Technology Deployment in Maritime Security: Emerging Issues

D. Dalaklis
TECHNOLOGY DEPLOYMENT IN MARITIME SECURITY: EMERGING ISSUES

Dimitrios Dalaklis
Associate Professor (Safety and Security)
World Maritime University
A Specialized UN Institution in Sweden
Outline

• Introduction, along with a couple (necessary?) clarifications;

• Highlight the need for a “pre-emptive” approach in the issue of maritime security;

• Limited discussion of the tools and systems supporting today the issue of Maritime Domain Awareness;

• Understanding their real potential, as well as limitations;

• Identify areas of strategic investment/trends for the future;

• Summary & Conclusions...
Maritime Transport:

• In the 21st century, maritime transport should be considered as the backbone of globalization and extremely vital for all “just in time economies”…

• Extremely large quantities of global trade (by volume) are being carried by sea.

• There is special/privileged relationship of commerce and maritime transport.

• Remember the axioms of geography:
  o Almost everywhere, excluding the poles (and the on-going reduction of ice-coverage is changing even this situation)

90% OF THE WORLD’S COMMERCE TRAVELS BY SEA;

THE VAST MAJORITY OF THE WORLD’S POPULATION LIVES WITHIN A FEW HUNDRED MILES OF THE OCEANS;
NEARLY THREE QUARTERS OF THE PLANET IS COVERED BY WATER.
Gulf of Guinea:

- The Gulf of Guinea is a vast and diverse region stretching from Senegal to Angola, including approximately 6,000km of coastline...

- Piracy, armed robbery at sea, illegal fishing, as well as smuggling and trafficking activities are unfortunately rather frequently recorded; these “threats” ultimately impact negatively the economic development of the entire region.
Gulf of Guinea:

- The Gulf of Guinea (GoG) is a busy shipping area and an important geo-political choke point for vessels transporting oil extracted in the Niger delta, as well as goods to and from central & southern Africa.

- Among the many rivers that drain into the Gulf of Guinea are the Niger and the Volta; its coastline includes the Bight of Benin and the Bight of Bonny.

- Apart from the truly vast sea area and the extended coastline, the physical landscape is providing numerous “hideout locations”...
Crime in the Gulf of Guinea:

- The discussion about “crime” or the manifestation of security threats usually involves two important elements:
  - MOTIVE (i.e. easy profit for a pirate or the person involved in an “armed robbery”)
  - OPPORTUNITY (i.e. the influence of geography (reducing speed when transiting a busy waterway, or if security resources available are impacting negatively the State’s capability to enforce the “Rule of Law”, or just by taking advantage of existing gaps in the security measures...)}
Clarifications: MDA

• The International Maritime Organization (IMO) defines Maritime Domain Awareness (MDA) as “the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment”.

• In the above definition, the maritime domain includes all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances.

• **KEEP IN MIND**: The mission of the IMO as a United Nations specialized agency is to promote safe, secure, environmentally sound, efficient and sustainable shipping through cooperation...
Clarifications: MSA

- The “Military” Approach (since -in most cases- there are already various types of sensors available):
Clarifications: MSA

• For NATO, Maritime Situational Awareness (MSA) is defined as: “the understanding of military and non-military events, activities and circumstances within and associated with the maritime environment that are relevant for current and future NATO operations and exercises -where the Maritime Environment (ME) is the oceans, seas, bays, estuaries, waterways, coastal regions and ports”.

• FOOD FOR THOUGHT:
  - In GoG, “Geography” is providing the necessary opportunity for illicit activities!
  - Is “Anything/Everything” feasible to be “Noticed/Spotted”?
  - “Noticing/Spotting” is very different than “Understanding”...
  - Even if we manage to “Understand”, is an appropriate “Response” possible?
  - Perpetrators are usually holding the initiative, by selecting the time and location of their “attack”...
  - The dilemmas of “Responsive” versus “Proactive” and “Resources Available”!
MDA vs MSA

• Are these approaches similar (or different)?

• Are they both “wide enough” in terms of scope?

• Stakeholders-Contributors-Partners?

• In recent years cooperation in GoG has clearly increased...

• However, there is still a need to discuss/identify/implement potential improvements; for example, are the existing surveillance capabilities “adequate” and more importantly, what type of technology applications can truly facilitate the much needed “effective understanding” towards MDA.
Security Collaboration in the GoG

[Map with regions and cities labeled: ECOWAS (Abuja), CMC Zone E (Cotonou), CMC Zone D (Douala), ICC (Youndé), ECCAS (Libreville), CRESMAC (Pointe-Noire), GGC (Luanda).]
Maritime Surveillance...

