NATO OTAN NURC
a NATO Research Centre
un Centre de Recherche de l'OTAN
NURC PARTNERING FOR MARITIME INNOVATION

Reprint Series NURC-PR-2007-005

Protection in ports: countering underwater intruders

Ronald T. Kessel

October 2007

Originally published in:

UDT Europe, Undersea Defence Technology Europe, Naples, Italy, 5-7 June 2007.

About NURC

Our vision

- To conduct maritime research and develop products in support of NATO's maritime operational and transformational requirements.
- To be the first port of call for NATO's maritime research needs through our own expertise, particularly in the undersea domain, and that of our many partners in research and technology.

One of three research and technology organisations in NATO, NURC conducts maritime research in support of NATO's operational and transformation requirements. Reporting to the Supreme Allied Commander, Transformation and under the guidance of the NATO Conference of National Armaments Directors and the NATO Military Committee, our focus is on the undersea domain and on solutions to maritime security problems.

The Scientific Committee of National Representatives, membership of which is open to all NATO nations, provides scientific guidance to NURC and the Supreme Allied Commander Transformation.

NURC is funded through NATO common funds and respond explicitly to NATO's common requirements. Our plans and operations are extensively and regularly reviewed by outside bodies including peer review of the science and technology, independent national expert oversight, review of proposed deliverables by military user authorities, and independent business process certification.

NOTE: The NURC Reprint series reprints papers and articles published by NURC authors in the open literature as an effort to widely disseminate NURC products. Users should cite the original article where possible.

PROTECTION IN PORTS: COUNTERING UNDERWATER INTRUDERS

Ronald T Kessel
NATO Undersea Research Centre
Viale San Bartolomeo 400
La Spezia (SP) 19126 Italy
kessel@nurc.nato.int

The advance of new capability depends on many things: the state of the art in technology, the clarity of the mission and requirements, the knowledge of the threat, the means of response, and, for developers, the state of the supporting literature. These are reviewed here insofar as they drive the advance of capability against underwater intruders for the protection of assets, both military and civilian, in ports and harbours. The purpose is to give more coherent direction toward new capability where fragmentation and fashion without substance have too often appeared. The review is based on technology demonstrations, a literature search, international meetings, and experimentation undertaken at NURC for protection in ports during 2006.

INTRODUCTION

Increased concern about terrorism has lead analysts to study the vulnerability of civilian infrastructure to attack. Not least are harbours where, among other things, millions of containers and hazardous bulk materials are handled, high-profile international political and sporting events may be hosted, and vessels of high strategic or symbolic importance may visit. The scenarios to be averted include, for example, the economic scenario—a major harbour is closed for a time with significant economic impact; a health-safety-environmental scenario—dangerous chemicals are spilled or detonated; and a political scenario—a high-profile event is marred and exploited by terrorists. (Weber 2006, Richardson 2004, Rust 2004, Katulski et al. 2006, Anderson 2005, European Communities 2004 & 2006).

Among the modes of attack is the delivery of explosives underwater by divers, assisted to their target perhaps by an underwater delivery vehicle. What do emerging technologies provide to counter such a threat? Quite a lot, judging from the literature (see the references listed at the end of this paper). Despite the sense of urgency, the transition path for technology, from developer to operations, has not been smooth. The integration of systems, needed for entry into operations, has suffered from fragmentation and insubstantial fashion.

Fragmentation is the result of apparently overwhelming demands pulling limited resources in many directions. For countering underwater intruders, for instance, one faces swimmers, divers, mini submarines, autonomous underwater vehicles, and more. Each class of threat poses particular demands on surveillance, and hence, calls for different sensors, or for particular use or configuration of sensors. The technical options are multiplied this way, being the number of threats times the number of prospective sensor technologies for each. Fragmentation results if there is no compelling principle justifying the inclusion or exclusion of options apart from the promotion of one's own favourite products and budget limitations.

