Final report

MARSUNO
maritime surveillance north

2011

The pilot project MARSUNO supports the policy process of the European Commission to create a Common Information Sharing Environment for the EU maritime domain

Table of Contents

Co-Financed under European Integrated Maritime Policy

Executive Summary

The need for an integrated functional and efficient exchange of appropriate information is crucial for the authorities and agencies related to the maritime arena.

The European Union has clearly recognised this need for improving and optimising of maritime surveillance activities, and interoperability at the European level concerning challenges and threats relating to safety of navigation, marine pollution, law enforcement and overall security by launching several measures and actions.

The pilot project MARSUNO supports the process of creating a Common Information Sharing Environment (CISE) which will serve as a decentralised information exchange network interlinking existing and future maritime surveillance and tracking systems cross sector and cross border throughout EU and connected to third countries as well.

The implementation of CISE will ensure the exchange of information within the EU community and including Third Countries and will have the effect of improving opportunities for better interoperability.

By this development, the Member States and Third Countries involved will be able to access relevant data and information within a shorter timeframe which will improve the opportunities for making better analyses and enabling faster, more accurate and efficient decisions.

The outcome of the Project studies fully confirms the prevailing situation described in the IMP planning documents. A central approach to achieve the necessary conditions for the enhanced exchange of information is to harmonise the legal framework preconditions. This approach presents proposals for amending and introducing new legislation at the EU level, in order to achieve a simultaneous harmonising impact. However, such a potent measure is far too time consuming to rely on only as the needs will suffer from the lack of viable solutions.

The MARSUNO project therefore concludes that it is now time to deploy planning into action and recommends that the EU Commission adopt the following **Implementation Policy** as the way forward to achieve a functioning intra-EU multilateral CISE.

This implementing policy has taken the following factors into account:

1. **Time efficient;** where results can be implemented within shorter timeframes compared to alterations of legislations which are dependent on time consuming formal procedures.
2. **Promoting harmonisation;** as the findings of the Work Group should be consensus founded the prerogative state that the solution responds to the entity of the opinions, thus presenting a "best unified solution for all".
3. **Need-based solutions;** as the action for each and every work group is directly related to the outcomes of the project recommendations (see Annex 8.4, Action List).
4. **Consensus;** the final positions of the work groups, based on common and shared opinions of the stakeholders, should be based on consensus agreements which constitute an equally stable basis as compared to the legal option.
5. **Concrete;** each solution related to the problem is direct and concrete.

6. **Direct implementation;** as the work groups are working closely on detailed, concrete needs, the declaration of the work groups could ensure shorter setup times compared to the legal procedures necessitating formal steps for adoptions.
7. **Cross sector / cross border capability focus**; the project actions correspond with the operators' need for unrestrained access to data/information.
8. **Respecting subsidiary;** as participation in the work groups consist of representatives from the Member States and Third Countries, this ensure their total commitment.
9. **Commission lead;** Responsibility to guaranteeing the fulfilment of the policy and safeguarding the coordination of objectives set out by the EU. The commission should be appointed to lead and supervise.
10. **Bottom-up approach;** the approach is founded on the setup that changes, adaptations and new proposals for solutions emanate from the need perspective.

The project recommends the following way forward to achieve a functioning intra-EU multilateral Implementing Policy

- The Implementing Policy should rely on the performance and outcome of designated Action Work Groups (AWG);
- The European Commission should be the body responsible to appoint AWGs;
- The European Commission should adopt Rules of Procedure (RoP) for the AWGs;
- AWG Final Implementing Decisions should be adopted on a consensual basis;
- The task of each appointed AWG is determined in accordance with the actions mentioned in Annex 8.4 Action List;
- The Commission should create sub-work groups whenever appropriate depending on the complexity of the action and to facilitate the achievement of reaching a solution; and
- The AWG should be composed of representatives from the relevant stakeholders related to the maritime information area, e.g. experts from Member State authorities and experts from Third Countries.

Co-Financed under European Integrated Maritime Policy

1. Introduction

1.1 Background

Integration of Maritime Surveillance (IMS) cross sector and cross border requires active participation of Member States agencies and authorities to succeed in the task. Since 2009 improved integration for maritime surveillance activities has been stated as a tool for the EU's Integrated Maritime Policy (IMP)[1]. In 2007, the Commission had already prepared for IMP for the EU domain with six strategic policy orientation points for the future:

- Integration of maritime governance,
- Development of cross-cutting policy tools, (maritime spatial planning, comprehensive marine knowledge and data, and integrated maritime surveillance),
- Defining boundaries of sustainability,
- Development of sea-basin strategies, (which allows adapting priorities and policy-making tools unique to the geographical, economical and political context of each maritime region),
- Development of international dimension of the Integrated Maritime Policy (to strengthen the EU's position in multilateral and bilateral relations) and
- Renewed focus on sustainable economic growth, employment and innovation**.**

The actions by IMP have the overarching aim of helping to deliver clean oceans and prosperous coastal regions for the future *while avoiding* useless duplication of spending and efforts.

During the project progress of MARSUNO, a parallel process on a larger scale has been ongoing due to development of a Common Information Sharing Environment (CISE). A draft Roadmap towards a CISE for the surveillance of the EU maritime domain was adopted in October 2010. Shortly afterwards a Technical Advisory Group (TAG) was established where representatives from several EU organisations take part, as well as one representative respectively from the MARSUNO and the BluemassMed (BMM) pilot projects. The purpose of the CISE is to function as a decentralised information exchange network interlinking existing and future maritime surveillance and tracking systems cross sector and cross border throughout the EU, but also with connections to Third Countries.

Need for cost efficiency

Cost-effectiveness and optimisation of data collection as well as of usage are also central to the initiative for the Integration of IMS and a CISE for the EU maritime domain, an initiative backed by the European Parliament.

