NATO Undersea Research Centre
Centre de Recherche Sous-Marine de l'OTAN

Reprint Series **NURC-PR-2006-027**

Underwater Intruder Detection Sonar for Harbour Protection: State of the Art Review and Implications

Ronald T. Kessel, Reginald D. Hollett

October 2006

Originally presented at:

The Second IEEE International Conference on Technologies for Homeland Security and Safety, Istanbul, Turkey 9-13 October 2006

NATO Undersea Research Centre (NURC)

NURC conducts world class maritime research in support of NATO's operational and transformational requirements. Reporting to the Supreme Allied Commander Transformation, the Centre maintains extensive partnering to expand its research output, promote maritime innovation and foster more rapid implementation of research products.

The Scientific Programme of Work (SPOW) is the core of the Centre's activities and is organized into four Research Thrust Areas:

- Expeditionary Mine Countermeasures (MCM) and Port Protection (EMP)
- Reconnaissance, Surveillance and Undersea Networks (RSN)
- Expeditionary Operations Support (EOS)
- Command and Operational Support (COS)

NURC also provides services to other sponsors through the Supplementary Work Program (SWP). These activities are undertaken to accelerate implementation of new military capabilities for NATO and the Nations, to provide assistance to the Nations, and to ensure that the Centre's maritime capabilities are sustained in a fully productive and economic manner. Examples of supplementary work include ship chartering, military experimentation, collaborative work with or services to Nations and industry.

NURC's plans and operations are extensively and regularly reviewed by outside bodies including peer review of the research, independent national expert oversight, review of proposed deliverables by military user authorities, and independent business process certification. The Scientific Committee of National Representatives, membership of which is open to all NATO nations, provides scientific guidance to the Centre and the Supreme Allied Commander Transformation.

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 are encouraged to cite the original article where possible.

UNDERWATER INTRUDER DETECTION SONAR FOR HARBOUR PROTECTION: STATE OF THE ART REVIEW AND IMPLICATIONS

RONALD T KESSEL AND REGINALD D. HOLLETT

NATO Undersea Research Centre (NURC), Viale San Bartolomeo 400, La Spezia (SP) 19138, Italy

E-mail: Kessel@nurc.nato.int, Hollett@nurc.nato.int

Sonar is the sensor of choice for wide-area underwater surveillance because sonar (based on sound waves) typically provides a much larger area of coverage than radar (electromagnetic waves) or video (visible light) can provide under water. Of particular interest of late is sonar for detecting and tracking underwater intruders in harbours, to provide an element of protection for ships, harbour infrastructure, nuclear power plants, and so forth, against terrorist attacks carried out from underwater. Sonar has long been used for detection and tracking by the military, but the application against intruders is relatively new as the mandate of civilian security agencies and the military expands now to include protection against terrorist attacks and counter terrorism. This paper reports the general results of a survey of commercial sonar systems (not including system-by-system rankings or detailed matters of procurement), as well their validation in part through sea trials and modeling, and on factors relevant to their use as a component in harbour protection.

1 Introduction

NATO enters into harbour protection for both military and civilian applications because of initiatives taken by the Conference of National Armaments Directors (CNAD), a senior NATO body who made protecting harbours and ships the second of ten priorities for technological advance in the Defence Against Terrorism (DAT) [1]. A program of technological development followed, including a new harbour protection project (start May 2005) at the NATO Undersea Research Centre (NURC); NATO-sponsored Harbour Protection Trials 2006 (HPT06) hosted by the Italian Navy (La Spezia, April 2006) with NURC leading the analysis [2]; and a NATO Industrial Advisory Group (NIAG) report on "harbour barrier systems" [3]. NURC's harbour protection team has since conducted trials [4] and a workshop on underwater intruder detection [5]. There are of course other projects in harbour protection in NATO member countries apart from the CNAD initiative.

The underwater threat is one part of the terrorist threat to maritime activities [6]. The underwater domain presents significant challenges to the attacker and defender alike. For the attacker, under water visibility is likely to be poor and a compass for navigation is likely to be confused by harbour junk, so an underwater intruder will probably be forced

to surface periodically to take visual bearings toward his or her target. Physical fitness will be required to swim some distance carrying or towing a weapon (explosives presumably). An underwater propulsion vehicle is likely for weapons of any significant size or weight, but the know-how to use and navigate with it is required. The effectiveness of explosives underwater is different than in air, requiring specialized knowledge for effectiveness. Unmanned vehicles might be used to deliver explosives, but these also have payload and power limits, as well as navigation issues, which could no doubt be worked out by a capable attacker, but the risk of betraying oneself before an attack, or of betraying one's support afterward, increases with technical complexity owing to the specialized purchases, training, practice runs, and so forth, typically required, making unmanned vehicles an unlikely first choice for attack, but a matter of concern nonetheless.

