Mobile Ad Hoc Network of Waterborne Sensors for Enhanced Maritime Security

Nathan Whittenton and Thomas Berger
L-3 PHOTONICS
Carlsbad, USA
Nathan.Whittenton@L-3com.com

***Abstract*—Recent advances in mobile networking capabilities and unmanned technologies, together with improved availability, has provided an opportunity for cost efficient increases in security for ports, harbors, and waterways. WaSPNet (Waterborne Surveillance and Protection Network) is aimed at providing a solution to the complex problem of maritime security. It comprises a swarm of network members, each configured as necessary in terms of sensor packages, mobility requirements and network capabilities to provide for information gathering and dissemination. A secure mobile ad hoc network of multiple unmanned maritime sensor equipped platforms meshed with existing fixed sensor networks can provide operators and decision makers with real-time eyes and ears on the scene. Initial operational experiments have validated this concept by integrating multiple sensing modalities through a mesh capable extended Ethernet WAN consisting of varied types of communication links. Extending this network across organizational boundaries will enhance decision making capabilities, enabling immediate responses to environmental, criminal, safety and security threats.**

Keywords—mobile ad hoc network; USV; UUV; unmanned

I. Introduction

L-3 PHOTONICS is developing a Mobile Ad hoc Network (MANET) of waterborne security and environmental sensors for the purpose of providing mobility and extensibility to existing fixed port protection infrastructure. Making use of small autonomous or remotely-piloted vehicles (UUVs , USVs) to provide detection, classification, localization and tracking of underwater or surface activities, with minimum human input, each platform is equipped with a package of sensors, configurable for specific missions and environments, such as radioactivity, sound, bio-hazard, SONAR, magnetic, and drugs or other illicit material detection. The platforms are each connected to a minimally-manned ground station and fixed assets using real-time communications via secure acoustic, optical or RF communicationss. These platforms are programmed to autonomously patrol and survey the maritime domain of harbors, ports and waterways, continuously sensing and surveying the environment for anomalies, and report back to operators in real-time in the event an abnormal situation is encountered, or when directed by signals from fixed assets. Similarly, using remote piloting, operators can vector in platforms to on-water situations reported via other means, such as boats or swimmers in distress, unusual environmental situations, reports of suspected illegal near-shore activity, or simply to warn away trespassers. Providing for a high speed, secure, and even covert communications capability is central to this concept of a network of mobile sensors, extending the traditional range of communications to remote, hard to reach and dangerous maritime environments.

The benefits of augmenting trained operator capabilities through the use of distributed unmanned platforms are numerous and have been well documented in the popular press [1]. Use of unmanned vehicles in the airspace and on land has become commonplace in theatres of war, and is rapidly becoming commonplace within the homeland. Over a decade ago the President indicated that the United States of America was "entering a period of consequences that would be defined by the threat of terror …" He went on to state that "Now it is clear the military does not have enough unmanned vehicles. We're entering an era in which unmanned vehicles of all kinds will take on greater importance - in space, on land, in the air, and at sea." [2] Interestingly, the maritime focus has indeed lagged behind the other environments listed. But there is a benefit to be gained from that lag; access to sophisticated unmanned capabilities is no longer available only to those with military-level budgets. Control systems, navigational capabilities both autonomous and remotely piloted, and complex sensor packages have all seen dramatic reduction in access costs, to the point where Intelligence Surveillance and Reconnaissance (ISR) capabilities are within the reach of state and local, and in many cases private, entities.

However the military infrastructure supports a myriad of secure, non-line-of-sight (NLOS) telecommunications capabilities; that infrastructure is often not available to the entities listed above. The usage of the personal mobile device infrastructure (cell phones, tablets, etc.) is available but nearly every out-of-the-ordinary event from power outages to security crises has overloaded that infrastructure to the point of unreliability.

Wireless networking is also becoming commonplace, and thus affordable. The obvious limitation lies in coverage distance; since the majority of the wireless networking equipment is directed at Local Area Networks (LANs) it is difficult to implement a wireless router infrastructure capable of continuous coverage of large maritime environments such as harbors or meandering waterways. Maritime environments are geographically and industrially complex, and are constantly

This data consists of L-3 Communications, PHOTONICS Division general capabilities information that does not contain controlled technical data as defined within the International Traffic in Arms Regulations (ITAR) Part 120.10 or Export Administration Regulations (EAR) Part 734.7-11.