[1] - Council conclusions on Integration of Maritime Surveillance 17 November 2009,
- Council conclusions on the Integrated Maritime Policy on 8 December 2008, Commission Communication on an Integrated Maritime Policy for the European Union and Action plan presented 10 October 2007
- the Commission Communication "Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain", presented on 20 October 2009;
- the Commission Communication on a Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain, presented on 21 October 2010;
- the Presidency conclusions of the European Council adopted on 14 December 2007;
- the Council conclusions on the Integrated Maritime policy adopted on 17 November 2009;

Co-Financed under European Integrated Maritime Policy

The Roadmap has a rather tight timetable to enable national authorities across the EU to exchange their data in a lawful, practicable and cost-effective manner, and the Commission already aims during 2011 to get results from tests of data exchange through practice in the two ongoing pilot projects. In times of recession and cuts in public spending, the Commission focuses on delivering results by limited means.

There is a strong need for expanding the sharing of information not only cross border but also cross sector, for instance the monitoring of transports of dangerous goods could be of interest to be shared with inspectors controlling illegal fishing and coastguards, police and navies to combat crime at sea. There could for instance be cost effectiveness in joint forces for intervention, and rescue operations with limited or no additional costs. The message from the Commission is clear, through better cooperation, data and assets can be shared and authorities will be better prepared to react while money will be saved.

European Union Strategy for the Baltic Sea Region

MARSUNO is also part of the European Union Strategy for the Baltic Sea Region (EUSBSR)[2], as a flagship project. It connects to one of four pillars, To Make the Baltic Sea Region a Safe and Secure Place, in priority area 13; "To become a Leading Region in Maritime Safety and Security". The Project corresponds to project 13.2,

"In a number of cases, the objective of the detailed actions in the action plan is to highlight priority areas of activity which are already identified or even in progress within the EU system or in other international frameworks, but which require enhanced efforts of coordination within the Baltic Sea Region and coherent funding strategies as a condition to success in the implementation."[3]

The Baltic Sea Maritime Functionalities (BSMF), with Finnish lead, strongly relates to MARSUNO. The aim of BSMF project is to improve exchange of information between functionalities nationally and internationally, focusing on the implementation of an individual state's national entity.

The European Council sets three parameters for the Commission in its development of the Strategy: 1) It should be without prejudice to the IMP endorsed in the same Conclusions, 2) it should inter alia help to address the urgent environmental challenges related to the Baltic Sea and 3) the Northern Dimension framework should provide the basis for the external aspects of cooperation in the region[4].

The Baltic Sea Region is a good example of a macro-region with sufficient issues in common to justify a single strategic approach. This could serve as a good example of efforts to achieve common EU objectives and a more effective coordination of territorial and sectoral policies based on shared territorial challenges. Implementation of the maritime actions in the strategy will be an important test case for the regional (sea-basin) implementation of IMP initiatives.

Cooperation already exists, but should be strengthened to make the region a world leader in maritime safety and security. Regional activity in combating crime should focus on intensified practical cross-border cooperation[5]. Member States with external borders, especially the after

2 SEC(2009) 712/2
3 SEC(2009) 712/2, page 4
4 COM(2009) 248 final
5 Ibid

Co-Financed under European Integrated Maritime Policy

abolition of checks at internal borders, need to take cooperative measures to safeguard internal security. In the Baltic Sea region very large volumes of oil are transported and there is an increasing trend towards the transport of liquefied natural gas. These activities carry risks for the environment, especially in difficult winter conditions. Further actions are still needed to improve cooperation, coordination and the coherence of maritime safety, security and surveillance agencies, as well as disaster response.

1.2 Purpose of the project

The pilot project is a step towards achieving the aims to render existing monitoring and tracking systems more interoperable between at least three coastal Member States to the Northern European Sea basins. Later on the aims is, in particular, to determine the extent to which this cooperation enhances exchanges of information and enforcement of international, Community and national legislation and cooperation that already takes place between the Member States[6].

Six objectives have been stated in the Grant Agreement of MARSUNO and these will be, among others, the terms to which DG MARE will follow up. Therefore, the report is following the structure of the objectives to clarify the predefined on-demand conditions

The report will mainly focus on results, based on the objectives and arranged according to the project specific sub-tasks for each layer. Other criteria as indicators (output indicators and result indicators), progress of components and other requests according to Grant Agreement will be reported in the fourth and final interim report of the Project[7].

The MARSUNO connection in priority area 13 on Maritime Safety and Security in the EUSBSR opens up for other issues, not only restricted to information exchange, but also concerning issues of operative character like for instance Place of Refuge, SAR areas, support tools like SeaTrackWeb and environmental aspects.

1.3 Methodological Approach

The project has been divided into different project organisational 'units', as work groups and a Steering- and a Management Committee (see Figure 1). The daily work has been directed from the Project Secretariat, provided by the Lead Partner the Swedish Coast Guard. The Constituent for the project is DG MARE that has been monitoring ongoing activities continuously by taking part as an observer in the Steering Committee. The EU Commission has been checking the interim reports as well as monthly reports on a regular basis.

Six work groups – also called layers – and corresponding to what is also called User Communities, have been working on 26 different sub-tasks connected to each layer. The Maritime Situational Awareness layer is a cross sector layer, aimed at connecting all common issues or other items of interest to give a comprehensive analyse of how to create a higher degree of interoperability between Member States and also Third Countries connected to the project. The final report contains the five Thematic Reports and the Common Information

[6] Call for Proposals MARE/2009/04, page 2
[7] Ibid, page 7, Outputs are the tangible deliverables of the project. Results are direct and immediate effects resulting from the project and the production of the outputs.

Sharing Requirements and Recommendation document as annexes and should be read in parallel with this report to get the full context of MARSUNO.

