CONFERENCE REPORT

# Summary of the 2nd International Waterside Security Conference


## AUTHORS

**Ronald T. Kessel**
NATO Undersea Research Centre, La Spezia, Italy

**Julie Pullen**
Stevens Institute of Technology


The 2nd International Waterside Security Conference (WSS2010, held 3-5 November 2010 in Marina di Carrara, Italy) brought together 153 experts from 21 different countries to describe advances in maritime technologies and to stimulate cross-disciplinary thinking for new capabilities in

- port protection, counter-piracy, counter-terrorism;
- protection of critical infrastructure and high-profile events;
- Small boat monitoring and stopping;
- protection of ships and energy platforms;
- prevention of underwater intruders; and
- maritime interdiction, maritime surveillance, and information sharing.

The greatest benefit of WSS2010 is the broadening of perspective that comes from the collaboration of experts from many different dimensions of waterside security—the technologists, security providers, industry, serious gamers, and military. The cross-disciplinary insights change the development and transition of new technologies into operations from a matter of random chance into a matter of purposeful planning. The detailed conference agenda is available at http://www.wss2010.org/. Below we share highlights and summarize the conference.

The deployment of layered technology for port security emerged as a dominant theme. From active/passive acoustics and autonomous surface and underwater vehicles to surveillance cameras, radar, Automatic Identification System (AIS), and satellite feeds—all of these technologies contribute to an overall situation picture and cue for action. Sophisticated sensor suites were demonstrated in numerous port protection scenarios, especially those focused on military force protection. At the same time, however, the need for ubiquitous, low-cost, rapidly deployable sensors for homeland defense was also stressed, as both a driver and constraint on new technologies.

Sensor density and coverage overlap play important roles in defining capabilities in waterside security. In the approaches or the outer harbor, coverage overlap may occur in only a small fraction of the available area. In areas of dense traffic and many complementary sensors, on the other hand, operators may face a confusing overload of data. A comprehensive approach to fusion across air, surface, water column, and seabed is an important goal for effectively combining multisensor information.

In sensor deployment, it is increasingly recognized that most sensing modalities are impacted by environmental conditions. Acoustic sensing of underwater intruders can be degraded by temporal and spatial variations in salinity and temperature, wave state, bathymetry, harbor geometry, pier structures, and background noise (including natural sources, like snapping shrimp in tropical ports). Research presented in a special session at the conference quantified this kind of environmental variability in harbors throughout the world. The effects of environmental variability on underwater surveillance can be predicted and mitigated by technological innovations. One sonar developer (Sonardyne) explained how they provide system operators with an estimated detection range or "performance indicator" projected from local conditions. How environmental conditions shape sensor performance will remain an important topic as coverage areas and geographical diversity of operations increase.

Foremost among the drivers of security technology are current and emerging threats, which WSS2010 covered in depth along with the associated waterside vulnerabilities to those threats. "Expect the unexpected" became the rule for scenario planning. The importance of imaginative "red team" gaming in security exercises was also stressed.

With regard to vulnerabilities, electronic hardening of communications and sensor networks is imperative. This was judged to be a particularly important aspect of security so that a

system does not fail at the moment it is needed most.

Improvised explosive devices (IEDs) pose a significant threat in ports and berthing facilities, under piers, and attached to a ship below the water line. Vulnerability to underwater IEDs in shallow maritime environments is high, and IEDs are relatively cheap, making waterside assets attractive to attackers. As with bomb scares generally, even hoaxes can result in closures with significant economic impacts demanding effective action. Proactive measures consist of strictly enforced exclusion zones and close inspection of the underwater domain. Innovative hull-crawler technologies for high-resolution underwater imaging are being developed.

Some at WSS2010 warned against neglecting response measures in system design. The capacity to respond is in fact a determining factor in the design of a complete security system. The response to an attack as it unfolds must be rapid and adaptive to unimagined and unfamiliar modes of attack, and constant high readiness is required for any level of response (lethal or nonlethal) to a threat or attack. Response measures need to be scalable in time, effort, and coverage. They must be lawful (proportionate) and responsible (involving a human in the loop).

As managers of research projects in waterside security, we constantly look for coherent themes that illuminate the way ahead and enable building the consensus that large projects require. One theme emerging from both WSS2010 and WSS2008 (held in Copenhagen) is that waterside security increasingly demands diverse expertise ranging from technology to policy to business and, of course, to security. Continued change and diversity in the vision for waterside security are signs that a vigorous maturing process is underway for technologies and their concepts of use. Some that looked plausible 2 years ago have proved more imaginative than realistic and have met serious constraints from unforeseen domains—from business and economics; from law, policy, and regulations; and from other human factors. New technologies that have productively navigated all factors are rare. AIS may be one of the leading examples of success taken from maritime security in general, but even AIS has experienced growing pains as it continues to transition from its original safety objectives (anticollision) to security (anomaly detection). Some forms of container scanning, radar, sonar, and electro-optics may be examples of notable success for surveillance in waterside security. Elsewhere, the development, testing, and transition into use of new technologies continue on many different fronts.

It is generally recognized that the technical security measures implemented at the point of impact of a threat—namely, the surveillance and response measures applied during the moments of attack or entry—are partial solutions. As pointed out at WSS2010, for instance, the solution for piracy lies more in nation building in collapsed states than in capturing pirates in the act on the high seas; the solution to terrorism lies more in intelligence gathering than in the stopping force during the moment of attack; the solution to human trafficking may lie more in alleviating countries from destitution and civil strife than from capturing boatloads of people along the coast. There are perhaps no threats that could not be significantly mitigated by sociopolitical solutions in these ways. This has a "capping" effect on the drivers for new measures in waterside security. Where there is a lack of political will, however (witness Somalia), the transition to a more serious, permanent state of security and increased motivation toward sustainable measures and new technologies is inevitable.

From Copenhagen in 2008 and Carrara in 2010, WSS2012 moves next to one of the largest maritime centers of the world, Singapore, to further advance these important topics, address emerging ones, and further stimulate a multidisciplinary approach.

## Authors:

Ronald T. Kessel
NATO Undersea Research Center
Email: kessel@nurc.nato.int

Julie Pullen
Stevens Institute of Technology
Email: julie.pullen@stevens.edu