For security forces, the area under surveillance in a harbour is relatively small (on the order of several kilometers, the size of the body of water in the harbour), but visual and aural cues are nevertheless of little use for detecting submerged attackers. One must rely almost entirely on sophisticated technology for surveillance. There is the risk, moreover, of mistaking innocent intrusions (sport divers, treasure hunters, equipment salvagers, boat owners doing maintenance, vacationing tourists) as threats, so care must be taken: security forces would presumably be obliged to

1. unambiguously identify attackers before using lethal force,
2. consider non-lethal means for deterrence and interception,
3. give contacts unambiguous warning and means to prove benign intent.

These challenges imply that one would ideally block all underwater access to the protected assets using physical barriers—floating booms from which underwater nets are hung—in this way clearly marking an exclusion zone above and below the water, blocking innocent intrusions while also justifying prompt lethal action against any intruders who force entry into the zone. Some subject matter experts have suggested that short-range sensors may be added to the underwater nets to detect breaks or the proximity of a diver. Nets clearly go a long way toward protection and deterrence, but they are not always feasible. The drawbacks are the disruption they can cause to legitimate traffic, their bulky size and weight (especially for self protection of naval forces in foreign ports [3]), the time and space required to deploy, recover, and store, and their maintenance. In some cases partial barriers may be beneficial, to produce a narrow "choke point" where underwater surveillance can be concentrated to good effect.

To rely solely on nets, however, falls short of counter terrorism proper, which is not just protection against attack, but also the awareness and supportive stance for the investigation, prosecution, and disruption of terrorism. One ought to know, for instance, of any failed or aborted attacks, which may not be evident if they occur when using nets alone. One should also know of any precursors of attack, such as a terrorist practice run, the placement of a time-delayed or remotely controlled explosive, the test or assay of security measures, a switch to a new mode of operation, and so forth. This is part of the underwater domain awareness that area surveillance provides whether nets are used or

not. At the same time, surveillance on its own does not amount to protection: it must be combined with plausible means of response against suspicious contacts to provide capability against underwater intruders. One should therefore consider combining surveillance with the blocking force of nets and with the means for effective interdiction.

2 Sonar for underwater intruders

Sonar gives by far the lowest cost per square meter of underwater coverage of all other means of surveillance (radar, video, visual). This is because sound waves have a low attenuation and long propagation distance in turbid harbour waters relative to other means of sensing (electromagnetic waves, visual light, temperature, magnetism). The leading sonar technology for detecting and tracking underwater intruders is active, monostatic sonar, using principles of conventional beam forming in its signal processing. Typical technical specifications for these sonars are given in Table (1). "Leading" here means that these sonars are now available from a number of different manufacturers who confidently recommend their use for surveillance against underwater intruders, whereas, other sonar technologies, such as active multi-static or passive sonar, possibly with model-based signal processing, remain at best in the development stage so far as intruder detection is concerned. The leading technology is nevertheless new, especially in its application against intruders in harbour protection, so its review is warranted.

Active monostatic sonar consists of an acoustic transmitter and receiver that are co-located. The transmitter sends a brief energetic sound pulse into the water, the pulse propagates and reflects from objects in the water, and these echoes propagate back to the receiver. An energetic echo indicates the presence of the object, while the time of round-trip propagation, from first transmission to the reception of the echo, indicates the distance (range) to the reflecting object. The transmitter and receiver are typically composed of many small transmitters and receivers arranged in arrays. These arrays allow the sound to be preferentially transmitted and sensed along narrow beams using well-known techniques of *beamforming* [7]. Beamforming allows one to determine the compass bearing of the reflective object (intruder) relative to the sonar. When the echo strength is plotted as a function of range and bearing the result is an *echograph*—a plan view of the coverage area showing the position of reflective objects underwater.

The sonar typically presents the operator with a navigation chart of the area under surveillance on which the echograph may be displayed in overlay, as shown in Fig.(1). The position of objects with strong echoes is immediately evident from the echograph. The echograph is refreshed with every transmission (ping) of the sonar, typically on the order of once or twice a second. An intruder would appear as a small moving "blob" of energetic echo in the echograph, and the operator could judge whether the contact is a threat that calls for further action from its speed, heading, track, and possibly from a trail of persistent, regularly spaced, exhaled bubble clouds. The operator can typically zoom into the echograph overlay for closer inspection as desired, but, in the absence of an obvious trail of exhaled bubble clouds, the physical resolution of the sonar is insufficient to make a conclusive classification.