By *fashion* is meant a typical response, more by developers than by security and funding agencies, namely, the presentation of a long shopping list of threat and sensor combinations from which buyers are expected to choose what is required, albeit with the implied danger of the obvious "gaps" in protection left by whatever has been excluded. The posture is superficial inasmuch as it plays on concern about security without fully understanding the problem, neither the threat nor the security forces, and offering little objectively demonstrable benefit in terms of capability. The shopping-list creates an illusion of grasp and preparedness in its presenter, and of indecision and ill-provision in the buyer or funder. No party is served very well this way because none arrives at solutions that are at once feasible and convincing, rarely winning the consensus and acceptance that large capital projects require.

This paper diagnoses the causes of fragmentation and fashion through a critical review of the literature dealing with technology for countering underwater intruders, and from experience with a number of technology validation trials. A way to vitalize technological advance is then proposed.

This paper is in effect a case study in *anchoring concepts* for a campaign of technological development. The case for anchoring concepts in technological advance is made in Albers & Hayes 2005 for the military, and for business enterprises more generally in Drucker 2005. An anchoring concept is the perspective adopted for action during sustained advance. It is a mission statement of sorts, such as every enterprise, simply by its existence, necessarily adopts.

For new technology, an anchoring concept guides engineers in higher-level system decisions, when deciding performance and cost tradeoffs, balancing competing objectives, or when deciding whether one or another sensor system should be included for instance. Some anchoring concepts are relatively weak and changeable (fragmentary and fashionable perhaps) while others are strong and productive. A strong anchoring concept becomes a unifying force of clarity for objectives, which in turn engenders consensus in decisions at many levels, within the development team and later among operational planners, funding agencies, and buyers. A weak anchoring concept, on the other hand, leaves the system design unfocused, with unrelated elements forced into proximity merely, each for its own reasons, unshaped by the whole. The system flounders in its design and is difficult to sell. The difference between the strong and weak anchoring concept can therefore mean the difference between purposeful and ad hoc capability, and between a fast and slow track from development, to market, to operation.

No anchoring concept is perfect. It is important, where possible, to knowingly choose a productive concept. Here it is argued that a *sensor-centric* anchoring concept has prevailed so far in the development for technology for countering underwater intruders (if not for harbour protection more generally), and that this concept has hampered progress. Another *capability-based* anchoring concept is recommended as corrective. There is nothing new about a capability-based concept. And like many high-level concepts, its basic elements may seem obvious, at least *after* they have been clearly stated. There is a need, however, as we shall see, to reiterate the role and utility of the capability-based approach in the context of harbour protection.

CAPABILITY

One obvious way to counter underwater intruders is the use of an underwater fence—steel nets hung from surface floats from sea surface to sea floor. But nets are not always feasible. They are bulky and heavy to transport, deploy, recover, and maintain (Cavagnaro 2006). They furthermore typically secure only a small exclusion zone in the immediate vicinity of stationary protected assets. Otherwise they interfere with business by blocking traffic. Or, if they encompass a large area, their effectiveness is compromised by encircling possible intruder entry points. Underwater surveillance is therefore required.

Surveillance alone is not enough for protection through proactive action during the moments before an attack. A form of response must be added to the actionable knowledge discovered by surveillance. Surveillance without response is at best impotent awareness, and response without surveillance (awareness) is misguided. Whatever the surveillance technologies may be, then, it is clear in principle that they must somehow be aligned to a plausible form of response for capability. A *capability-based approach* in this context therefore means the integration or alignment of surveillance and response. This view of capability is admittedly obvious, but let us see where development generally stands.

REVIEW OF DEVELOPMENT

Forty-four papers listed among those at the end of this paper were reviewed and classified according to their content. These were chosen in particular for review because they dealt specifically with new technology for countering underwater intruders. (Also included among the papers listed are those dealing with threat and vulnerability analysis, and with the text of this report. A more detailed literature review will be forthcoming.) The subset of forty-four reviewed here is by no means exhaustive for a technology review. They were the papers that were hit upon during the course of a larger program of technology validation that included a number of realistic demonstrations at sea. These were also chosen because they were

believed to have a level of editorial independence. Marketing brochures were excluded, for instance, while conference proceedings, government-funded reports, and articles in engineering magazines were included. Papers were classified according to their perspective on underwater intruders and type of sensor coverage. Over time, a low showing on the topic of response spurred increased search effort toward response, but response made a smaller showing nonetheless; the distribution of topics covered (with topic overlap) being

Surveillance	93 %	(37 papers)
Response	25	(10)
Surveillance + Response	15	(6) .