978-0-933957-40-4 ©2013 MTS

changing to meet the needs of commerce, further exacerbating this issue.

It is this convergence of needs and capabilities which needs to be recognized and utilized. Robust information connections enabled by a network of mobile unmanned platforms presents a solution which utilizes existing technologies to bridge these gaps in the communications network. The Waterborne Surveillance and Protection Network (WaSPNet) comprises a swarm of network members, each configured as necessary in terms of sensor packages, mobility requirements and network capabilities. Making use of mesh networking technology, this MANET may be dynamically configured to provide ISR where and when it is needed, in response to threats or changes in the operational environment.

This paper presents a Proof-of-Concept (PoC) implementation of a maritime MANET comprised of manned and unmanned nodes. The initial operational experiments were aimed at developing the concept of operations (CONOPS) and defining design goals and parameters to inform advancements in system capabilities. Applications of these CONOPS will provide situational awareness in remote or hard-to-access areas which have historically presented a major challenge to ensuring security in a maritime environment.

II. Baseline: Existing Maritime Security Capability

Maritime security may be defined as the protection of ports, harbors, maritime facilities and waterways. Threats are numerous and varied, and may include acts of terrorism, drug and/or human smuggling, oil or other toxic chemical spills, natural disasters, and human error resulting in emergency situations.

Maritime security environments are also diverse and often complex. Port facilities, local harbors and waterways, and border lakes and rivers present significant security and monitoring challenges. Importantly, ports, power plants, dams and water supplies, which due to their size, immobility and significance, represent choice targets for terrorist attacks.

There are many products out on the market that offer fixed security solutions for maritime threat detection and surveillance. Most of these products are offered separately and from multiple sources. Current maritime security solutions include cameras, security guards/ patrol, underwater sensors, buoys with sensors, tethered vessels and the need for constant communication and collaboration between governing agencies.

Cameras and monitoring systems are one of the key components to surveillance of harbors and ports. These fixed systems can offer low cost surveillance solutions and are relatively easy to install and maintain. There are, however, many drawbacks to fixed camera systems. Fixed cameras are highly anticipated and can easily be tampered with or bypassed. They lack visibility to underwater dangers and do not offer anything more than line of sight into detecting threats.

In general ISR in the maritime environment has been comprised of single sensors providing information to single users in a single organization responsible for security. This information is then disseminated via a non-real-time information connection provided to other users across other organizations using a labor intensive review prior to dissemination. This rather inefficient path has been driven by the lack of real-time communications capability to provide operators and decision makers with situational awareness and command and control capability of assets. In addition, any single user or organization responsible for security may be challenged by marshaling enough resources to provide a complete security solution.

A. *Extending the Baseline:*

Information connection and network thickening is the focus problem considered here. WaSPNet provides an example of how disparate sensor platforms can be enabled as network nodes and connections, and how this MANET can be configured in real time to provide information paths across platforms, users and organizations.

III. Concept Definition

WaSPNet comprises a swarm of mobile and fixed network members. Each swarm member can operate as a node in the ad hoc network; the nodes are then configured (both in their capabilities and in their physical position) as needed to respond to changes in the operating theatre. Since the swarm is intended to work in a maritime environment, each swarm member was developed with the appropriate level of environmental protection.

The basic intent of WaSPNet is to provide an extended LAN or WAN capability via communications between the mobile swarm members. For this study, we implemented a Gigabit Ethernet Local Area Network (LAN) to communicate with the various sensors, imagers and remotely piloted vehicles. The physical components of the LAN included wired and Free Space Optical (FSO) communications links supporting the full 1Gb/s bandwidth, and RF communications links with bandwidths to 20Mb/s. This extended LAN demonstrated the capabilities of the WaSPNet concept, it was intended as a proof-of-concept accepting of limited scope and capability including bandwidth and network performance limitations. The fiscal realities of today will likely impose similar constraints on many end-users. However, we were able to provide a realistic implementation on a modest budget. Fig. 1 indicates the block level diagram of this network.

