ZESZYTY NAUKOWE AKADEMII MARYNARKI WOJENNEJ
ROK XLVIII NR 4 (171) 2007

**Mariusz Kościelski**
**Ryszard K. Miler**
**Centrum Operacji Morskich**

**Mariusz Zieliński**
**Akademia Marynarki Wojennej**

# MARITIME SITUATIONAL AWARENESS (MSA)

## ABSTRACT

Protecting maritime commerce from attack or exploitation by terrorists is critical to the security of the global market. Maritime security has also a major defense dimension because military seaborne transport will remain crucial for future operations. It is highly unlikely that the NATO military will be able to sustain a major campaign in the foreseeable future without the capacity to transport significant assets by owned or chartered merchant ship. That is why accurate, given in real time, selected when necessary, picture of all aspects of maritime activities is vital to NATO.

This article provides a short overview of the NATO Maritime Situational Awareness (MSA) program which is NATO response to the recent threat and is treated as a high priority task for entire organization after Riga Summit 2006. The idea, concept of operation (CONOPS) and all commercially available sources of merchant information are pointed.

## INTRODUCTION

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'.[1]

NATO has been dealing with it for the last couple years as stated in several doctrines, documents and other related papers. In January 2006 Joint Force Command

[1] North Atlantic Treaty Organisation, MC MSA draft definition, 05 March 2007.

Naples sent a letter to SACT requesting support 'to improve capabilities under Operation Active Endeavour (OAE)' in order to enhance CC-Mar Naples, Maritime Domain Awareness (MDA) tools.

MSA is an important concept for many nations and organisations. ACT engages with other MSA communities on an extensive basis, commands and organisations dealing with MSA such as: International Shipping, SHAPE, CC-Mar Naples and Northwood, European Union, NATO Command, Control and Communication Agency (NC3A), Joint Warfare Centre (JWC), MAROPS, MCCIS working groups, CJOS (Combined Joint Operations from the Sea), COE (Centre of Excellence) and nations in order to gain synergy and avoid duplicity of efforts. Several nations are contributing with their national data to enhance NATO MSA.

## FROM MDA TO MSA

NATO MDA has evolved, at the end of 2006 and within NATO, from NATO Maritime Domain Awareness (MDA)[2] to NATO MSA as a result of NATO RIGA Summit 2006. MSA activities have been divided into two different categories:

1. Short Term (0 – 2 years)
   - Conceptual Area
   - MSA Technology Area
     - LOEs (Limited Objective Experiments)
2. Long Term (2 – 5 years)
   - FUMARSER (Future Maritime Functional Area Services).

NATO MSA is a high priority program for ACT and as a natural consequence of this fact an Integrated Project Team (IPT) has been established. The team is implementing and delivering several products that are being assessed through LOEs activities that are also used to capture and refine requirements as it is being done through other activities such as the ones that are taking place related to MSA.

## THE IDEA

The mission analysis assumed that the majority of Alliance members would share aspects of existing maritime information and resources in order to create MSA

[2] Formerly a US Concept.

and initial collection systems and assets already exist. With these assumptions and the definitions above, it is assessed that the aim of MSA should be to create an enduring level of situational awareness of the Maritime Environment through a collaborative, holistic network of information systems. This can result in the following goal: **The Alliance, its member nations, Partners, other nations and organisations it chooses to work with, generate sufficient MSA to detect all maritime and maritime-based threats to the security of the Alliance in sufficient time**.[3]

To achieve the aim and goal, the overall objective of MSA should be to maximize the synergy of the MSA stakeholder contributors to produce sufficient awareness in order to detect and prompt appropriate action on illegal activity in sufficient time to prevent harm.

The objective above can be achieved through the creation of a number of effects as follows:

1. Organize
    1) An MSA network to process and share information/anomalies (classified or unclassified) is established. A network of national, international, civilian, military and industrial organisations with interests in the ME.
    2) A NATO maritime organization as a focal point to collate, manage, analyze, share and act upon information is established. (A NATO centric network must be established for military information collection and distribution to enable NATO operations. This organization will also utilize the use of the 'MSA Network' in order to obtain all available ME information).
2. Process – Bulk data is collected, collated, validated and fused with intelligence in order to detect anomalies and illegal activities, locate and track threats and share information, in accordance with defined SOPs (Standard Operational Procedures), with stakeholders.
3. Technical – Stakeholder assets are available to produce pertinent information. Pertinent present and future stakeholder sensor, collection and distribution systems (hardware and software) are or will be available and connected to the network.
4. Cultural – Stakeholders understand and contribute to the MSA concept. Stakeholders have shared beliefs, practices and attitude towards MSA.