The proportions are indicative of the relative effort. The effort is heavily biased toward the development of sensors and surveillance. Of the papers dealing with surveillance and response together, half refer to a single USA integrated surveillance and response system.

A sensor-centric bias is evident elsewhere through the frequent use of terms such as “layered defence” and “sensor barrier” when speaking of sensors alone, as if sensors themselves constituted defence and barriers. Some survey papers focusing entirely on surveillance neither mention response nor point out its exclusion, again as if security were a entirely a matter of surveillance. A few papers expressly excluded response. The mandate in the NATO study (Cavagnaro 2006) for instance, expressly excluded response, but the report ventured into response nonetheless, making general bounding assumptions because this was necessary to generate integrated system recommendations.

There are many sensor options. Among the commercially available are active acoustics, passive acoustics, and passive magnetic sensors, for instance. A detailed review cannot be given here (see elsewhere, in Cavagnaro 2006, Kessel and Hollett 2006, Keil and Croix 2006, for example), but readiness can be surveyed more generally.

Assessing technical readiness is admittedly qualitative and subjective. A step toward analysis can nevertheless be made using the NATO technology readiness levels (TRLs):

TR Level	Description	Literature Distribution
1	Basic principles observed and reported	3.5 %
2	Technology concept or application formulated	12.9
3	Analytical and experimental proof of concept	14.1
4	Component or breadboard validation in laboratory environment	14.1
5	Component or breadboard validation in relevant environment	22.3
6	System/subsystem model or prototype demonstration in relevant environment	24.7
7	System prototype demonstration in an operational environment	8.2
8	System completed and 'flight qualified' through test and demonstration	0
9	Actual system 'flight proven' through successful mission operations	0

The papers dealing with particular technologies for countering underwater intruders were classified in terms of technology readiness. TRL 8 and higher were not awarded because no paper spoke of exercises beyond demonstrations; of unalerted simulated attacks, that is, as TRL 8 certainly requires. A case for higher readiness could perhaps be made by developers using additional proofs and operational experience that has not been reported in the literature. At the same time, *any* show of capability during a demonstration would constitute a proof of concept in a field trial; at TRL 3 that is. Thus one would generally expect TRL 3 to 7, or *medium* readiness in the literature, and this is what one finds. The distribution is listed in the table above.

As shown in the table, roughly half (47 %) fall in the TRL 5 to 6 level—i.e., demonstrated in realistic environments and conditions, short of operational (unalerted) evaluation. This confirms the view generally held in port protection, that technical readiness is relatively high, at least beyond development, and that it is ready for use. Advance onward from TRL 6 means pressing technology further toward integration with other systems in operations. Integration requires a guiding principle if it is to escape arbitrary association by proximity alone. A sensor-centric

view provides one principle for integration, while the capability-based approach provides another.

SENSOR-CENTRIC INTEGRATION

The sensor-centric approach is more insidious than it may first appear. It hampers technological advance by casting the anchoring concept too far from the final objective, from proactive protection that is. Indeed, the outstanding problem—in other words, the technologically hard point that developers pose for themselves—is *sensor fusion*: the integration of many diverse sensors into a single "system of systems" manageable by a single operator. *Integration* typically means multi-sensor fusion in fact. Although fusion is often mentioned and recommended, few if any details are provided in the literature, owing perhaps to reservations about proprietary information. Fusion is seen as the battle field where the security problem is finally going to be solved. Multi-sensor fusion therefore features in the literature as a place-holder for proprietary developments, or for future work still without details. In any case, sensor fusion poses as the final and most essential item on the long shopping list of sensors, justified by all of the others.