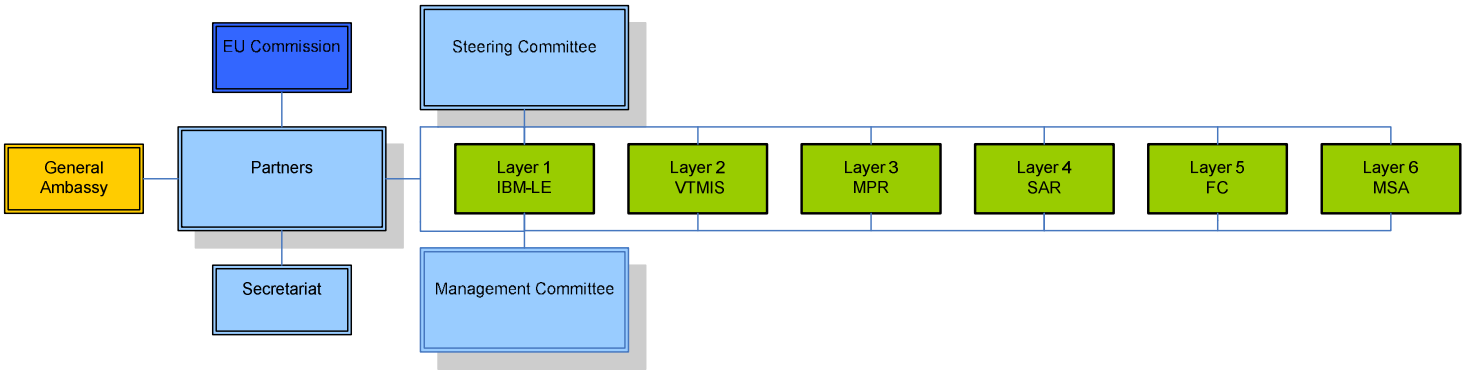


Fig. 1

Work groups/Layers:

1. Integrated Border Management – Law Enforcement (IBM-LE)
2. Vessel Traffic Monitoring and Information System (VTMIS)
3. Marine Pollution Response (MPR)
4. Search and Rescue (SAR)
5. Fisheries control (FC)
6. Maritime Situational Awareness

Workflow:

Parallel to the sub-task work within each layer a mapping process of data has been processed within each layer/user community, for further analyses within the Maritime Situational Awareness layer.

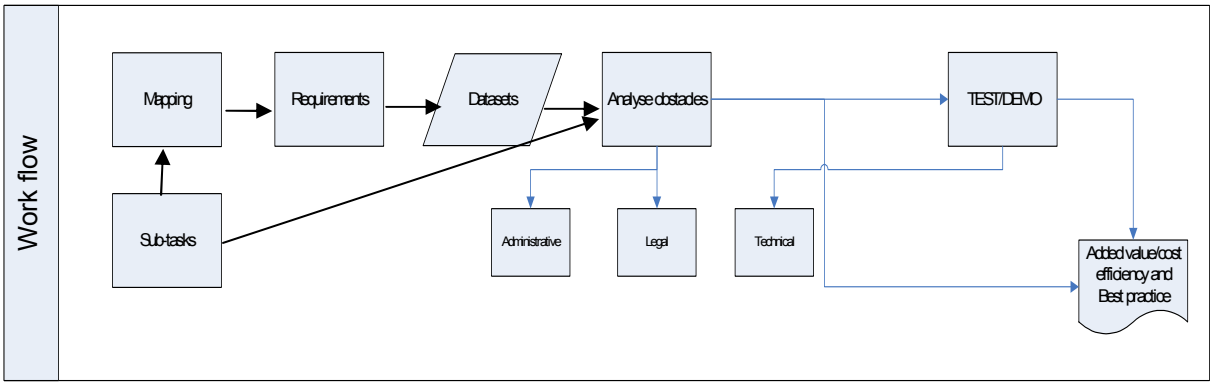


Fig. 2

Mapping of:

•Basic data
•Additional data
•Open or restricted data/information
•Availability and requirements
•Current agreements, bilateral/multi-lateral

Co-Financed under European Integrated Maritime Policy

The work has been done by studying former reports and results from other projects, case studies have been made, mapping process of available and requested information has been undertaken within all the layers. A specific cross-sector workshop on administrative, technical and legal gaps was arranged in March 2011[8], followed by a civil-military seminar[9] with the purpose of discussing and sharing understanding between the civil and the military layers. In October 2011, a MARSUNO Demo[10] was arranged by the Lead Partner which was an opportunity to test the capacity of more than two partners exchanging information, both cross sector and cross border.

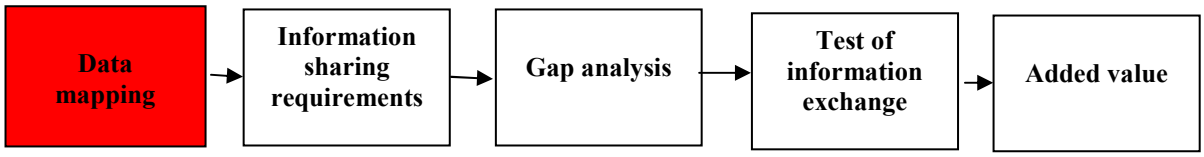
It is important to note that there are some limitations in relation to the project scope. MARSUNO is primarily focuses on administrative (including cultural) and legal obstacles in the gap analysis. Technical obstacles have been investigated but are not the main focus of the report. Neither have organisational changes or conditions been addressed in the report, nor gains from rationalisations. There should also be awareness of the development that is going on in other forums like for instance the IMO, where a lot of effort has been put into defining common standards. This will not be addressed in the project report.

[8] See www.marsuno.eu /Reports
[9] See www.marsuno.eu /Reports
[10] See www.marsuno.eu /Reports

2. Project partners capacity to exchange surveillance and monitoring information - Objective 1

To test the capacity of project partners to exchange surveillance and monitoring information relating to border control, customs, fisheries control, maritime safety, search and rescue, marine pollution, maritime security of ships and ports, prevention and suppression of criminal activities and the efficiency of maritime traffic and maritime transport that take place in the Northern European Sea basins with all the relevant authorities in the same Member State and in other Member States. Project partners may also acquire information for the purposes of exchanging it from existing or emerging structures in the field of internal security in which Member States are involved.

2.1 Project partners' capacity to exchange surveillance and monitoring information



Within the MARSUNO, a mapping process of how the different layers are able to exchange information has been performed. By identifying a common ground of basic data that is relevant to exchange when it comes to maritime data, all participating partners have filled out predefined matrices to visualise how the current information environment works between the partners involved.