Unfortunately the echograph fluctuates randomly and noticeably from ping to ping, even in regions where there are no moving sonar contacts. An intruder appears visually then as a small fluctuating “blob” against a fluctuating background of sound clutter and reverberation, making it difficult to visually detect intruders, especially if more than one intruder can be expected. Fortunately this is something that automation can do more reliably than humans for many contacts at once. Automated detection and tracking is therefore a feature of all commercially available systems. Reliance on automation means that the sonar display can be simplified if the operator wishes, by optionally suppressing the echograph and displaying only the chart and the detection and tracking symbology automatically generated and displayed by the sonar system. This is the mode most often recommended by sonar manufacturers because it significantly reduces the demand on the operator.

Sonar Parameter	**Manufacturer’s Specifications**	**Remarks**
vertical transmit beam	• 3.5 to 24 degrees wide • -24 to +24 degrees tilt	Electronically adjustable width & tilt on some models
horizontal transmit beam	• 30 to 360 degrees wide	Some models require multiple sonar heads for 360 degree coverage
Transmit pulse	• Continuous wave, frequency modulated • 3 ms to 100 ms long • 80 KHz to 300 KHz centre frequency • 200 to 220 dB re 1μPa at 1 m	All adjustable on some models
sonar resolution	• m to 1.0 m in range • 0.25 to 2.0 degrees bearing	
Detection Range	• 150 m to 800 m	For diver with open-circuit breathing equipment
Automation	• Auto detection and tracking • Track management tools • Adjustable sensitivity	Necessary in practice for unalerted detections

Table 1. Nominal intruder detection sonar specifications

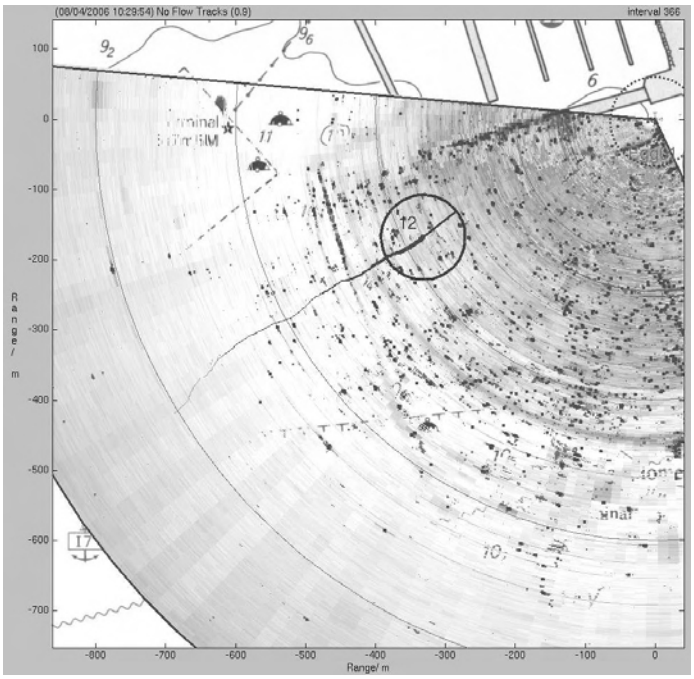


Figure 1. Example (QinetiQ's Cerberus system) of an echograph overlay on chart view near La Spezia. A single intruder is automatically detected and tracked starting in this case at a range of about 800 m from the sonar. A boat wake can be seen near the intruder.

3 State of the art

NURC staged trials[1] and participated in the demonstration of several different models of sonar diver detection sonar from different manufacturers[2]. Intruders were simulated by military divers (Italian Navy) wearing either open-circuit or closed-circuit breathing equipment. They typically followed predetermined tracks that followed straight-line approaches toward or past the sonar, with no intention of being either particularly easy or difficult for detection. The sonar deployment, the staged intrusions, and the times and weather conditions of the demonstrations were furthermore chosen for realism and convenience, not for reasons that would knowingly have affected normal sonar performance. The demonstrations were unbiased in these respects but they fall short of performance evaluation because the number of samples—simulated intruders and deployment sites—although respectable, was too small for quantitative performance

[1] Two trials, May 05 and Apr 06, focusing on diver detection: target strength measurements, technology validation, and detection range. Report from Apr 06 trials due later in 2006.