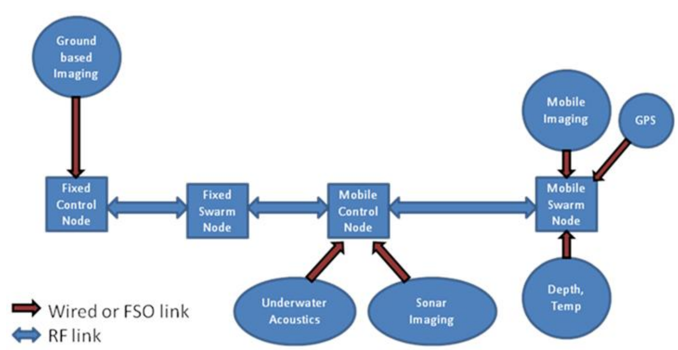

Fig. 1. Proof-of-concept WaSPNet Implementation Block Diagram

IV. Development of a Maritime MANET

A. Research and Development Goals

1) Implementation of a maritime MANET

- In-field performance measurements of COTS RF mesh networking hardware to provide performance comparison with tactical communications hardware
- Development of a low-cost, minimally-manned operating station (Ground Control Station) for vessel and network control
- Demonstration of NLOS operation of vessels via the network
- Integration of multiple imaging and listening techniques into the mobile sensor suite
- Integration of multiple communications technologies within the MANET

2) Demonstration of proof-of-concept capabilities of a maritime MANET, including
    a. remote internet access and control capabilities, enabling centrally located decision makers to have eyes & ears on site as well as on-demand control of vessels
    b. demonstrations of capabilities in various maritime environments geographically near Carlsbad, CA

3) Development of realistic Concepts of Operation (CONOPS)

B. Network Configurations

A total of 4 wireless routers, implemented as a combination of fixed (buoy) and mobile (USV/manned vessel) nodes were used. Each router was configured to the same subnet (192.168.216.0/24) to represent a real-world wireless network implementation.

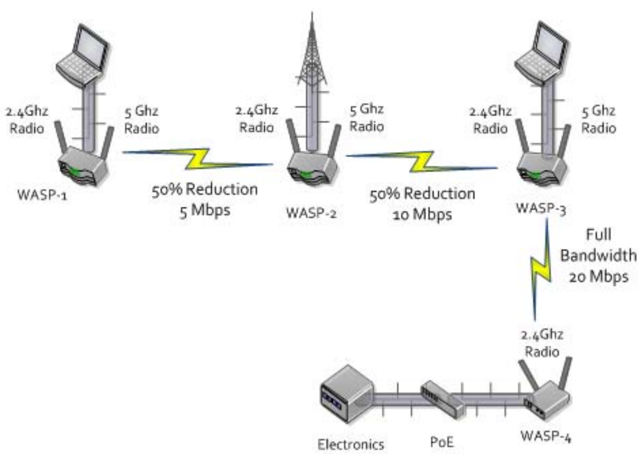

Fig. 2. Network Topology for Proof of Concept WaSPNet Implementation

The network and the access points were implemented in the data link layer (layer 2), enabling them to act as end nodes as needed. Testing was supported at each router via a separate wired test connection to a laptop, enabling packet inspection and router performance monitoring. The IP camera and other sensors mounted in the USV are designated as WASP-4 in Fig. 2. The typical configuration was the multi-hop WASP-1 ↔ WASP-2 ↔ WASP-3 ↔ WASP-4 path, although all other combinations were dynamically configured as needed to demonstrate mesh network capabilities.

C. Maritime Testing

Transport and deployment of the network hardware and the USV was possible with two people using a small box van. Setup, operation, take-down and re-deployment were demonstrated on a daily basis. Fig. 3 shows a typical load-out for test operations.

Fig. 3. Equipment transport for typical test scenario

WaSPNet was successfully demonstrated in controlled-access maritime environments. Remote NLOS navigation and real-time command and control of a USV was performed utilizing streaming on-board Point of View (PoV) video in addition to sensor information provided wirelessly over the MANET to a minimally manned control station. Hands-on real-time control of the USV was implemented with commercially available input devices and software running on a laptop. Various tests sessions were completed over the Feb-April 2013 time frame. In addition to the PoV video stream, ground based imaging was used to provide the operator with wide area situational awareness.

The Ground Control Station (GCS) infrastructure was kept extremely simplistic to demonstrate capabilities while keeping access costs as low as possible. In addition to real-time remote operation, waypoint guided navigation of the USV was demonstrated using an off-the-shelf Arduino-based auto-pilot. No attempt was made to implement full autonomy due to the difficulty of sense-and-avoid feedback for obstacles, people or animals in the water. Though full autonomy is a useful tool for platform navigation, it was not the focus of this demonstration; our focus was to thicken the information connection.