[3] http://tide.act.nato.int/mediawiki/index.php/Unclass_Concept_of_Operations_CONOPS_for_NATO_MSA_30_Mar_07"

## THE CONCEPT OF OPERATION (CONOPS)

As MSA is not an operation in its own right but a tool, which would be used in an operation, no courses of action were developed. However in order to create the effects and to achieve the objective in support of the aim, a number of actions have been determined as an equivalent to an MSA CONOPS.

**Organize Effect 1** – An MSA network to process and share information/anomalies (classified or unclassified) is established – ongoing.

1. Identify all stakeholders in the AOIs (Areas of Interest).
2. Develop liaison with stakeholders in the AOIs determined above.
3. Develop agreements and protocols (policy, procedural and technical) for sharing MSA information multi or bilaterally at different levels of classification[4].

An example of a Mediterranean MSA Network is below at Figure 1. It is not all-inclusive. It is many more bilateral, multilateral networks would need to be identified and shown.

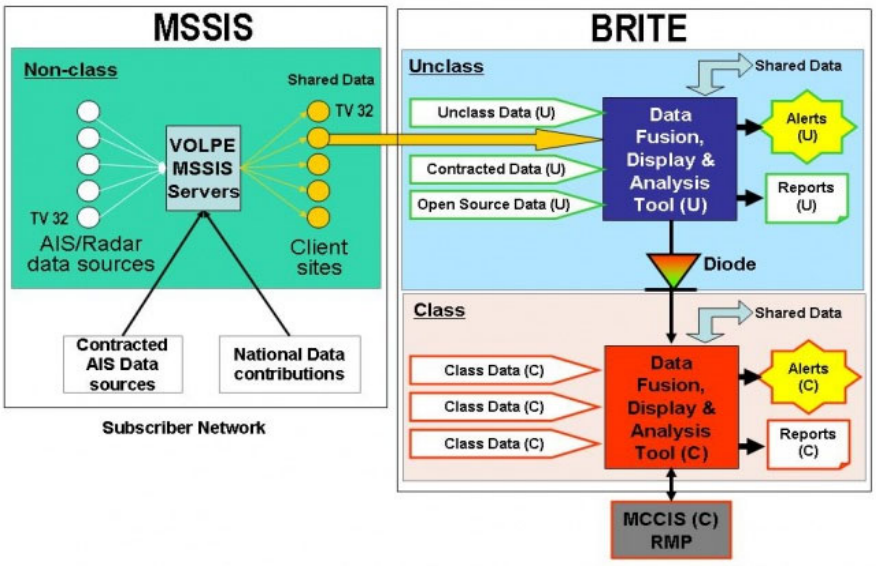


Fig. 1. MSA Architecture

*Source: http://tide.act.nato.int/mediawiki/index.php/NATO MSA Architecture – 11.09.2007*

[4] Some of the enclaves would need to be very small (e.g. Shell may be happy to share information with NATO concerning position, cargo and routing of their ships but would not be content to share this information with Exxon).

**Organize Effect 2** – A NATO maritime organization as a focal point to collate, manage, analyze, share and act upon information is established – ongoing.

1. Establish a focal point within NATO (a CC-Mar) to act as a MSA Coordination Centre for receipt, processing and distribution of information.
2. Establish regional collection and distribution centres (e.g. National collection centres and International/National operations in the AOO and adjacent areas).

**Process Effect** – Bulk data is collected, collated, validated and fused with intelligence in order to detect anomalies and illegal activities, locate and track threats and share information in accordance with defined SOPs (Standing Operational Procedures) with stakeholders – ongoing.

1. Develop agreements and protocols (policy, procedural and technical) for sharing MSA information multi or bilaterally at different levels of classification[5].
2. Standardize Information programs and equipment.
3. Develop Maritime Security Safety Information System (MSSIS):
   - Develop tools for processing data/sharing data;
   - Fuse MSSIS with the NATO Maritime Picture;
   - Promote initiatives for the policing of AIS;
   - Encourage and support implementation of regulations to widespread AIS systems to all ships.
4. Check Personnel Data (e.g. on intelligence 'watch' lists).
5. Track cargo.
6. Promote development of a standard ship routing plan[6] in conjunction with IMO.
7. Promote development of the Long Range Identification and Tracking System (LRIT) in conjunction with IMO.
8. Conduct Information Gap Analysis in areas of interest both geographical and in activity and develop plans to fill the gaps.
9. Establish Training requirement for the teaching of the processes.
10. Train Personnel to recognize anomalies, terrorist and associated activity and civil maritime environment (NATO Personnel).

**Technical Effect** – Stakeholder assets are available to produce usable information – ongoing.

1. Collect/gather info about present MSA systems from stakeholders. Conduct audit of what is already out there, which could contribute to MDA for the specific operation.

[5] See: Organize Effect 1c.
[6] Equivalent to Aviation Flight Plan.