This has been followed by defining requirements in data/information (see Chapter 3) that would be of benefit for the receiver to access, in order to improve their own performance. The capacity of information exchange is striking, and in regards to what is actually possible to exchange and the availability to exchange information the current situation needs to be adjusted to the requirements for accessing information. Within each layer, specified in the different layers' sub-tasks, the use of data/information through which channels and systems the information is exchanged, have been described. Obvious for most layers is that there is a strong need for moving over from a situation where limiting availability impedes the flow to a more user-defined state of the art.

Co-Financed under European Integrated Maritime Policy

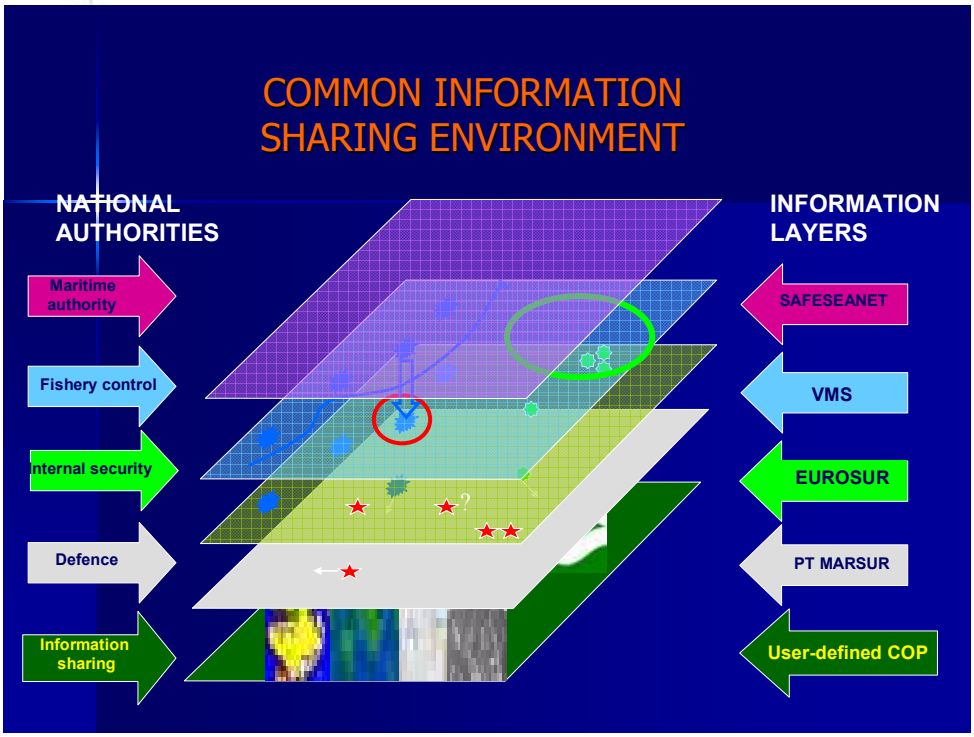


Fig. 3 Illustration of User communities and connections to different information layers[11]

2.2 Main purposes of information sharing

Each partner in the CISE community needs to build/define their own set of information to be used in Maritime Situational Awareness.

The purposes of Maritime Situational Awareness are the following[12]:

- to know in near real time what the situation at sea in the area of responsibility is (e.g. position, tracks and related information in order to select objects of interest)
- to have in near real time a vision of risk and threats based partly on analyses tools in order to conduct preventive and adequate action using available assets (e.g. patrol boats, patrol aircraft, MPR-resources)
- to have in near real time the best understanding and knowledge of events at sea in order to conduct adequate action

2.2.1 Situation at sea

The situation at sea is a specific situation depending on the mission of each authority/administration. Each MARSUNO layer has its own definition of which kind of information is necessary.

The information needed within each layer varies, but some of the information demanded will be the same in having a common near-real-time picture, including geographical parameters.

[11] CISE Technical Definition Draft V1 31/05/2011
[12] See more in Common Information Requirements and Recommendations (CISRR) document, Layer 6 Maritime Situational Awareness, www.marsuno.eu /Reports

The common denominators are the ones to be taken into account when it comes to Maritime Situational Awareness. Some sector examples are listed below:

Integrated Border Management and Law Enforcement (IBM-LE):

- Cooperative tracks (AIS)
- VMS tracks
- Non-cooperative tracks (radar)

Vessel Traffic Monitoring and information system (VTMIS):

- Cooperative tracks (AIS)
- Other cooperative tracks (radar)
- VTMIS = Non-cooperative tracks (radar, sensors)
- Weather
- MSI (e.g. AtoN status information)
- METOC

Marine Pollution Response (MPR):

- Cooperative tracks (AIS)
- VMS tracks
- Non-cooperative tracks (radar)
- Satellite images
- Weather
- Drift
- Illegal spill distribution
- Accident spill distribution

Search and Rescue (SAR)

- Weather
- Current
- SAR events
- Cooperative tracks (AIS)
- VMS tracks
- Non-cooperative tracks (radar)

Fisheries Control (FC):

- VMS
- AIS
- Non-cooperative tracks
- Fishing log
- Protected area
- Fishing area

2.2.2 Risk/Threat analysis

In order to have a in near real time knowledge and awareness of risk and threats, the project came to the conclusion that each administration should use its own analysis tools as well as using intelligence information and support tools like environmental atlases, drift calculation and other devices.

Analysis tools use all the information available in order to detect abnormal behaviour automatically or manually, (e.g. road, speed, and rendezvous at sea), incoherence between information, etc. Analysis tools should also consolidate information, i.e. create reference data bases, historic and statistics.

Common information sharing should enable to provide all these tools with the necessary basic information.

2.2.3 Ability to react to an event at sea

In order to detect events at sea each operational centre needs to aggregate a sufficient amount and level of information that will enable it to understand the situation and make good decisions in order to act on the situation. Often, the situation of interest moves from one area of responsibility to another as the ship (source of problem) continues its voyage. Currently sharing of information concerning an event is not processed automatically and an automatic near real time sharing would represent a major added-value.