[2] NATO's Harbour Protection Trials 2006 (HPT06) 3-7 April 2006, La Spezia.

results. The trials were instead a technology validation of sorts, with the observations made under realistic conditions by independent experts. This validation provides background for knowledgeable procurement and for operational planning, but it stops far short of completeness for either.

It was found that intruder detection sonar technology is mature inasmuch as:

1. It has demonstrated 360 degree coverage with detection ranges of 300 to 800 m against intruders wearing open-circuit breathing equipment. The coverage is significant relative to the area of open water and to the possible entry points for intruders in many harbours.
2. Reduced detection range and track fragmentation, when it occurred, could be accounted for by environmental (sound propagation) conditions at the time (see below).
3. Random false alarms are rare (when the auto-detection properly adjusted), and they are recognizably false because they are of short duration and do not follow a track.
4. Non-random false alarms caused by genuine underwater contacts that happened not to be intruders—by large fish, or schools of fish, or marine mammals, for instance—can usually be recognized by an experienced operator from the contact's behaviour, especially the evolution of their track, so these "false" alarms are unlikely to be troublesome in practice. They furthermore provide feedback about the functioning of the sonar and domain awareness.
5. The automatic algorithms are capable of detecting and tracking many contacts simultaneously.

On the negative side, as with sonar generally, one finds that performance—in this case, intruder detection range and track continuity—depends on the oceanographic conditions in the harbour. Variations in detection range of a few hundred meters have been observed from one day to the next in La Spezia harbour for instance, and track fragmentation is much more the rule than the exception for long tracks (several hundred meters, say). Track fragmentation can sometimes make a genuine intruder appear to be a false alarm to the operator, reducing in effect the probability of detection in practice. It can also hamper the response against an intruder if its position is lost for a time.

The main cause for the variation in performance follows a chain of cause and effect [7]:

1. sea water naturally stratifies into layers of differing salinity and temperature;
2. variations of salinity and temperature produce corresponding variations with depth in sound speed;
3. variations in sound speed have a refractive lens effect on sound propagation over long ranges (distances much greater than the water depth), bending its propagation path vertically upwards or downwards, as shown in Fig.(2) for example; and

4. this refraction intensifies the transmitted sound in some places (where rays are close together), enhancing sonar performance, while weakening the sound in other places (where rays are far apart) degrading performance.

Acoustic shadowing can also occur near the sea surface and the sea floor due to their roughness; to the sea state above, that is, and to the geology and plant life below. The sea water stratification is weather and tide dependent, and can change dramatically from day to day, and from season to season, causing performance to vary accordingly, often significantly. It would appear (speculating only) that the manufacturers' reported detection ranges are typically under ideal conditions, with little vertical refraction (homogeneous body of water) and little surface or seafloor shadowing (calm sea and flat seafloor).

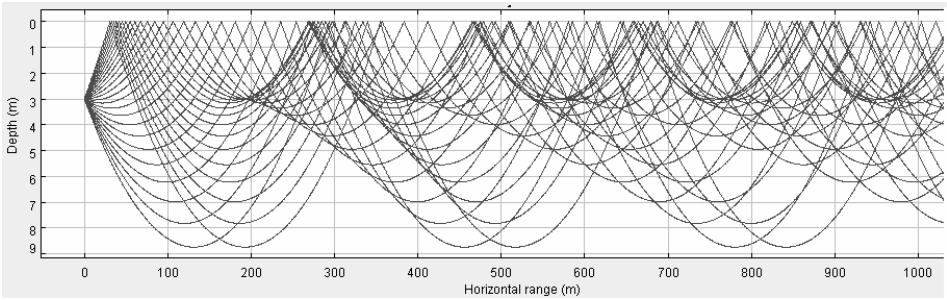


Figure 2. Example of refracted ray paths for sound transmitted by a sonar on the left (at 3 m depth and 0 m range). The water is upward refracting in this case, giving better detection and tracking against intruders near the surface (0 m depth) than near the sea floor 9 m depth. This illustrates one of many possibilities.

Mitigation of environmental variation is more a matter of technology use than of sonar design. Multiple sonars with overlapping coverage, for instance, may go a long way against environmental variability, with the strong coverage zones of one sonar filling in to some degree in the weak zones of another. The relevant oceanographic properties (sound speed as a function of water depth) can furthermore be measured and the resulting propagation effects modeled to make users aware of the conditions for the day. At least one manufacturer has included software tools for the purpose. The alert stance for the defence team, the security resources, and the activities in the harbour can be changed according to the conditions of the moment if necessary.