- Maritime transport enables trade and contacts between all nations of the World and provides the most cost effective tool for imports/exports that are serving the needs of the global economy!

- Maritime surveillance is essential for creating maritime awareness (also known as “what is happening at sea”);

- The IMO defines vessel traffic service (VTS) as: “a service implemented by a competent authority designed to improve the safety and efficiency of vessel traffic and protect the environment. The service shall have the capability to interact with the traffic and respond to traffic situations developing in the VTS area”...
Maritime Surveillance:

- Typical VTS systems use radar, closed-circuit television (CCTV)/Electro-optical sensor (EO), VHF radiotelephony and automatic identification system to keep track of vessel movements and provide navigational safety in a limited geographical area.
Maritime Surveillance:

- Framing the different components:

  [Diagram of maritime surveillance components]

  - Radar
  - AIS
  - VHF on IP
  - Weather Station
  - RDF
  - CCTV
  - Drone
  - Tablet
  - Monitor
  - Port Database
  - Radio

https://www.vissimvts.com/maritime-awareness/
Framing the relevant distances into a common perspective:

**Maritime Surveillance:**

- Satellites provide long range surveillance at lower resolution and higher latency.
- Terrestrial sensors provide real-time zero latency surveillance of ~90% of maritime activity within 75nm of the coast line.

**Snapshot: An Integrated Coastal Surveillance System**

- >80 nm VMS and Satellite AIS
- 25-80 nm Coastal AIS
- 0-30 nm Radar
- 0-10 nm Optical/Infrared

[Image of a coastal surveillance system diagram]
Maritime Surveillance:

• Managing effectively maritime traffic requires solving immediate challenges and planning ahead...

• A Common Information Sharing Environment (CISE) is currently being developed jointly by the European Commission and EU/EEA member states; Cutting a long way short, this initiative will facilitate the “integration” of existing surveillance systems by setting **common standards** for the exchange of information...
Maritime Surveillance...

EU’s approach:
- Taking advantage of all existing “tracking” systems such as RADAR, AIS, LRIT and the portfolio of VTS already available (provided by individual member-states) and adding on top certain satellite services;
- An extended network of trust and collaboration!
- “Cost issue” and expected “Return on Investment” (ROI)?
AUTOMATIC IDENTIFICATION SYSTEM (AIS)

AIS is a maritime broadcast system, based on the transmission of very high frequency radio signals. Ships send reports with ship identification, position, and course, as well as information on cargo. In Europe, the exchange of AIS messages is done through the SafeSeaNet system.

SATELLITE AIS

New systems are being developed to enable satellites to receive AIS position messages. This extends the geographical range over which ships can be tracked using the AIS system.

SYNTHETIC APERTURE RADAR SATELLITE IMAGERY

Satellite radar sensors measure the roughness of the sea surface independent of weather and sunlight conditions. On the satellite image, oil spills appear as dark areas, and vessels and platforms as bright spots. This is used in vessel detection systems (VDS) as well as pollution monitoring.

LONG RANGE IDENTIFICATION AND TRACKING

LRIT is a global ship identification and tracking system based on communications satellites. Under IMO regulations, passenger ships, cargo ships (100 gross tonnage and above), and mobile offshore drilling units on international voyages send mandatory position reports once every six hours.

METEOROLOGICAL-OCEANOGRAPHIC DATA

In situ remote sensing and model forecast meteorological and oceanographic data including wind, wave, temperature, currents, sea level, etc.

OPTICAL SATELLITE IMAGERY AND VIDEO

Earth observation imagery from satellite sensors operating in the optical spectrum, providing high resolution images of vessels or coastal areas.

VEssel monitoring system (VMS)

VMS uses communications satellites for tracking commercial fishing vessels. Vessels are equipped with on-board transceiver units which transmit messages every two hours.

 drones

EMS is currently exploring the possibility of using data from remotely piloted aircraft systems (unmanned aerial vehicles) for maritime surveillance purposes.

USER SPECIFIC DATA

EMS can also process other varied forms of national data provided by users. To date, this has included encrypted position reports from patrolling vessels and position reports from leisure crafts.