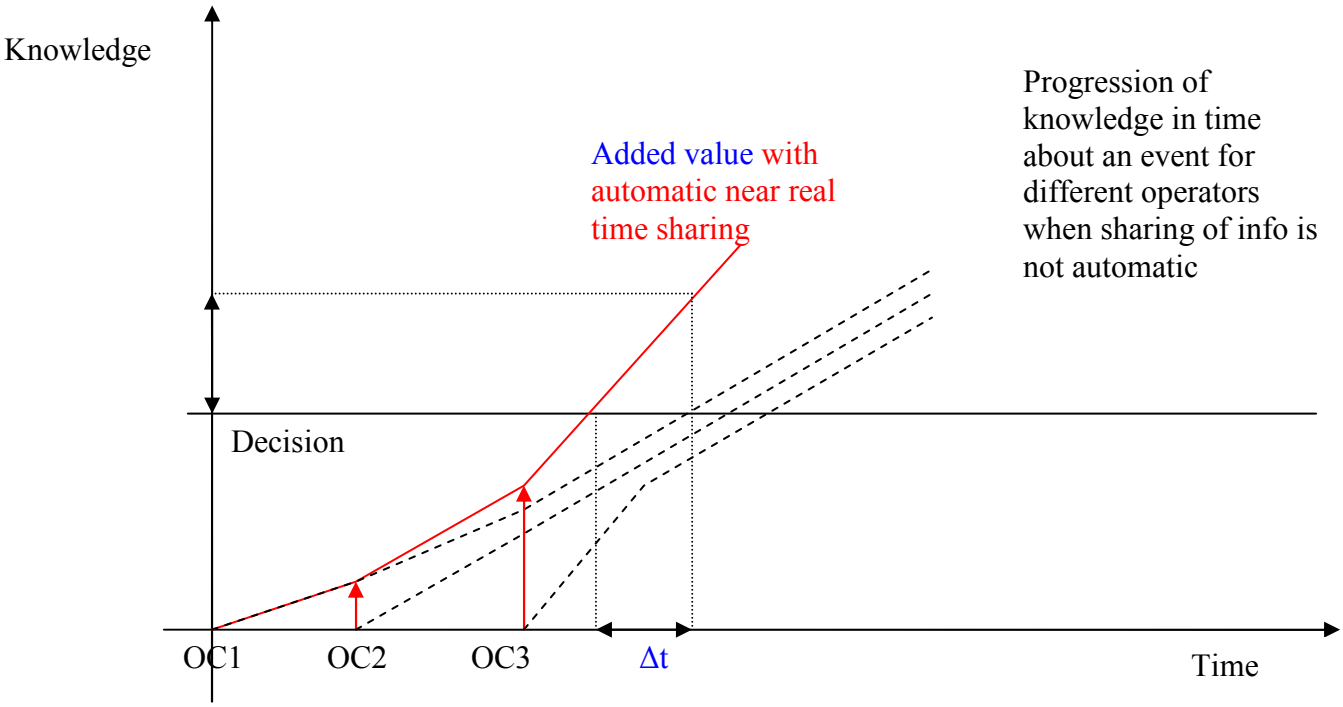


Fig. 4 Without automatic near real time information sharing, the operators from different countries responsible for the maritime area crossed by a ship that has problems, are doing virtually the same job in gathering information about it. They phone to the ship owner to obtain detailed information on the cargo, to the departure port, to other operational centrse, etc. In this way, they all spend almost the same amount of time to reach the level of decision (black lines).

If all operational centres could share information automatically about any dangerous ship or any event, they would have the highest level of info available about any event (red line) from the start. That way, end-users can be more efficient, using less time to find only missing information and obtaining better knowledge of the situation. Automatic information sharing creates a double added value (time and knowledge) as illustrated in this figure.

2.3 Information sharing needs within MARSUNO

2.3.1 What information needs to be shared?

The MARSUNO Matrix identifies the following data sets:

- ship positional data,
- ship current voyage data including persons on board data,
- ship ID data,
- historical data, (for instance, ships having recently loaded or unloaded oil or chemical products), and
- geographical information (e.g. weather conditions, currents and sea state forecast, pollution, area of marine resources, area of authorised fishing, seabed mapping), and

Co-Financed under European Integrated Maritime Policy

- Maritime Events Management (Security of commercial shipping, SAR, (SAR cooperation plan[13], ship rescue plans, ship evacuation plans and contacts by area[14]) shipborne pollution[15], shipborne illegal immigration, maritime customs action

It should be noted that the EU Technical Advisory Group (TAG) recently published matrices which suggest a different classification compared to the data sets proposed by MARSUNO[16].

Generally the quantity of information that can be shared is extensive. More than 500 data sets have been identified by TAG.

For example, it will also be of interest to share alerts or specific monitoring of ships for a better management of several risks (SAR, fisheries control, pollution prevention etc):

- SAR high risk ships[17]
- Fisheries control high risk ships
- Sub-standard ships
- Black listed ships

The bulk of information is related to a ship, which in turn is connected to a track (voyage).

Another large part of the information available is connected to a geographical position (weather conditions, currents and sea state forecast, pollution, exercise, area of marine resources, area of authorised fishing, seabed mapping). The rest of the info is essentially context information, background information defining organisations and responsibilities.

Several propositions in order to store data sets have been done. MARSUNO usually uses the following classification:

Basic information: Tracking information originates from sensors, observations etc. which is free to be exchanged inside CISE. Basic information is not open information. The information is produced inside the community using CISE

Additional information: This is information created or enriched mainly through the use of analysis tools. This kind of information is often responding to a specific mission or functionality and will be shared based on user demands inside the CISE community

Restricted information: This information is sensitive and cannot be shared freely inside the community using CISE. The main fear is the risk of information leaking that could complicate or endanger an operation[18].

These three categories of information are not exclusive or complementary. They simply reflect the fact that MARSUNO partners are willing to exchange data, basic information, additional information and restricted information. It is a common understanding that this sharing will improve efficiency.