It is important at this stage to acknowledge the legitimate origin of the sensor-centric approach. One begins naturally enough by speculating about the nature of the threat, the attackers' mode of operation, their means and opportunity, their salient features in the moments before an attack at any time of day or night, under any weather conditions, and so forth. Many papers therefore include a developer's arm-chair threat analysis in the introduction (much as we did here). And then one matches sensors to detect those threats under various conditions, in this way very quickly generating a long list of threat-sensor-environment combinations. The sensor-centric approach therefore originates in threat analysis.

Threat analysis has proven itself many times, especially for military development, and especially during the Cold War in which the threat was relatively clear, and where matching the threat point by point was the basis of strategic deterrence. The (asymmetric) terrorist threat by comparison is hardly defined at all. The mode of attack cannot be predicted with former certainties except to say that it will, until its final moments, probably blend in with legitimate civilian activity in the area. The degree of uncertainty now about the threat may be among the more important transformations in the military. It may also be among the more longstanding distinctions between military combat and civilian security, with implications for port protection. Among developers, the threat is limited only by the inventiveness of the imagination. Scenario after scenario is typically made up, each calling for ever more vigilance, and more sensors.

Although threat analysis properly motivates new technology, the asymmetric threat, because of its uncertainty, fails to impose the former unity and clarity on the design process—on the long series of design decisions, tradeoffs and exclusions, which must inevitably be made at many points throughout a design. After the threat analysis stage, one typically begins by reducing the set of threats addressed, reducing the problem space, that is, if only because one must begin with a well-defined bounded design problem to solve. The reduction amounts to a set of assumptions made reluctantly about the threat, but necessarily, because the problem is otherwise too large. These assumptions enable the generation of system requirements on which the design of the new system is based. Design priorities, tradeoffs, and exclusions, for instance, are justified and decided with these requirements in view.

The nature of the threat is in principle unknown and therefore remains the subject of continual debate and speculation among expert analysts, but especially among developers. In the developer's domain, system-determining decisions stand with no more (or less) force than the principles by which they were settled. Insofar as these stem from a threat analysis, they are, like threat analysis, uncertain and endlessly debatable. At times, in order to keep to a given design track, one repeatedly invokes the initial assumptions, almost dogmatically, much more for the sake of the project budget, that is, than for objective deductions drawn from a threat analysis. This engenders arbitrariness in the system design. It also undermines consensus and acceptance throughout.

The need for scope reduction cannot be disputed, especially in the face of limited resources. The capability-based approach also reduces the project scope, as we shall see, perhaps more dramatically than the sensor-centric approach. The reduction is likewise made for pragmatic reasons, though for

reasons of a different kind, which can be much more compelling.

CAPABILITY-BASED INTEGRATION

As pointed out earlier, the capability for proactive protection when a threat materializes requires that surveillance be matched with response. Thus capability exists only insofar as both surveillance and response are simultaneously feasible and sustainable. Other modes of security than proactive protection are possible, such as using surveillance alone for deterrence through apparent show of vigilance, or for investigation and prosecution *after* an attack has taken place, but these are not the modes envisioned by those providing underwater security. Granted, then, that the main purpose of the underwater protection system is to intervene proactively, to stop an attack during the moments before harm is done, it follows 1) that any sensor unmatched with a plausible form of response, because it does not contribute to capability, is useless; and that 2) response has drivers and constraints that exert no less force on the system design than the threat characteristics do.

One example from underwater surveillance may be the sensor *trip wire* that is often proposed. The trip wire is a line of sensors that detects an intruder crossing the line, but typically provides little or no tracking of the intruder. It is often misnamed a *sensor barrier* that ostensibly serves as an outer layer of *defence*. If such as sensor is to be considered for integration for capability against underwater intruders, then one must first come up with a plausible story-line of response to such a detection, linking the cause-and-effect chain of events by which protection against the intruder is achieved. A plausible story line for response may in fact exist, but it apparently remains to be written. Until then response provides a principle for excluding the trip-wire, and it does so for the most part independently from the kind of sensors used in the trip wire or the threat properties one hopes to detect with it. Thus it imposes a significant, very pragmatic reduction in the scope of a project, at least so far as the long list of sensor options is concerned.