ADDITIONAL SHIP AND VOYAGE INFORMATION

Member States also exchange a range of additional data through the SafeSeaNet system, including: port notifications (e.g., arrival and departure times), Hazmat notifications (carriage of dangerous and polluting goods), ship notifications (additional information sent in mandatory reporting areas), and incident reports (e.g., pollution reports).
Explaining AIS

• The Automatic Identification System (AIS) is intended, primarily, to allow ships to “view” marine traffic in their area and to “be seen” by that traffic;

• Automated tracking system used on ships and by Vessel Traffic Services (VTS).
Explaining AIS

• The International Convention for the Safety of Life at Sea (SOLAS) requires AIS to be fitted aboard ships engaged in international voyages with 300 or more gross tonnage (GT), as well as and on all passenger ships regardless of size.

• AIS integrates a standardized VHF transceiver with a positioning system such as a GPS receiver, with other electronic navigation sensors (such as a gyrocompass or rate of turn indicator)...

What about vessels of a “smaller size”, as well as fishing vessels/boats/canoes? Vessel Monitoring Service (VMS) can help, but not solve each and every case...
Explaining AIS

• AIS information supplements marine radar, which continues to be a very important tool for monitoring activities within the maritime domain;

• Vessels fitted with AIS transceivers can be tracked by AIS base stations located along coast lines or, when out of range of terrestrial networks, through a growing number of satellites that are fitted with special AIS receivers which are capable of de-conflicting a large number of signatures.

• When satellites are used to detect AIS signatures, the term Satellite-AIS (S-AIS) is used...
AIS is an open-sourced system that relies on VHF broadcasts on open frequencies.

It is therefore vulnerable to malicious transmissions and runs the risk of being manipulated by individuals seeking to deceive the system...
Potential Problems?

• AIS is vulnerable to data manipulation, spoofing and hacking, which can take place within two main components;

• The most common and widely recognized issue of AIS manipulation has been with Internet-related usage of AIS data on publically available websites that display data compiled from multiple sources. (Easiest source to manipulate, the validity of data used has often been called into question).

• The other possibility is within the live AIS network of transmissions to and from vessels via VHF.

  ◦ Going dark (turning off the AIS), is a very common way to alter AIS data reported…
LRIT is solving all these problems!

- The Long Range Tracking and Identification (LRIT) is an international tracking and identification system incorporated by the IMO -under the SOLAS convention- to ensure a thorough tracking system for ships across the world.
Summary & Conclusion

• “Integrated Maritime Surveillance” is about providing authorities interested or active in maritime safety and security tasks with ways to exchange information and data.

• Sharing data will make surveillance cheaper and more effective!
Summary & Conclusion

• Existing tracking systems, such as RADARS and CCTVs/EOs quite often cannot detect each and every activity at sea; especially small in size boats can often move around “unnoticed”...

• Automatic Identification System (AIS) can be used to “supplement” the recognised maritime picture, however it is not obligatory for all vessels to be equipped with that system, or simply they can “switch it off”...

• Additionally, AIS can easily be manipulated to provide false information; LRIT is a very secure system!

• Even if AIS is operating normally, there are two main type of manipulation:
  o Internet based;
  o “actually” altering AIS transmissions.
Summary & Conclusion

• “Building further” and simultaneously “integrating” the already existing maritime surveillance capabilities can be made via the creation of a common network, with suitably layered information...

• This can also facilitate the various different public actors/stakeholders to better communicate and exchange information (therefore, paving the way for “effective understanding”);

• Future use of drones?

• How to achieve optimised/effective response (almost real time) at sea?
Summary & Conclusion

- Widespread recognition that this cannot be done by security forces alone; dealing effectively with crime, requires the so-called “Holistic/Comprehensive Approach”:

Integrating Law Enforcement Agencies with the Maritime Industry?

- Navy
- Marine Police
- Port Authorities
- Coast Guard
- Custom (Marine)
- Seafarers
- Fishery Agencies
- Insurance (Marine)
- Ship Registry
- Ship Owners
- Ship Agencies
Summary & Conclusion

INFRASTRUCTURE, COMMUNICATION, RESPONSE

Long Range Identification and Tracking
Vessel Traffic Services
Automatic Information System
Vessel Patrols
Aerial Patrols
Satellite Monitoring
Aids to Navigation
Synthetic Aperture Radar
Marine Weather Risk Monitoring
Hydrography

INFO

MONITORING
EARLY WARNING
EARLY RESPONSE
RIGHT RESPONSE CAPABILITY
RIGHT PARTNERSHIPS
COMMUNICATION
ACCOUNTABILITY
EQUIPMENT

WMU WORLD MARITIME UNIVERSITY

DRONES
ETV
PATROL VESSELS
HELICOPTERS
FIXED WING
OTHER ASSETS

OIL SPILL RESPONSE KIT
Thank you for your attention!