---

[13]

[14] Thematic report Layer 4 SAR

[15] Thematic report Layer 3 MPR

[16] MARSUNO has chosen to only use the matrices in a guiding purpose to extract relevant data, to define what would compose the common ground for common basic data, and also for additional data. The results have been passed over to further TAG development. The following categories are used within TAG; Maritime Traffic Data and Maritime geospatial data. (TAG Maritime Data Supply-demand 21-11-2011 edited.xls

[17] Thematic report Layer 4 SAR

[18] See Legal analysis, section 4.4.

Measures have to be taken in order to improve current sharing, i.e.;

- enabling each partner to have access to basic info as needed, and
- enabling sharing of additional and restricted information.

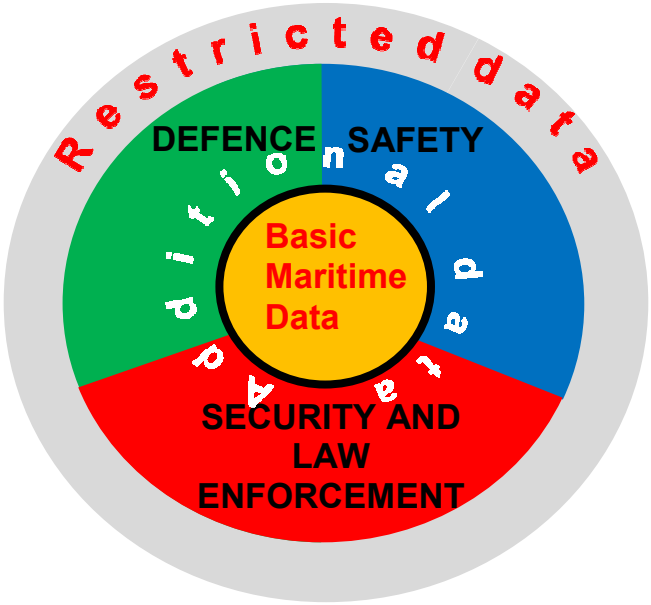


Fig. 5 Maritime functionalities and classes and levels of information

2.3.2 Information - Shared between whom?

In general all administrations and agencies in Europe in charge of maritime surveillance produce a part of the basic, additional and restricted information. They also provide means and networks for information sharing. In this way, any administration in Europe in charge of maritime surveillance is potentially a publisher of information for the interest of other administrations.

Hence, every administration is striving for an improved own maritime situational awareness and is looking for the best way to have access to more information and more accurate information concerning an area, a ship, an event or a context.

Shipping is global but it is clear that the need for sharing is essentially regional and sectoral. That's why the first step has already been mainly reached at Baltic Sea regional level and inside sectors as reported in the thematic reports. That is why basic information at least, should be shared freely and easily (automatically) between all administrations in charge of maritime surveillance in Europe. Concerning additional and restricted information, the sharing of information is currently very limited for two main reasons;

- fear of information leakage on recipient's side, and
- lack of knowledge of the existence of the information on potential recipient's side.

Today it is difficult to define who will need additional and restricted information from whom. A large part of this information is certainly sectoral and could be exchanged only within that sector. Otherwise, a part of this information is restricted and must therefore be protected and

shared only between two identified persons with for the case in question the appropriate authorisation.

The following three examples give an introduction to the different approaches regarding information sharing at the individual level:

- Any person working in an administration in charge of maritime surveillance, identified as Mr Smith or M. Dupont, working for 'XXX' administration in a European 'Country' should be able to ask for information concerning a ship, an area, etc, from all the communities inside the CISE and receive direct answers from all or coordinated answers from a contact person.
- Any person working in an administration in charge of maritime surveillance, identified as Mr Smith or M. Dupont, working for 'XXX' administration in a European 'Country' should be able to transmit any sensitive or restricted information securely to any specific group of recipients (sometimes only one person) belonging to administrations or agencies in charge of maritime surveillance.
- Any person working in an administration in charge of maritime surveillance, identified as Mr Smith or M. Dupont, working for 'XXX' administration in a European 'Country' should be able to have informal exchanges with his partners using cooperative tools (video conference, email, chat, whiteboard, etc).

Even though individuals are connected within CISE and exchange information at the individual level they must always act according to the duties, rights and competence of the person's agency of origin.

2.3.3 Sectoral and general information exchange in a cross-border perspective

The information exchange cross border within each sector is generally well established, mostly due to good cooperation through bilateral or unilateral agreements. Since the information is flowing within each sector, there are no direct obstacles for information exchange since in general the legal framework is applicable within the sector.

The level of cooperation and information exchange varies considerably depending on the Member State and the Third Country in question. Some Member States have developed cross sector information exchange systems at a national level, but in some Member States this is still a challenge. At a cross border level inside some, but not all, user communities, information is already exchanged rather well, but the information stays inside this user community.

2.3.4 Information exchange in a cross-sector perspective:

In the thematic report of Layer 1 – IBM-LE - some of the ideas have been defined.

Information is exchanged inside user communities, but it is not exchanged between different authorities on an international basis.

Cooperation between different authorities is still a challenge. Currently there are only a few types of internationally organised cooperation between different user communities (for instance within MPR, OPR). Some Member States have developed their own cross-sectoral information exchange systems, but these are only national.

A great deal of development work has been done in the field of national and international cooperation during the past few years. There are at the moment several active cooperation structures which have already been in operation for many years. Considerable experience has been received and gained from regional cooperation structures and needs.

It has been noticed that it is possible to exchange most of the information between partners without major obstacles, at least inside the EU. Some of the currently running regional cooperation may serve as good examples of exchange opportunity platforms. Reasons for barriers to information exchange could be e.g. approach policies or restrictions in legislation:

The willingness of exchanging information is mainly the key issue for actors involved in maritime issues, which has been thoroughly described in the Layer 1 thematic report. One of the most crucial issues is the lack of common cultural understanding for cooperation at the national as well as international cross-sector and cross-border levels. This has been reported in several layer reports and it has also been brought up at meetings and in discussions during the Project.