When a clear story line of response—detection, tracking, classifying, and prosecution, for instance—is imposed, it is likely that many sensors now being proposed as layered defence and barriers may be orphaned, remaining without adoption because their case cannot be made. Their justification through "what-if" threat scenarios is undermined, not because the scenarios can be dismissed, or because sensors are not feasible, but because the response is not feasible. Response may call for unsustainable readiness for instance. It may call for nothing short of rapid automated targeting, making the security system a more immediate threat than the threat of attack. Or it may fall outside the mandate or purview of the security forces with jurisdiction in the harbour, making the supporting sensors superfluous.

CONCLUSIONS

The difference in strength of the two anchoring concepts during the design process can be explained as follows. Where the sensor-centric approach is founded largely on the nature of the threat, which is in principle uncertain owing to the uncertainty about the threat, the capability-based approach can be founded largely on the response, which is in principle much more certain because it consists in effect of one's own actions, and it depends on one's own resources and resolve. The response is in principle knowable because it is a matter of self knowledge. At the same time it is no less a constraint or driver than the threat in proactive protection.

If capability depends on response, then it will be necessary to define what response entails. This can be difficult. In many cases the response may be classified in its details, which may be why response is expressly separated from surveillance at times. In other cases, the response remains to be defined inasmuch as the security mission is new, or new to a particular agency. What can generally be said about response is the following.

Given that one is providing proactive protection to counter an attack, and given that one is using surveillance (and therefore response) to do it, it is likely that response will be characterized above all by the rules of *self defence*, namely, by a duty to warn, a duty to prove intent, and a duty to use proportional force. These may be the dominant themes in the story line of surveillance and response. They can go a long way towards shaping a system design. Beyond these generalities, however, one must become acquainted with the user agencies, military or civilian, and their mandate, their likely rules of engagement, resources, technological skills, and so forth.

Both anchoring concepts enforce a pragmatic reduction of scope and direction throughout a project, but with a productive force that corresponds to the uncertainties faced by their perspectives. The sensor-centric takes its perspective from the uncertainties of the nature of the threat. The capability-based counters that uncertainty by with the perspective of plausible means of response. The effect on the design process, and on the design culture, can be dramatic, making the difference between ad hoc and purposeful capability, substance and fashion, integration and fragmentation, consensus and endless debate. As technology readiness emerges now from development into operations, through the integration of systems, a capability-based concept becomes absolutely necessary, to guide the system design and for the product to win acceptance. A strong concept is an asset for development and marketing alike. More generally, the role of anchoring concepts must not be overlooked in a campaign of development.

REFERENCES

[1] T. Akal, T. Tubitak, and F.B. Jensen, "Underwater acoustics for harbour protection and littoral security", Proc. of the IEEE International Conference on Technologies for Homeland Security and Safety, TEHOSS2005, Gdansk, Poland, 28-30 Sept 2005.

[2] T. Akal, K., Koprulu, P.Guerrini, and P. Roux, "Surveillance and protection of underwater Archaeological sites 'Sea-Guard'", Proceedings of the IEEE International Conference on Technologies for Homeland Security and Safety (TEHOSS2006), Istanbul, Turkey, 9-13 Oct 2006, pp. 169 - 178.

[3] D. Alberts and R. Hayes, "Campaigns of Experimentation: Pathways to Innovation and Transformation", CCRP Publication Series, 2005

[4] M.E. Anderson, "Underwater security garners more cash and new technologies", Government Security News, www.gsnmagazine.com/may_05/underwater_security.html, May 2005.

[5] M. Audenino, "SOBCAH – Surveillance of Borders, Coastlines and Harbours", Presented at the Joint Workshop of the European Security Research Advisory Board (ESRAB) Working Group on Boarder Security, Ispra, 30-31 March 2006.

[6] E. Basaran, S. Aksoy, and Y. Bahadirlar, "Time Domain Signal Analysis of Diver Attack Scenarios for Harbour Security", Proceedings of the 2nd IEEE International Conference on Technologies for Homeland Security and Safety (TEHOSS2006), Istanbul, Turkey, 9-13 Oct 2006, pp. 161-168

[7] E. Basaran, O. Livvarcin, and N. Yildirim, "Standardization of Harbour Protection Surveillance and Protection Systems", Proceedings of the 2nd IEEE International Conference on Technologies for Homeland Security and Safety (TEHOSS2006), Istanbul, Turkey, 9-13 Oct 2006, pp. 153-160.