2. Develop interoperability and connectivity among present systems/networks. This is building the technical solutions to achieving developing of MSSIS.
3. First phase of technical integration (Synergy of present systems) – Develop links between existing systems/networks for connectivity. Determine which systems can operate together, which have common computer protocols, which have compatible system communications etc.:
   - Share data with other appropriate HQs/organisations in MSA network;
   - Define the standards for information exchange among participants;
   - Agree with partners the requirements for connectivity and information exchange;
   - Provide technical guidance/assistance to partners if necessary;
   - Plan and conduct training as necessary.
4. Establish a working/steering group on technical aspects of MSA.
5. Second phase of technical integration – developing MSA network to include new systems and improved automatic anomaly detection systems. Improve it continuously with an open-architectural fusion capability to be able to cooperate with new systems:
   - Information Gap Analysis in the AOIs (lack of information gathering agencies, networks, etc. in a specific geographical area)[7];
   - Encourage use of satellite connectivity instead of UHF/VHF for AIS and LRIT[8].

**Cultural Effect** – All stakeholders understand, support and contribute to the MSA concept. This is most important, as it is the 'glue' that will hold the MSA network together. Still it is one of the most difficult as it may require cultural changes to the organisations concerned – ongoing.

1. Prioritise stakeholders in the AOIs in importance.
2. Develop strategies to persuade the individual stakeholders to join the network:
   - Identify 'win-win' solutions;
   - Establish and promote liaison with stakeholders;

[7] For example the west coast of Africa.

[8] IMO is developing Long Range Identification and Tracking system (LRIT) which will securely transmit ship's identity, location and date and time of the position over long ranges. There will be no interface between LRIT and AIS. Whereas AIS is a broadcast system, data derived through LRIT will be available only to the recipients who are entitled to receive such information and safeguards concerning the confidentiality of those data have been built into the regulatory provisions.

- Build trusting relationships;
- Identify mechanisms to persuade stakeholders to join the network.

3. Develop an information ('marketing') strategy to promote MSA with all stakeholders:
   - Develop a road show to 'sell' the product;
   - Allay the fear of an 'Open' web;
   - Allay the fear that MSA is only a military tool.

## INFORMATION SOURCES

There are considerable resources of merchant shipping data available for MSA, from commercially available databases to get records of vessels passing through the world's ports posted on port websites. AIS has vastly enhanced the availability of vessel track data which has been exploited by commercial companies and international agencies alike in building databases.

While raw AIS broadcast data are available to NATO many of the governmental information sources which could be used to verify the inherently unreliable AIS data are not releasable to the military. There follows a review of potential merchant shipping information sources:

1. AIS.
2. MMSI (Maritime Mobile Services Identification) – The International Telecommunication Union (ITU) is the authoritative source for the MMSI number used as the user ID for AIS messages. The ITU publishes a number of resources about the MMSI number online.
3. Lloyd's MIU (Maritime Intelligence Unit) has a number of online databases which could be used to validate ship information. Some of these databases are included in the NSCIMA project. Lloyds MIU also has ship voyage information available.
4. Lloyd's Register Fairplay is a separate company which provides reference information on vessels and shipping companies. This company issues the IMO number on behalf of the International Maritime Organization (IMO). It is a must that NSCIMA uses the Lloyd's Fairplay database instead of the Lloyd's Lloyd's MIU database.
5. International Maritime Organisation (IMO) provides:

- Global Integrated Shipping Information (GISIS);
- Certificate verification.

6. INMARSAT ship directory provides search by ship name or INMARSAT Number.
7. WMO (World Meteorological Organisation) operates a Voluntary Observing Ships (VOS) Scheme to take and report met observations:
   - SAILWX is a source of weather data for sailors and VOS fleet tracking information. A ship tracker is provided to search the VOS fleet database;
   - METEO FRANCE provides a similar database of VOS reporting vessels.
8. The US Office of Naval Intelligence (ONI) Civil Maritime Analyses Department collects data from several sources. It issues Worldwide Threat to Shipping Reports (mariner warning information) available to all. The threat is presented per region and per nation. It also provides HIVs (High Interest Vessels).
9. Ports web sites: arrivals and movements.
10. Paris MOU on Port State Control provides:
    - Banned Ships by ship name, IMO no, giving dates and reasons;
    - Current Detentions by IMO no, ship's name, flag, date of detention and detaining authority;
    - Detention Lists are published monthly as MS Office files;
    - Inspection Database can be searched on line.
11. National Maritime Companies and Agencies.
12. Vessel Classification Societies[9].

## MSA IN POLAND

MSA data contributions and MSA data is required from nations to NATO. This data will be updated as new information is available. Same nations (Table 1.) have already contributed to.