The main problem is connected to the national level, since actors or authorities are not sharing enough relevant information internally. To improve the information sharing there will be a need to start from a national point of view; then broaden it towards international cooperation and wider forms of information sharing. Such an initiative is the BSMF project.

Most of the information (including personal data) can be shared nationally between all authorised authorities without any specific barriers (see more in Chapter 4, Legal obstacles). The basic principle is that authorities are able to share information with other national authorities ordained in national law. To use a direct technical interface with other authorities' registers will require certain agreements between the authorities. It is nevertheless prohibited to pass on information to third counterparties without permission from the information's owners.

Information as well as personal data may be transferred to an EU Member State or an EEA country on the same grounds. When transferring data, confidentiality provisions of national legislation should also be observed.

Information (including personal data) can also be transferred also to Third Countries. It must be ensured that the recipient of the data has the right to process such data and ensured that the recipient will follow relevant national regulations concerning data protection and that all necessary notifications concerning its activities to the national data protection authorities have been complied with. The main rule (22 § of the Personal Data Act) is that personal data may only be transferred outside the territory of EU Member States or EEA countries if the country in question ensures an adequate level of data protection (the nature of the data, the purpose and duration of the intended processing, the country of origin, and the country of final destination, as well as the general and sectoral legal provisions, codes of conduct, and security measures applied in that country).

The adequacy of the level of data protection in the Third Country in question is, in each case, assessed by the controller. As a rule, Member States must allow transfer of data to such Third Countries as the Commission has deemed to have an adequate level of data protection. However, the permitted transfer of personal data also requires that other provisions of the

Personal Data Act are complied with prior to the transfer of data. Even if the level of data protection has not been deemed to be adequate in the country in question, data can, however, be transferred on the grounds provided by Section 23 of the Personal Data Act, e.g. if:

a) The transfer is necessary or called for by law for securing an important public interest, or for the establishment, exercise, defence or decision of legal claims;
b) The transfer takes place using the standard contractual clauses approved by the Commission and referred to in Article 26 (4) of the Data Protection Directive.

Maritime situational awareness is a goal which cannot be reached without cooperation or exchange of information. Cross sector information exchange should be encouraged to be carried out nationally as a first step, and it should be promoted based on the principle of *responsibility to share*. All in all, cross-sector and cross-border cooperation, especially including civil-military cooperation is important since it helps to achieve an improved situational awareness in the maritime domain.

There are, however, some obstacles to achieving effective cooperation and information exchange. The most important is lack of common language and definitions. There are also differences in organisational structure, working methods and political or professional culture. The lack of common understanding is a challenge, since it might even prevent cooperation in certain cases. Different interpretations of used terms and concepts used make it very difficult to have functional cooperation. Therefore, it should be noted that a structure for regional or multinational cooperation is not workable unless all counterparts understand each other. Therefore, it can be concluded that definitions, concepts and terminology should be commonly agreed on, including at least common definitions concerning classes and levels of information, maritime functionalities as well as risk analysis. Issues of willingness and trust should also be acknowledged. An important aspect in creating a cooperation structure is that there should be an atmosphere of trust and a common language.

Based on the assumption that even restricted information such as personal data may be exchanged without barriers, there should not be any obstacles for preventing different actors to make the exchange.

2.3.5 Information exchange in the perspective of civil military cooperation

The navies are an integral part of European security architecture. The participation of navies in Maritime Security Operations (MSO) varies from country to country and very much depends on the national legislation and allocation of responsibilities within the maritime domain.

For the successful implementation of their national and international Maritime Operations, such as operations fighting terrorism, weapons proliferation, narcotic trafficking, illegal migration, piracy and armed robbery, the cooperation with civilian authorities is becoming increasingly important.

Maritime Operations require a high degree of synergy of civilian and military maritime security activities and information sharing in order to achieve a coordinated effort to address all kind of threats. An important part in Maritime Operations is the naval cooperation and guidance of shipping (NCAGS). Today information is fed into the cooperation by ship owners

on a voluntary basis. Most of the information that is given also exists in information systems within the civilian sector. This means that an enhanced cross-sector information flow may avoid what today seems to be a duplication of sources.

At the EU level, within the framework of the EDA, 15 Member States have developed a maritime surveillance network, the pilot project MARSUR. A demonstration of the network has been tested by six of the participating members and was presented in Brussels on 30 June 2011. The network is fully decentralised and has been developed to be easily expanded. The network will be further developed along two lines of operation, one live phase where methods and supporting documents will be refined with a daily use of the network and one category B project to develop the technology. The MARSUR network was originally aimed at supporting maritime operations by contributing to a recognised maritime picture. It will also enhance Maritime Security Awareness within the participating Member States and is also marketed to be the cross-border information carrier within the defence CISE layer. Therefore it is possible for the network to be connected with other systems within the CISE.

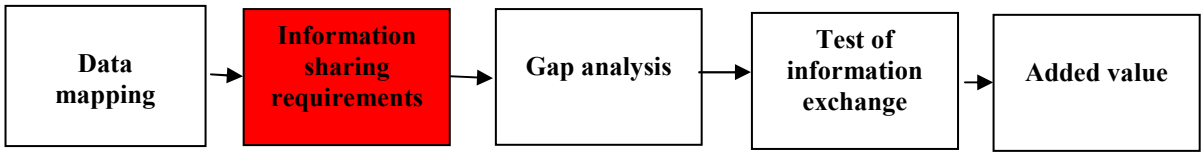
The EU Commission is supporting better use of resources within the union and is also encouraging civil and military authorities to interact by better coordination in different operations. This has also been strengthened via the Lisbon Treaty.

To close the gap between possible capacities of information exchange between the sectors, there is a need for policy decisions for making the exchange of information process easier. The military sector is able to support the civil society, agencies as well as private actors in various forms of cooperation.