[8] F. Cavagnaro, Editor, *Study Report on NATO integrated harbour barrier system (NIHBS), Final Report,* NATO Industrial Advisory Group (NIAG) SG.86, NIAG-D(2006)0006, AC/141(NG/3)D(2006)0001, 17 Feb. 2006 (NATO Unclassified)

[9] X. Chen, R. Wang, and U. Tureli, "Passive acoustic detection of divers under strong interference", Proceedings of the IEEE Oceans 2006, Boston, 18-21 Sept 2006.

[10] P. Clarke, "Swimmer Detection", Special Operations Technology, Online Edition, www.special-operations-technology.com, Vol. 3, Issue 6, Sept 12 2005.

[11] J. Demkowicz, K. Bikonis, A. Chybicki, A. Stepnowski, and A. Rucinnski, "Coastal zone critical infrastructure protection using dedicated geographical information system", Proceedings of the 2nd IEEE International Conference on Technologies for Homeland Security and Safety (TEHOSS2006), Istanbul, Turkey, 9-13 Oct 2006, pp. 129-136.

[12] P.F. Drucker, "The Essential Drucker", HarperCollins, New York, 2005.

[13] J.T. Dobkowski, "Polish Integrated MultisensorSystem for Underwater Situation Monitoring", OBP Centrum Technik Morskiej (CTM) (R&D Marine Technology Centre), Gdynia, Poland, Slides sent to NURC, R. Kessel, 14 Sept 2005.

[14] S. Dunham, "Defending the Fleet in Harbour – Stevens Tech Studies Navy Antiterrorism and Force Protection Measures", HIS Journal of Homeland Security, www.homelandsecurity.org/newhournal/Articles/display/Article2.asp?article=112, April 2004.

[15] European Communities, "Meeting the Challenge: the European Security Research Agenda", European Security Research Advisory Board (ESRAB), Luxemburg, September 2006

[16] European Communities, "Research for a Secure Europe", Report of the Group of Personalities in the field of Security Research, Luxemburg 2004

[17] A. Falcone, "Harbour Protection trials 2006 (HPT06): Description", R.Kessel Editor, Proceedings of the NATO Undersea Research Centre Workshop on Underwater Intruder Detection, NURC-CP-2006-002, La Spezia 27-28 Feb 2006 (NATO Unclassified; Not for Public Release).

[18] V. Farinetti and E. Rossotto, "Detection and Identification of Non-Authorised Underwater Vehicles in "Acoustically Cluttered Areas (Ports and Harbours)", Presented at the Joint Workshop of the European Security Research Advisory Board (ESRAB) Working Group on Boarder Security, Ispra, 30-31 March 2006.

[19] J. Feirerlein, "A general approach to cost effective sea and harbour surveillance systems", IBCOL Technical Services GmbH, Munich, Slides presented at the IEEE International Conference on Technologies for Homeland Security and Safety (TEHOSS2005), Gdansk, Poland, 28-30 Sept 2005

[20] A. Gabellone, "Caiman Experiment", Proceedings of the NURC Workshop on Underwater Intruder Detection, La Spezia, 27-28 Feb 2006.

[21] G. Gilbert, "When sonar isn't enough: Marine optics for port security", Course Notes, SPIE Short Course, Homeland Defence and Security Symposium, Orlando, April 2005.

[22] H. Guthmuller, "Naval Coastal Warfare Integrated Anti-Diver System", R.Kessel Editor, Proceedings of the NATO Undersea Research Centre Workshop on Underwater Intruder Detection, NURC-CP-2006-002, La Spezia 27-28 Feb 2006 (NATO Unclassified; Not for Public Release).

[23] R. D. Hollett, R. T. Kessel and M. Pinto, "At-sea measurements of diver target strengths at 100 KHz: Measurement technique and first results", Proceedings of UDT Europe 2006, Hamburg, Germany, 27-29 June 2006.