D. Latency of Video feed affect on USV control

A high-definition video camera mounted on the USV seen in Fig. 4 provided an on-board PoV video stream used for real-time, hands-on control and navigation. Excessive latency between the image and reality increases difficulty of control. The level of difficulty was seen to be operator dependent. The most experienced operator was able to compensate for roughly 500ms latency with no observable lack of control

Fig. 4. USV platform with imaging sensor

Minimum latency of ~30ms was measured via a directly wired network connection, dominated by the codec settings and the frame buffering internal to the camera. Maximum latency of ~50ms occurred during the 3-hop mode indicated in Fig. 2, over a total pathlength of ~280 feet, mainly due to internal delays within the routers. This presented no navigation or control issues to any operator.

E. Sensor data

Various sensors were employed to demonstrate the disparate data types capable of transport through the WaSPNet architecture. GPS information including vessel speed and heading, water temperature and depth, full-motion video and multi-spectral imaging, and hydrophone data were integrated into the extended WAN. Depending on the data type, additional analysis or on-board processing was necessary prior to dissemination or user review. As a simple example, the data from the high-frequency capable ITC-8095 hydrophone was processed for spectral content; the direct time-domain signal being less appropriate for direct user review, particularly for any higher frequency content.

An example of on-vessel PoV video used for surveillance of shore activities as well as other vessels is shown in Fig. 5. HD Video resolution was either 720p or 1080p, dependent on test parameters.

Fig. 5. On-board PoV video feed

To provide an example of a high performance imaging system, an L-3 Wescam MX-10 [3] multi-spectral imaging turret pictured in Fig. 6 was integrated into the network. Video comprised of standard visible, low-light visible and IR imaging was streamed over the network via the MANET, as well as via wired and Free Space Optical (FSO) links. Additional information including GPS coordinates, orientation, heading, etc. is included in the data stream, and is seen in some of the images as the light colored text overlays. Standard frame capture software was used to capture these images from the stored videos. Fig. 7 indicates IR imaging of USV operations at night, captured from the video feed.

Fig. 6. L-3 Wescam MX-10 imaging sensor

Fig. 7. L-3 Wescam MX-10 IR image

SONAR images were collected using an L-3 Klein UUV-3500 dual frequency Side Scan SONAR shown in Fig. 8 [4]. As a test example an object was added to an underwater structure to simulate a possible parasitic attachment. The anchor for a navigation buoy is shown in the left picture of Fig. 9. After the object, (in this case, a medium-sized propeller) was mounted to the buoy the area was scanned again, shown in the right image of Fig. 9. The new object is visible; details are minimal but sufficient to indicate further investigation.

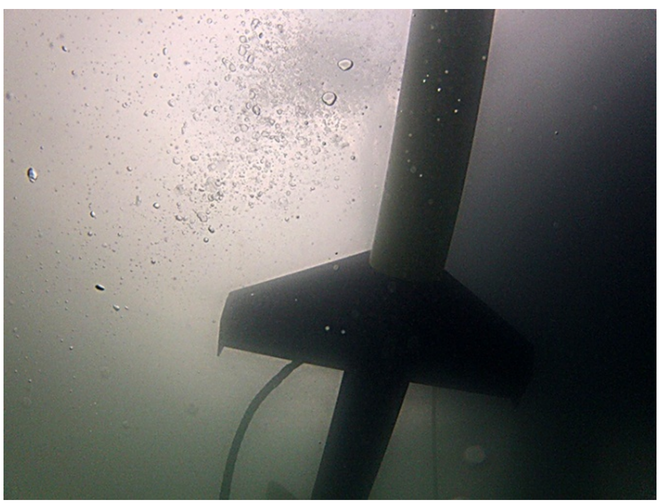

Fig. 8. L-3 Klein Side-Scan SONAR deployment.

