Return to main article

APPENDIX: CAPABILITIES AND SYSTEMS FOR MARITIME DOMAIN AWARENESS

Several existing capabilities and systems, mentioned in the main article, could assist in providing an offshore self-reporting tracking capability, the situational-awareness backbone for the maritime domain. To avoid detailed explanation within the article, these systems and capabilities are described below.

Maritime Mobile Service Identifier (MMSI). The MMSI is a nine-digit "string" designed to be "transmitted over a radio path in order to uniquely identify ship stations, ship earth stations, coast stations, coast earth stations, and group calls. These identities are formed in such a way that the identity or part thereof can be used by telephone and telex subscribers connected to the general telecommunications network principally to call ships automatically" (from Appendix 43 of the International Telecommunications Union Radio Regulations, as quoted on the U.S. Coast Guard Navigation Center website). In the United States, the National Telecommunications and Information Administration assigns federal MMSIs. The Federal Communications Commission assigns nonfederal MMSIs, normally as part of the ship-station license application; an MMSI is assigned whenever a vessel purchases an InMarSat terminal, an Automatic Identification System (AIS), or a Digital Selective Calling (DSC) maritime radio. Additional information can be obtained at the U.S. Coast Guard Navigation Center website, www.navcen.uscg.gov/marcomms. Inquiries can be directed to nisws@navcen.uscg.mil.

Automatic Identification System. AIS is an International Maritime Organization (IMO)–approved system developed at least in part by the U.S. Coast Guard as a collision-avoidance, port traffic–control system. Its primary component is a small broadcast transceiver, broadcasting at 160 MHz in Time Division Multiple Access (TDMA) format. A VHF signal, AIS propagates only in line of sight, so it can only be used when within visual distance of another transceiver, either mobile or ashore. The IMO has agreed to require that one of these transceivers be active on every commercial ship greater than three hundred gross tons by 2004. The system provides identification (MMSI) and location, as well as range and bearing from all other units in sight, in its field of regard. This capability allows a crew to calculate quickly its vessel's closest point of approach to all other AIS units in range. AIS also provides vessel tracking and control to Coast Guard captains of the port and their counterparts worldwide. The system's collisionavoidance benefits alone are such that most merchant ships leave it on at all times, even on the high seas, for warning should risk of collision develop. There is an international effort to establish an interface to satellite communications systems to allow long-range tracking of all large commercial vessels.

Digital Selective Calling. DSC capability is built into new maritime VHF radios, preset as channel 70. It is configured as a search and rescue system with additional selective calling capabilities, but it does not use TDMA or any other modulation scheme that would permit it to share its frequency; thus it quickly saturates with co-channel interference when more than a couple of units are active at the same time in the same area. This limitation precludes its use as a wide-area surveillance system. In localities, however, it is an excellent identification and tracking tool, as it employs the MMSI and can be coupled to the Global Positioning System (GPS) or LORAN, automatically providing the unit's location. (However, since the location data can also be manually inserted, this system could be used to send deliberately false and misleading position reports.)

Commercial Satellite Communications Systems. The third set of systems of interest to a "maritime FAA" comprises the various commercial communication systems that routinely operate over water. Those systems include the several manifestations of InMarSat, a geosynchronous satellite communications system designed to provide worldwide maritime coverage; the Argos system, which operates in a highly elliptical orbit; and the low-earth-orbiting OrbComm, GlobalStar, and Iridium communications satellite systems. These systems either have now or could be easily modified to develop position reports from either an embedded or separate GPS system and transmit periodic short, formatted reports containing time, position, and MMSI reports, thereby reporting location and identification of specific units at a specific time. The several communications ground systems receive these messages from mobile units and from them generates identification, position reporting, and tracking data at user-determined intervals. Furthermore, these are two-way systems; a vessel can be selectively interrogated and its transponder forced to send an immediate position report, change its reporting interval, or query attached sensors. (These functions cannot be modified on board.) The automatic position reporting interval can be preprogrammed in firmware of the satellite communicator anywhere from once a day to once per minute. For instance, a reporting interval for vessels at sea might be four times per day, then automatically increase to once per hour when the vessel crosses a specified threshold, such as five hundred miles from the coast. At the twelve-mile limit the interval might increase to four times per hour, and within the boundaries of a port to once every ten minutes or less. Using other preprogrammed features the unit can report any time it is rebooted, when the vessel starts to move, stops, or slows below a specified speed, etc. A dual-mode device containing both satellite and ground-based cell-phone transceivers, as already exists with some systems, would provide redundancy as the vessel enters U.S. waters. These systems would thus provide all of the functionality of the radar-based IFF system, but at much greater ranges, since they are satellite based.