A sonar echo is the superposition of echoes from objects in the same vicinity. An energetic echo from an underwater object can therefore mask the echo of a nearby intruder, making it difficult to detect and track while the two are close together. This masking may occur near rock outcroppings, buoys, harbour junk, piers, and so forth. One reason for viewing the echograph is to identify where masking clutter is likely to be a problem.

One important cause of masking is the wake from small boats. A wake consists of micro bubbles that reflect sound and can persist for some time under water along the path followed by the boat. The defence force must take care not to screen contacts with its boat wake. As a wake evolves over time it can trigger false detection and tracks, but these are usually evident as false to the sonar operator, either because the boat generating the wake has been seen by the operator, or because the false detections and tracks overlay the straight path of the wake as seen in the sonar echograph. An intruder's track can also be seduced away from the genuine intruder to follow a boat wake for a time; the seduction being evident from inspection of the echograph, by a sudden change of direction in a track to follow a crossing wake. The seduced track typically ends shortly afterward with loss of true track, and resumes much like a new detection as the intruder leaves the vicinity of the wake.

Although the automatic detection and tracking algorithms work well, relieving the operator of the meticulous watch of the sonar echograph, the operator must nevertheless receive specialized training and support in several respects:

1. To understand the cause and effect of the environmental variations, and to make and use the sound-speed measurements to mitigate their impact.
2. To knowingly adjust the sensitivity of the automatic detection and tracking algorithms for the particular sonar at hand. The adjustment may require a known reference target (simulated intruder) against which the automatic detector and tracker can be optimally adjusted.
3. To develop and maintain the situation awareness required to discriminate non-intruder underwater contacts (fish, clutter, boat wakes) from genuine intruders, which would require competence with the echograph view of coverage.

4 Conclusions and future work

Intruder detection sonar is an important element in counter terrorism in ports and harbour. The state of the art was reviewed here. Its performance deficiencies—variable detection range and track fragmentation—are those affecting sonar generally inasmuch as they are due to environmental factors. These can be mitigated to some degree through environmental measurements and concepts of use, but they are unlikely to be completely overcome.

Two critical requirements for capability against underwater intruders are the need for rapid response against a contact after the moment of first detection and, the need to positively identify hostile intent to justify the use of appropriate force. Capability against underwater intruders furthermore means surveillance plus response. NURC is therefore advancing the concept of a semi-autonomous craft, vectored into strategic position relative to a suspicious contact by the intruder detection sonar, plus a sensor suite on board of the vehicle (e.g., a high-resolution acoustic camera) to reacquire, warn, and closely observe the contact before and while further actions are taken against it. The

work will, and already has, built on the participation of NATO member countries through joint efforts.

NURC is also processing data collected earlier in 2006 on intruder (diver) target strengths and their key determinants (tanks, equipment, suits, etc.) for characterizing the underwater threat for surveillance purposes. Not considered thus far are the detection and tracking performance against autonomous underwater vehicles.

References

1. "NATO Defence Against Terrorism (DAT) programme: Countering Terrorism with Technology", NATO website http://www.nato.int/issues/dat/in_practice.htm, 16-Nov-2005.
2. NATO Harbour Protection Trials 2006 (HPT06), La Spezia, Italy, 3-7 April 2006, NURC Analyst Report to appear 2006.
3. F. Cavagnaro, Editor, Study Report on NATO integrated harbour barrier system (NIHBS), Final Report, NATO Unclassified, NATO Industrial Advisory Group (NIAG) SG.86, NIAG-D(2006)0006, AC/141(NG/3)D(2006)0001, 17 Feb. 2006
4. R. D. Hollett, R. T. Kessel and M. Pinto, "At-sea measurements of diver target strengths at 100 KHz: Measurement technique and first results", to appear proceedings of UDT Europe 2006, Hamburg, Germany, 27-29 June 2006
5. R.T. Kessel, Editor, Proceedings of the Underwater Intruder Detection Workshop, NATO Unclassified, La Spezia, Italy, 27-28 Feb 2006, NURC CP-2006-002, June 2006.
6. C. Weber, Maritime Terrorist Threat: Focus Report, New York State Office of Homeland Security, New York, Feb 2006
7. R. J. Urick, Principles of underwater sound, McGraw-Hill, 3rd ed., 1983.