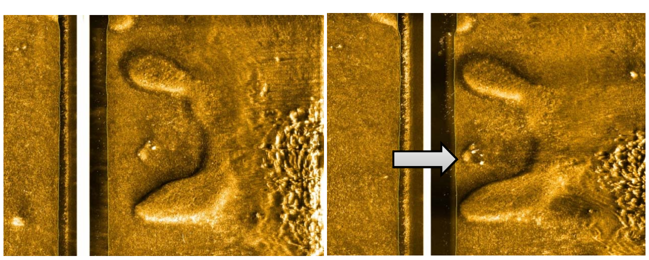

Fig. 9. L-3 Klein SONAR images

F. *Expanded network capabilities*

To demonstrate the transparency of the network to the physical implementation of the Ethernet WAN and to demonstrate enhanced capability through diverse connection types, additional communications links were integrated into the WaSPNet network. The performance of a Free-Space Optical (FSO) communications link was compared with a standard Cat-5 wired link. The FSO link consisted of a pair of L-3 PHOTONICS developed low-cost point-to-point GigE bi-directional transceivers. The WaSPNet concept is intended to accommodate almost any data connection type and can be implemented or enhanced with wired, RF, optical (fiber or free-space), or acoustic data transport either above or below the water surface.

G. *VPN via the Internet*

Connectivity via the Internet enables remote administration and control of the MANET. Demonstration of this capability was enabled with the use of a mobile Wi-Fi hotspot and a local Internet connection. A single point-to-point VPN connection was established using a 3rd party utility, LogMeIn Hamachi. This VPN access behaves as a single network, masking the additional network traffic, i.e. the intermediate router hops. Internet connection sharing was used as a method of terminating the VPN tunnel and establishing a link with the rest of the WaSPNet network. Proof-of-concept testing was completed within a campus environment. Maritime environment testing of internet control of the USV will occur in the next phase of this project.

Another technical challenge being addressed by PHOTONICS is the protection of the network of sensors from cyber attack. The multiple platforms interconnected together via optical, RF or acoustic communications, in effect create and ad hoc mobile network, that makes use of the internet and other existing infrastructure to disseminate command and control and sensor data and analysis. Even though the local environment may be linked with secure tactical communications, once the information or asset administration is extended to a WAN connected to the larger Internet, the network is subject to cyber Denial of Service or other types of attacks. An enemy could “spoof” the network at the critical time where the platforms are intercepting or analyzing targets. Making use of the L-3 PHOTONCIS NOTX cyber protocol, WaSPNet is defended against DDOS / DOS attacks, ensuring robust and reliable communications between each mobile platform, the operators controlling them, and the offsite decision makers who dictate what actions to take in the event of an emergency.

H. *CONOPS development*

Multiple threat scenarios and CONOPS to identify and deal with these threats have been developed. Fig. 10 depicts a possible WaSPNet deployment. Secure RF communications between a 4WD vehicle and personnel on foot is being coordinated at a local Ground Control Station; the GCS is also in touch with WaSPNet nodes on the surface of the water via the FSO link.

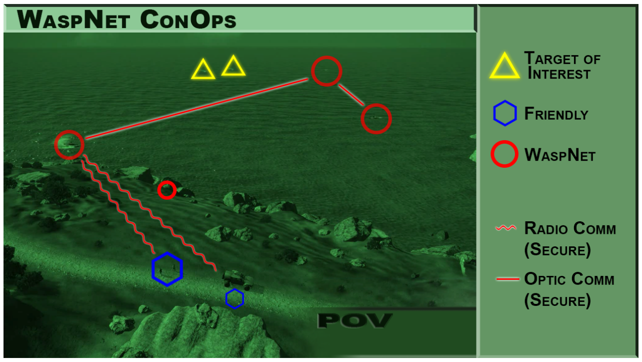

Fig. 10. Eye in the sky view of WaSPNet communications links

This eye in the sky view indicates relative positions of WaSPNet nodes, identified friendlies, and unidentified targets of interest. From this view point, it is difficult to discern details of the targets. Fig. 11 indicates on-board PoV video from one of the mobile WaSPNet nodes. Details of the targets of interest become visible; as the zoom factor is increased, further details become apparent. These screen shots were taken from a simulation which indicates the value of on-demand eyes on the scene.