[24] B. Houston, J. Bucaro, and T. Yoder, "Acoustic Monitoring of Underwater Harbour Threats", R.Kessel Editor, Proceedings of the NATO Undersea Research Centre Workshop on Underwater Intruder Detection, NURC-CP-2006-002, La Spezia 27-28 Feb 2006 (NATO Unclassified).

[25] R. Katulski, R. Niski, J. Stefanski, and J. Zurek, "Areas of research in maritime security", Proceedings of the 2nd IEEE International Conference on Technologies for Homeland Security and Safety (TEHOSS2006), Istanbul, Turkey, 9-13 Oct 2006, pp. 145-152.

[26] R. Katulski, J. Stefanski, R. Niski, A. Rucinski, and J. Zurek, "Infrastructure vulnerability analysis of a port container terminal, Proceedings of the 2nd IEEE International Conference on Technologies for Homeland Security and Safety (TEHOSS2006), Istanbul, Turkey Oct 2006, pp. 137-144A.

[27] R.T. Kessel and R.D. Hollett, "Underwater Intruder Detection Sonar for Harbour Protection: State of the Art Review and Implications", Proceedings of the IEEE International Conference on Technologies for Homeland Security and Safety (TEHOSS2006), Istanbul, Turkey, 9-13 Oct 2006, pp. 207-215.

[28] R.T. Kessel and R.D.Hollett, "Force Protection in Ports: integrated surveillance and response against underwater intruders", Proceedings of NATO RTO System Concept and Integration Panel, Symposium on Force Protection in the Littorals, Ottawa, Canada, Sept 2006 (NATO Unclassified).

[29] D. Hopkin, "Underwater Intruders and Port Protection: A Canadian Perspective", R.Kessel Editor, Proceedings of the NATO Undersea Research Centre Workshop on Underwater Intruder Detection, NURC-CP-2006-002, La Spezia 27-28 Feb 2006 (NATO Unclassified).

[30] M. Keil and R. De La Croix, "Security: Stopping the Diver, Undersea Threat", Maritime Technology Reporter, October 2006, pp. 38 – 42.

[31] W. Kuperman, "Performance of a high-frequency acoustic forward-scatter barrier in dynamic coastal environment," Presented at the 2nd IEEE International Conference on Technologies for Homeland Security and Safety (TEHOSS2006), Istanbul, Turkey, 9-13 Oct 2006.

[32] W. Kuperman, K. Sabra, P. Roux, M. Stevenson, A. Tessei, T. Akal, P. Guerrini , P. Boni, , "Performance of a high-frequency acoustic forward-scatter barrier in dynamic coastal environment", Presented at the 2nd IEEE International Conference on Technologies for Homeland Security and Safety (TEHOSS2006), Istanbul, Turkey, Oct 2006

[33] F. Maeda, K. Kuramoto, Y. Kawashima, and K. Hantani, "Development Status of a Wharf Security System", Presented at the 2nd IEEE International Conference on Technologies for Homeland Security and Safety (TEHOSS2006), Istanbul, Turkey, 9-13 Oct 2006.

[34] S-Y Lee, S-T Moon, and D-Y Kim, "Integrated Waterside Security System", Proceedings of the 2nd IEEE International Conference on Technologies for Homeland Security and Safety (TEHOSS2006), Istanbul, Turkey, 9-13 Oct 2006, pp.101-109.

[35] S.T. Makrinos, United States Port Security in the War on Terrorism: Employing commercial off-the-shelf and emerging technologies to extend the security zone around US ports", Sea Technology, March 2004, p.p. 33-34

[36] L. McDonald and R. O'Sullivan, "Integrated Harbour Security System Enhances Port Protection", Sea Technology, March 2004, p.p. 27-30.

[37] T. Meurling, D. Suchman, and M. Baldwin, "An integrated approach to Underwater Intruder Detection", Proceedings of UDT Pacific, 6-8 Dec 2006

[38] S. Michell, "Industry rises to the challenge of increased maritime security threats, Jane's International Defence Review", Jan 2007, pp. 34-39.