The current systems range in cost from $450 to over five thousand dollars, depending on additional capabilities. Most of them interface to asset-tracking software that maintains a record of where each transponder is, and was at any point in time, as well as other pertinent data. The cost would most probably decrease if their use was mandated and became widespread and there was more than one system that met the standard. Indeed, no one satellite communications system should be specified; rather, a standard should be created and all applicable satellite communications systems encouraged to build to the promulgated standard.

It is estimated that up to 80 percent of all commercial ships still employ radio teletype as their primary means of communications. Additionally, between 10 and 15 percent of all commercial ships still rely on either continuous-wave manual Morse or single-sideband voice. However, the satellite transponders are now so inexpensive that they can reasonably be required for all ships entering U.S. territorial waters, just as all aircraft except the very smallest must be equipped with an IFF.

Container Tracking Systems. One other aspect of the various satellite-based transponder-tracking systems is their ability—already in widespread use—to track high-value/high-interest containers from point of origin to final destination. If the United States decided to put transponders on every U.S.-bound container worldwide (five hundred thousand units?), economies of scale would bring the per-transponder cost down from over five hundred dollars, acceptable only for high-value/interest shipments, to about $170, plus installation. (Installation costs vary depending on the type of container—reefer, dry cargo, etc.—and whether the unit is installed at the container's manufacture or retrofitted.) Significantly more capable transponders, which can be configured to tell if and when, and for how long, the container has been opened or out of a specified temperature range (important for fruits, vegetables, meats, etc.), will cost in the three-hundred-dollar range. In some systems, such as OrbComm, these transponders can be programmed, when within range, to switch automatically from the satellite system to the Global System for Mobile Communications (GSM) cellular telephone grid, in use throughout the world and one of the three primary systems in the United States. GSM is also useful for vessel tracking because it provides, at low cost, a high rate of position reporting should an agency desire to track a container or vessel in port more closely than is economically feasible with the satellites since, once the ship carrying the container is within line of sight of a cell-phone tower on the coast—as far as seven miles out— the reporting automatically switches to the cell-phone system, with its lower costs.

Shipping lines currently use these systems for many commercial reasons, among them improving demurrage billing, thereby reducing periods in which a container earns no revenue and the number of containers that must be kept in circulation. Some companies estimate that they are able to reduce container inventories by up to 15 percent. Other advanced features available to shippers (aside from security) are designed to reduce operational costs through automation, consolidation, and centralization.

Ultimately, there must be a convergence of commercial and security interests if this level of sophisticated vessel and container management is to be pursued on a wide scale. If adoption of such a hardware/service standard, already in use for commercial purposes, allowed shippers to develop a trust relationship with monitoring agencies and thereby reduce entry time into the United States, Canada, and Mexico, the unit cost of the hardware would be further justified. "Associated data" such as cargo manifests, transport routing, crew lists, etc., would be shared by agreement with foreign and domestic customs services and other government authorities, as well as with specific entities ashore, including family and exporters, importers, and shippers, as the specific user would desire. All users could determine who, besides the government, could access their specific files. With appropriate electronic customs seals on cargo containers, every shipment can be continuously tracked from the point of origin anywhere in the world to its final destination in the United States. Customs and other civilian and military authorities would be able to view the manifests as soon as the containers are sealed and data posted electronically by the shipper. Although the form and substance of the electronic postings now vary from country to country, sufficient data is available to form the basis of the system proposed by this article. Future standardization, however, is desirable.

