danger posed by it, we can notice that the required time left for a counter-action team is only 6 to 8 minutes, which implies an extremely rapid action.

It might seem that we have forgotten that the physical security mechanism, as component part of the harbor security mechanism has as a main goal to detect, delay and stop (or annihilate) a hostile action or a dangerous situation. The global response time of the security system depends on the barriers that lay in the intruder's entry path, on the system's detection time, and on the response speed of the intervention forces (figure 3).

On a summary analysis we find that:

- It is required to deploy physical barriers in order to delay the aggressor, and to increase the time available to the action against it;
- It is required to use (in addition to sonar sensors) non-acoustic sensors (TV/laser, magnetometers, etc) and developing solid algorithms for data fusion in order to increase detection probability, but at the same time lowering (within reasonable limits) of the false alarm probability, with a direct effect on lowering the time constraints of the security system; and
- It is required to conduct in-depth research and to develop databases of "fingerprints" (to be able to make the difference between a diver and a dolphin for example), in order to lower the time interval between triggering the first alarm and the moment of identifying and classification of the aggression.

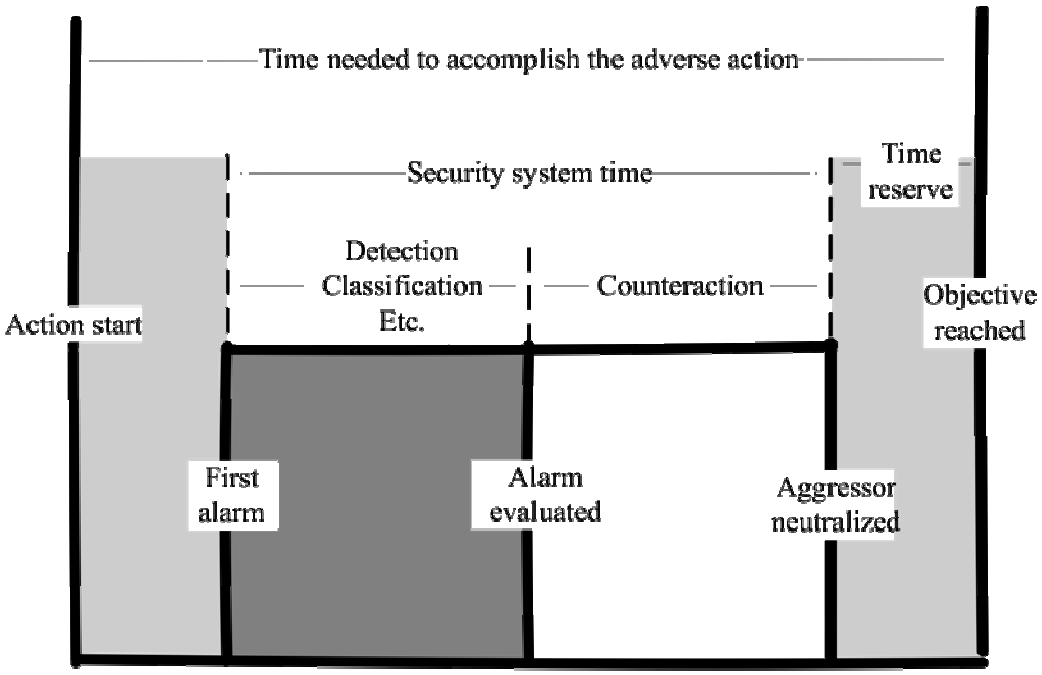

Figure 3: Time for conducting attacks and counter-attacks

Such analyses (actually much more in-depth ones, accounting for the specificity of the protected installation, types of attack, and so on) must be conducted for all threats, and for all possible action environments (aerial, terrestrial, underwater), for the entire harbor, but also for particular installations in the harbor area that have an increased vulnerability or a major importance.

Of the essence, an integrated harbor security system is a typical command and control system (C4I) which has as primary functions:

- Gathering information using various means, including technical devices;
- Transmitting and processing the information;
- Assisting the decision process; and
- Providing means to counteract.

All the mentioned requirements lead to the conclusion that we cannot use an all-purpose single detection technology against all possible threats, especially when we need to protect littoral areas whith intense naval traffic, and the objectives to defend are multiple. Also, we need a complex mix of detection technologies so that the information is redundant, and to provide a rate of false alarms as low as possible, and that target tracking to be accurate. Discovery distances of potential targets will be determined such that they allow for an efficient intervention from the response forces.

4.0 CONCLUSIONS

There are two axioms that are unanimously accepted when conducting an analysis in this area:

- It is a practical impossibility to assure 100% protection of a critical piece of infrastructure; and
- It does not exists a single universal solution to solve this problem.

When outlining the security systems for harbors, we must use the following principles:

- The security system is the result of a concept, of a chosen strategy, and of a careful cost-efficiency analysis;
- It is adaptable, open and perfectible, but is tailored to meet the needs of the objective it protects;
- It is of a mixed structure (man and machine), cybernetic in nature, with self-adjusting and learning depending on which security policies are successfully applied;
- "Freezing" and non-adjusting in security means no security; and
- Relatively high costs of security can be dramatically lowered through professional analyses and adequate mechanisms, and are compensated by having safe ships, satisfied customers, staff safety and behaviour.

The harbor protection system against terrorist attacks must:

- Be modular;
- Be adaptable;
- Employ modern technologies;
- Incur low maintenance and repair costs;
- Provide a detection probability as high as possible while at the same time having a false alarm probability as low as possible; and
- Be easy to use.

The concept uses the depth protection method which is based on outlining concentric monitoring areas, where de detection systems for potential intruders are deployed as close to the perimeter as possible, so that they have a low time needed for identification and reaction in the responsibility area. The subsystems of the protection system that have a role of detection, delay and neutralization of aggressors must be deployed in a circular-concentric pattern, in order to provide an efficient separation of the vital areas situated on the inside, compared to the external environment. The number of protection layers/barriers needed is designed so that we obtain the required delay.

The satisfactory functioning of the system and its efficiency is appreciated through analyzing the response times for each stage of the functioning cycle in figure 3. These response times depend on both the design solutions and on the performance of the sensor system (detection and alarm transmission time) and on the performance of the methods and identification algorithms (time of identifying a source), and also on the human and procedure factors (time needed to reach a decision, and for reaction forces to intervene).

[1] SARCINSCHI, A. and BĂHNĂREANU, C. (2005). *Redimensionări şi configurări ale mediului de securitate regional (Zona Mării Negre şi Balcani)*. Editura UNAp, Bucureşti.

[2] MARRET, Jean-Luc (2000). *Techniques du Terrorisme.* Presses Universitaires de France.

[3] SCHNEIDER, D. and CORSTEN, A. (2005) *Combined Performance of various Sonar Systems for Own Ship / Harbour Protection against an Asymmetric Attack.* http://www.tica05.org/papers/schneider.doc

[4] SUCHMAN, D. (2005). *Basic Do's and Don'ts of Designing, Installing and Operating a Harbor Protection System.* http://www.tica05.org/papers/dan_suchman.doc

[5] HOLLETT, R.D., KESSEL, R.T., PINTO, M. (2006). *At-Sea Measurements Of Diver Target Strengths At 100 KHz: Measurement Technique And First Results*. Conference Proceedings - UDT Europe 2006.

[6] Siegfried, Ralf (2006). *Protection Against New Asymmetric Underwater Threats.* Conference Proceedings - UDT Europe 2006.