Document Data Sheet

Security Classification		Project No.
RELEASABLE TO THE PUBLIC		
Document Serial No.	**Date of Issue**	**Total Pages**
NURC-PR -2006-027	August 2006	12 pp.

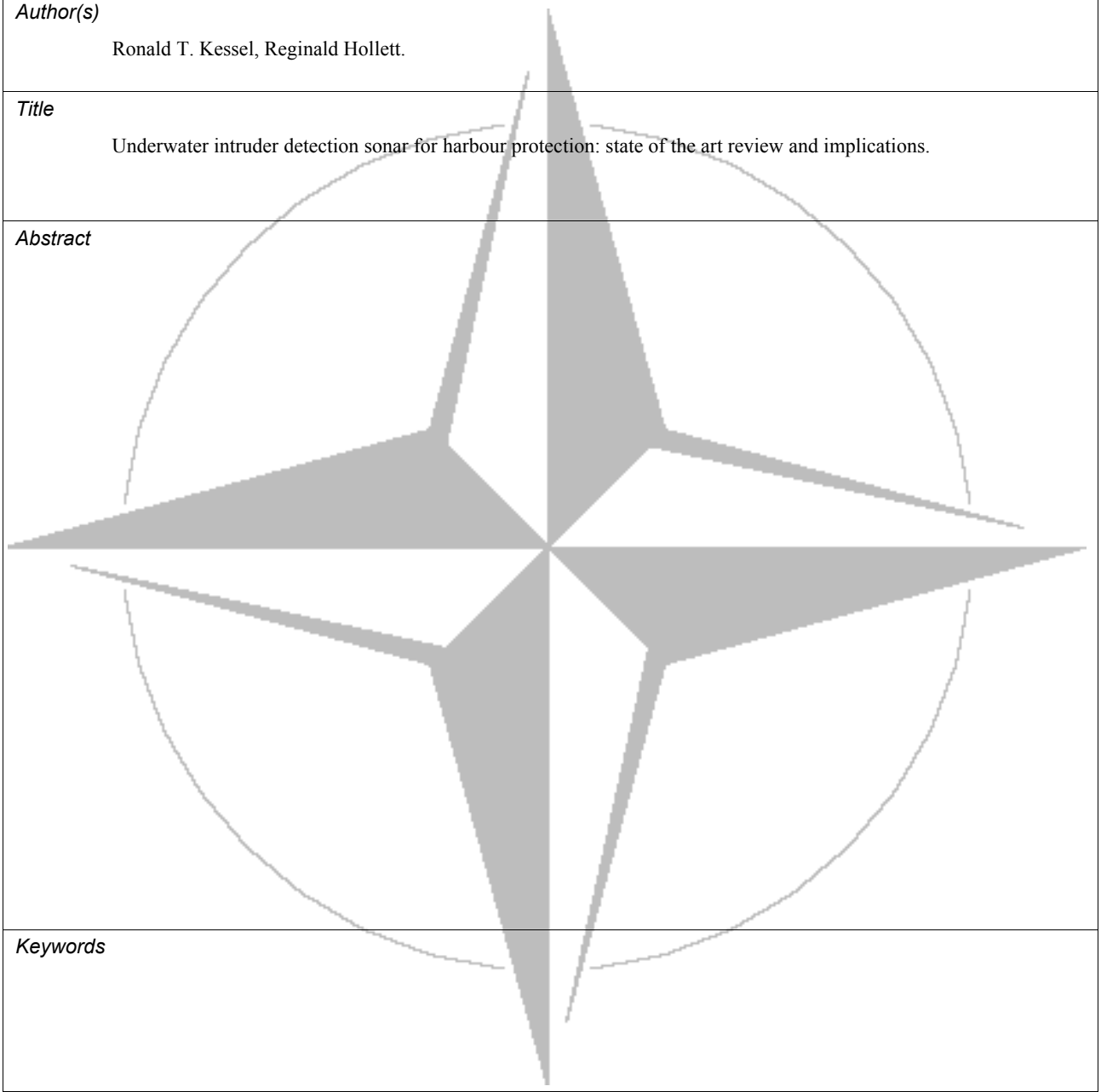
Author(s)

Ronald T. Kessel, Reginald Hollett.

Title

Underwater intruder detection sonar for harbour protection: state of the art review and implications.

Abstract



Keywords

Issuing Organization

NATO Undersea Research Centre
Viale San Bartolomeo 400, 19138 La Spezia, Italy

[From N. America:
NATO Undersea Research Centre
(New York) APO AE 09613-5000]

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

E-mail: library@nurc.nato.int