Additionally, satellite communicators inside cargo containers can be programmed to send a security report when the container is sealed at the point of origin, when it is loaded on a vessel, and when it is removed from the vessel. Should the container be opened after it is initially sealed, an alarm is transmitted automatically. Built-in sensors automatically report conditions within and around the containers. This cradle-to-grave monitoring is economically practical with existing hardware. The only question today is whether to retrofit existing containers or build the equipment into new units only.

Multilevel Security. Multilevel security, the need to mesh the data exchange requirements from systems with differing levels of security, has plagued the military and intelligence communities for years and is now greatly complicating homeland security efforts, due to the increased need to tie military security systems to law enforcement classification systems. Backoffice associations (not exposed to the general public), the trust relationships required by civil and military authorities, and the hardware and software needed to effect multilevel security are all available and in commercial use today at every classification level (except special compartmented intelligence, which is and must be treated separately).

Good models already exist, such as Pennsylvania's Web-enabled statewide criminal Justice Network (JNET), recently demonstrated to Admiral James L. Loy (USCG, Ret.), formerly commandant of the Coast Guard and now head of Transportation Security Administration. JNET constitutes a virtual single system, based on open Internet technologies, that links information from the seemingly incompatible systems of sixteen criminal justice agencies. It enables agencies to share information but does not affect independent operating environments. As required by certain confidentiality statutes, each agency can determine the extent to which the others have access to its data. JNET is a secure "extranet," providing a secure publish-and-subscribe architecture featuring encryption and digital user/server authentication certificates.

Area Security Operations Command and Control. The ASOCC is a Defense Information Systems Agency (DISA) "advanced technology concept demonstration" that combines information-handling tools into a command-and-control tool for homeland security. Conceptually, it could link all of the communications capabilities envisioned in this article. It would be the link to both the NMIC and the military command authorities, as well as to the regional intelligence centers and civilian authorities, including law enforcement agencies—the Federal Bureau of Investigation, the Customs Service, the Drug Enforcement Agency, the Border Patrol, the Immigration and Naturalization Service, and the Coast Guard—and their intelligence entities. After "9/11" it was realized that no such capability existed; the ASOCC concept was the response.

DISA is also developing an overseas counterpart to the ASOCC, the Coalition Rear Area Security Operation Command and Control (CRASOC), to tie U.S. overseas rear-area force-protection assets into host-nation force-protection assets for mutual support. Its test bed is in Japan, at the headquarters for the Commander U.S. Forces Japan. The engineering design models for both the ASOCC and CRASOC are in use today, and further development is under way. The proposed maritime homeland-security center would also be linked to both the U.S. military command authority in its area and the NMIC via wideband communications channels using the ASOCC. The ASOCC would also provide wideband communications to civilian satellite communications systems, and thereby access to the databases of such organizations as Interpol (to which NMIC is already linked) and, potentially, commercial databases such as that maintained by Lloyds. These tie-ins would be crucial for tracking and identifying cargo and crew, but they could also have a major impact on efforts to identify and track suspicious vessels. The ASOCC would assist local fusion points for all information in a region and provide linkage to the Coast Guard maritime security squadrons, captains of the port, and port masters of a region, as well as to regional intelligence centers. Since November 2001, the ASOC has become the information backbone for a new force protection entity called the Joint Harbor Operations Center (JHOC); it is being used almost exactly as is postulated here, except its focus is on close-in harbor and port security.

Smart Agents. Software tools known as "smart agents" are now being experimented with in several warfighting roles. One such effort is the Defense Advanced Research Program Agency's CoABS (Control of Agent-Based Systems). It arrays smart agents in grids to perform specific warfare-associated information-manipulation functions. CoABS grids could assist in processing data from the sensors, automatically routing items to databases while passing tasking refinements back to the sensors, and forwarding to the fusion system information they derive from sensor data. The fusion system could have its own set of CoABS, passing tasking updates back to processors and sensors while routing correlated (linked together) or collated (intermixed) data on to the decision and display system.

Return to main article