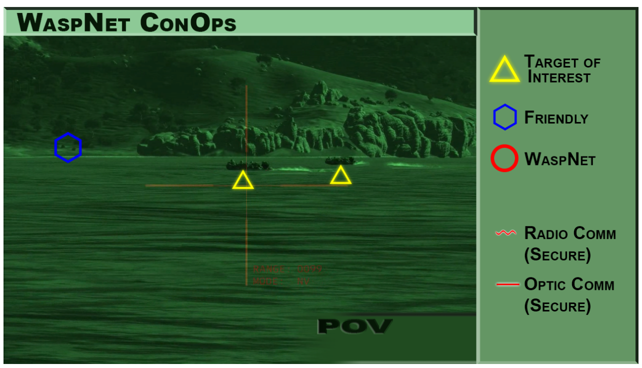

Fig. 11. Example CONOPS showing remote PoV from WaSPNet node

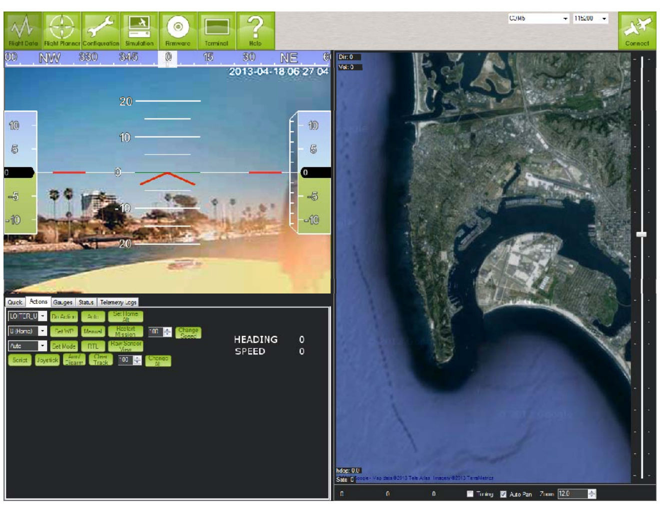

Fig. 12. Command and Control Interface

A preliminary command and control interface, Fig. 12, was developed based on the free-ware "APM Mission Planner" Streaming PoV video and terrain maps with GPS-based navigation overlays were included. Future command and control interfaces would be tailored to the particular environment and theater of operation with specific overlays or masks for individual platform types.

V. Conclusion

L-3 PHOTONICS is developing the Waterborne Surveillance and Protection Network (WaSPNet) with the vision of providing integrated maritime security solutions to entities whose mission is to protect and defend harbors, ports and waterways. WaSPNet makes use of unmanned or remotely piloted vehicles (USVs and / or UUVs) to provide detection, classification, localization and tracking of underwater or surface activities with minimal human input. Each platform is equipped with a package of multiple sensors, user configurable for specific missions and environments. All platforms are networked using real-time communications via secure RF, free-space optics, or underwater acoustic communications. This secure communications channel provides operators and decision makers real-time command and control with eyes and ears on the scene. These unmanned platforms can be programmed to autonomously patrol and survey the maritime domain of harbors, ports and waterways, continuously or using real-time control, operators can vector in platforms to on-water situations reported via other means. High-bandwidth, secure, and, as-necessary, covert communications capability is the hallmark of the WaSPNet solution.

L-3 Communications makes many of these sensors, communications technologies and software to enable autonomous monitoring and control of the WaSPNet platforms. And unlike the smaller companies and university based technology houses, L-3 has the capability to integrate all of these components and necessary logistics into a standalone system that can be tailored to each unique environment.

Acknowledgment

We gratefully acknowledge the contributions of: Craig Walker of NAVSEA NUWCDET, San Diego and Rich Granger of Battelle–Undersea Systems for invaluable insights and vision; L-3 Wescam and L-3 Klein, particularly Steve McCann and Mike Mitchell, for providing assistance and sensor platforms with truly exceptional capabilities; Prof. Mike Buckingham of Scripps Institution of Oceanography for expertise in underwater acoustics; and the WaSPNet team members including Tim Collins, Chris Collins, Tom Gibson, Jeremy Kunkel, Jeff Lastofka, Scott Miller, Gary Poon and Seth Taylor.

References

[1] "Wired for War: The Robotics Revolution and Conflict in the 21st Century", P.W. Singer, 2009, Penguin Books

[2] Speech to the Citadel Cadets, delivered at The Citadel, Charleston, S.C., December 11, 2001.

[3] http://www.wescam.com/index.php/products-services/airborne-surveillance-and-reconnaissance/mx-10/

[4] http://www.l-3mps.com/Klein/sidescansonar.aspx.