[39] O. Radu and L. Cosereanu, "Harbour Protectoin Against Terrorist Threats: Difficulties and Possible Solutions", Proceedings of the NATO RTO System Concept and Integration (SCI) panel symposium on Force Protection in the Littorals, Ottawa, Sept 2006.

[40] K.W. Rehn and P.K. Riggs, "Non-Lethal Swimmer Neutralization Study", Applied Research Laboratories, University of Texas at Austin, Technical Document 3138, May 2002.

[41] M. Richardson, "A time bomb for global trade: Maritime--related terrorism in an age of weapons of mass destruction, VIEWPOINTS, Institute of South East Asian Studies, Singapore, 25 Feb 2004.

[42] E. Rust, "The Economic Benefits of Ports and Harbours in the United States", Sea Technology, 2004, pp. 20 – 25.

[43] R. Schaefer and M Grapperhaus, "Nonlethal unfriendly swimmer and pipe defence combining sound and flash pulses using a new sparker", Proceedings of the SPIE, Volume 6204, Photonics for Port and Harbor Security II, May 2006.

[44] K. Shaw, R. Scott, and G. Holdanowicz, Sonar sentinels on guard for submerged swimmers, Jane's Navy International, Oct 2005, pp.10-18.

[45] G. Shwaery, "Incorporating non-lethal technologies into port security capabilities", Proceedings of the 2nd IEEE International Conference on Technologies for Homeland Security and Safety (TEHOSS2006), Istanbul, Turkey, 9-13 Oct 2006, pp. 191-197

[46] R. Stolkin, A. Sutin, S. Radhakrishnan, M. Bruno, B. Fullerton, and M. Raftery, "Feature-based passive acoustic detection of a diver", Proceedings of the SPIE, Volume 6204, Photonics for Port and Harbor Security II, May 2006.

[47] D. Suchman, "Harbour Surveillance 101: Basic Do's and Don'ts of Designing, Installing, and Operating a Harbour Protection System", A. Tuncay et al. Editors, Proceedings of the Turkish International Conference on Acoustics 2005, new Concepts for Harbour Protection, Littoral Security, and Underwater Communications, Istanbul, 4-8 July 2005.

[48] J. Traxl, "100 KHz Intruder Detection Sonar Trials at Kiel Naval Base, August 2003", R.T.Kessel Editor, Proc. of NURC Underwater Intruder Detection Workshop, La Spezia, 27-28 Feb 2006.

[49] M. S. Twardowski, R. V. Zaneveld, C. C. Moore, J. L. Mueller, C. C. Trees, and O. Schofield, "Diver visibility measured with a compact scattering-attenuation meter", Proceedings of the SPIE, Volume 5780, Photonics for Port and Harbor Security, April 2005.

[50] G. Vettori, "Harbour Protection System Approach Against Terrorist Attacks", R.Kessel Editor, Proceedings of the NATO Undersea Research Centre Workshop on Underwater Intruder Detection, NURC-CP-2006-002, La Spezia 27-28 Feb 2006 (NATO Unclassified).

[51] R. Walker, "Coast Guard's Underwater Port Security R&T", Proceedings of the 7th Marine Transportation System Research & Technology Coordination Conference, The National Academy of Sciences, Washington, DC, 16-17 November 2004.

[52] C. Weber, Focus Report: Maritime Terrorist Threat, New York State Office of Homeland Security, New York, 21 Feb 2006.

[53] D. Weidemann and G. R. Fournier "In harbor underwater threat detection/identification using active imaging", Proceedings of the SPIE, Volume 5780, Photonics for Port and Harbor Security, April 2005.

Document Data Sheet

Security Classification		Project No.
Document Serial No.	**Date of Issue**	**Total Pages**
NURC-PR-2007-005	October 2007	9 pp.

Author(s)

Kessel, R.T.

Title

Protection in ports: countering underwater intruders.

Abstract

.

Keywords

Issuing Organization

NURC
Viale San Bartolomeo 400, 19126 La Spezia, Italy

[From N. America:
NURC
(New York) APO AE 09613-5000]

Tel: +39 0187 527 361
Fax:+39 0187 527 700

E-mail: library@nurc.nato.int