MSA is being developed for already 7 years and it has been put into live as SWIBZ means Shipping Safety Information Exchange System. All participants of the system (Polish Navy, Maritime Authority, Coast Guard, SAR Authority, and Hydrografic Office) agreed to exchange information which is aimed on increasing safety of the shipping within our Area of Responsibility. Special software has been developed to gather and display information which would be required by the participants of the system.

[9] http://tide.act.nato.int/mediawiki/index.php/MSA_Information_Sources – 12.09.2007

Table 1. Nations contributed to NATO MSA

| Country | Non Class data | NATO Unclass Data | NATO Class data |
|---|---|---|---|
| Belgium | | AIS | MCCIS |
| Bulgaria | | AIS | |
| Canada | | | MCCIS |
| Denmark | AIS | | MCCIS |
| Estonia | | | MCCIS |
| France | | | MCCIS |
| Greece | AIS | | MCCIS |
| Germany | | | MCCIS |
| Italy | | | MCCIS |
| Latvia | | | MCCIS |
| Netherlands | | | MCCIS |
| Norway | | AIS | MCCIS |
| Poland | | AIS | MCCIS |
| Portugal | AIS | | MCCIS |
| Spain | AIS | | MCCIS |
| Turkey | AIS | | MCCIS |
| United Kingdom | | | MCCIS |
| USA | | | MCCIS |

*Source: http://tide.act.nato.int/mediawiki/index.php/Data_Contribution_Matrix – 12.09.2007*

As of now there is no (and will not probably be in foreseen future) straight connection between SWIBZ and LEBA (the Polish Navy RMP collect and display System). The Polish Navy uses MCCIS and there is interface built between LEBA and MCCIS which allows information transfer from LEBA to MCCIS.

Information gathered in the Command Support Systems used in the Polish Navy is focused on Polish Exclusive Economic Zone. In Poland has been established system which is commonly used by main sea users (Polish Navy, HQ, Maritime Authorities, Coast Guard and SAR). In the context of COI or CCOI[10] tracking that could be done as a part of everyday data collection and validation within common legal frame which are quite difficult to use when it comes into real life. Like other navies, also the Polish Navy more widely uses information from AIS, but as of now it is not very common.

## CONCLUSIONS

During the next 20 years, maritime commerce will likely become an even larger and more important component of the global economy. The main elements of this transformation will probably include continued growth in the seaborne shipment

[10] COI (Contact of Interest), CCOI (Critical Contact of Interest).

of energy products, further adoption of containerized shipping, and the continued rise of mega ports as commercial hubs for transshipment and deliveries.

The challenges for maritime security are complex and growing. Addressing vulnerabilities, ensuring access to the maritime domain, and maintaining economic competitiveness while protecting 'western world' interests from sea-based attacks will be no easy task for NATO. The strategic nature of the challenge requires a strategic response. The next steps in that response must include further development of the NATO MSA concept, technical development of its main tool (BRITE) and maximizing the number of participating nations.

## BIBLIOGRAPHY

[1] Allied Command Transformation, *MDA Concept (draft 0.2)*, 27 October 2006.

[2] Allied Command Transformation (ACT) – TIDEPEDIA – http://tide.act.nato.int/mediawiki/index.php – 08.09.2007.

[3] North Atlantic Treaty Organization, *AAP-6, NATO Glossary of Terms and Definitions*, January 2006.

[4] North Atlantic Treaty Organization, *MC 367, Maritime Surveillance Coordination Centre Concept,* 3 May 2000.

[5] US White Paper, *Concept for Alliance and Coalition Maritime Domain Awareness*, January 06.

## STRESZCZENIE

Ochrona interesów żeglugi handlowej przed atakiem terrorystycznym staje się kluczowym elementem bezpieczeństwa globalnego rynku. Bezpieczeństwo morskie ma również swój wymiar militarny, bowiem transporty wojskowe drogą morską z uwagi na ekspedycyjny charakter operacji nabierają coraz istotniejszego znaczenia. Jest więc mało prawdopodobne, aby NATO mogło wykonać swą misję bez zdolności do przerzutu wojsk i zaopatrzenia za pomocą własnego lub czarterowanego statku. Dlatego też rzeczą pierwszoplanową staje się dla NATO posiadanie wiarygodnego, rzeczywistego i poddającego się selektywnej analizie zobrazowania sytuacji morskiej.

Artykuł przedstawia problematykę systemu zobrazowania i ostrzegania o sytuacji na morzu (MSA), który wydaje się odpowiedzią NATO na rosnące zagrożenia i jest programem priorytetowym w NATO po szczycie w Rydze w 2006 roku. W artykule w sposób syntetyczny wskazano ideę, koncepcję operacyjną oraz zakres źródeł zasilenia informacyjnego programu MSA.

Recenzent prof. dr hab. Andrzej Makowski