In order to access all the necessary information, there is a need for sharing it both on cross-border and cross-sector levels. It is essential for all major international actors to act in a coordinated way, and to apply a wide spectrum of civil and military instruments in a concerted effort that takes into account their respective strengths and mandates. Information exchange reduces possible information gaps and allows the authorities to gather all the necessary information for knowing, analysing and understanding a situation in a cost-effective way. In addition to maritime surveillance picture and information exchange, analysis of the acquired information is needed so that situational awareness can be achieved.

3. How to ensure an exchange of information mechanism cross sectoral and cross border in a long-term perspective - Objective 3

To determine the extent to which project partners are potentially able to set up an exchange of information mechanism at cross-sectoral and cross-border levels that is viable and durable in time. This may involve actions within the remit of the areas referred to above in Paragraph 2 with the aim of developing an integrated network of reporting and surveillance systems for all maritime activities. This mechanism may also identify possible gaps and inconsistencies in fields where cooperation between civil and military assets exist or where they could be developed on enhanced in the future.



3.1 Exchange of information mechanism

3.1.1 Requirements regarding information sharing

Many requirements have been expressed by the MARSUNO partners:

In general

- The sharing of information should be efficient, secured, balanced and represent an added value for partners.
- Partners should be able to exchange freely and directly raw information (basic data) themselves.
- Partners should be able to exchange freely and directly additional information (including sensitive one) and restricted information with the specific partners they want and whenever they want.
- All partners are equal. There is no centralised authority. An encompassing administrational handler function is however required to maintain all the commonly agreed rules e.g. IT standards and data models.
- The sharing of information should be done within an appropriate timeframe, regarding the use of the information.
- The majority of sharing of information should be automatic, in accordance with an established configuration.

Co-Financed under European Integrated Maritime Policy

3.1.2 Regarding data and information shared

- Ideally only original information should be shared in order to minimise duplication of information and avoid network 'overload' by the same information.
- Origin and quality of information should be known and there should be parameters of exchange.
- A confidence value should be associated to the shared information. This confidence indicates if the data has been verified and validated by the source.
- Each administration is responsible for the information it publishes.
- Each information has a level of protection (e.g. unclassified, restricted, classified or secret) and can be used by administrations that have been authorised for this level and have an information system validated for this level.
- Each administration keeps the control of the data it shares. It has the possibility of correcting it at any time.
- The origin of information shall be known (traceability) in order to:
    - Avoid duplication of data.
    - Facilitate confidence and quality assurance
- Exchanged information remains the property of the providing administration.
- In many cases, information is over-classified and needs to be downgraded to match the good level of information classification well balanced between risk of leakage and useful dissemination.

3.1.3 Regarding organisation of sharing

- The information sharing environment should be built according to a system of systems approach (i.e. non-centralised system). The data exchange process shall rely on the existing national maritime surveillance systems and information sources.
- The information sharing environment (can be organisation, system, standard etc) should be interoperable with existing and future EU systems and systems of relevant Third Countries.
- The sharing environment of information should be flexible and scalable.
- The information sharing environment should enable automatic (as far as possible) and manual sharing of information between systems. Automatic sharing is done according to programs that can be modified by the owner of the information at any time.
- Network administration and security can be externalised but each administration manages the list of authorised persons for each level of protection according to criteria that have been defined beforehand.
- The information sharing environment should provide functionality to request a specific category of data as a single request based on certain search criteria, e.g. reply with data of the most recent information on the crew of vessel X.
- The information sharing environment should provide functionality to request a specific category of data based on certain search criteria, Example: immediate reply with data of the most recent information on the crew of vessel X.
- The information sharing environment should provide functionality to subscribe a specific category of data based on certain search criteria's. Example: immediate reply

with data of the most recent information on the crew of all vessels and continue reporting every new (update) information on crew data of vessels.

3.1.4 Several domains can be considered in building a long-term interoperability framework:

- organisation and resources management,
- concept of operations and standard operating procedures,
- implementation of the information sharing environment, and
- training of users.

3.1.5 Conducive[19] technologies

Service-oriented architecture is recommended. Nowadays, it is highly standardised enables system integration and in an easier way. Service oriented architecture could be implemented using REST[20] principles or the SOAP[21] protocol. Even if another approach could seem easier, other existing architectures suffer from a lack of standardisation and could be costlier to maintain in the long term. Thus a service oriented architecture using SOAP and web service standards is preferable. A pragmatic approach could also be to carefully mix both technologies. To respect the decentralized approach promoted by the project, a SOA capability (hosted by a specific gateway or existing systems) should be available at each participating site.

3.2 Necessity of a network of National CISE service

In the work done by the actors in MARSUNO the need for a function coordinating information sharing between the user communities has been identified and supported. During the discussions and seminars the need for the establishment of a network of so-called national CISE service (N-CISE) has appeared. The idea is that the N-CISE will be a complement to already existing NCCs or NMCCs. The maritime domain is a complex arena and therefore creates a high demand for a specific coordinating function enabling cross-border and cross-sector cooperation for creating opportunities for the best preconditions for CISE. Consequently this will give improved preconditions for the agency's ability to make fast and accurate decisions in their operational tasks.

By establishing national N-CISEs, existing national systems incorporated within already existing services in all types of maritime related matters, this could be a way forward for improved interoperability between existing systems and user communities.

The N-CISE shall not have any responsibilities for conducting or organising operations, only to facilitate coordination of information exchange. The N-CISE may be of virtual construction.

[19] Conducive - supportive
[20] REST – Representational State Transfer (interface)
[21] SOAP – Protocol for exchange of information (XML-based)

The establishment of such a network;

- should be founded upon national legislation or instructions , and
- will need to be built on certain standards and instructions common for all N-CISE independent of the national level or agency this function is designated. (see Section 4.3.4).

The N-CISE function should be executed in a virtual network or designated to a suitable national agency depending on national preconditions.

The tasks of the N-CISE will be;

- to provide the user communities with access to information for an updated basic Maritime Situational Picture (real-time situation picture),
- coordination and user management of national cooperation related to maritime surveillance,
- facilitate national coordination of information sharing related to maritime surveillance, and
- to direct external information to the appropriate agency.

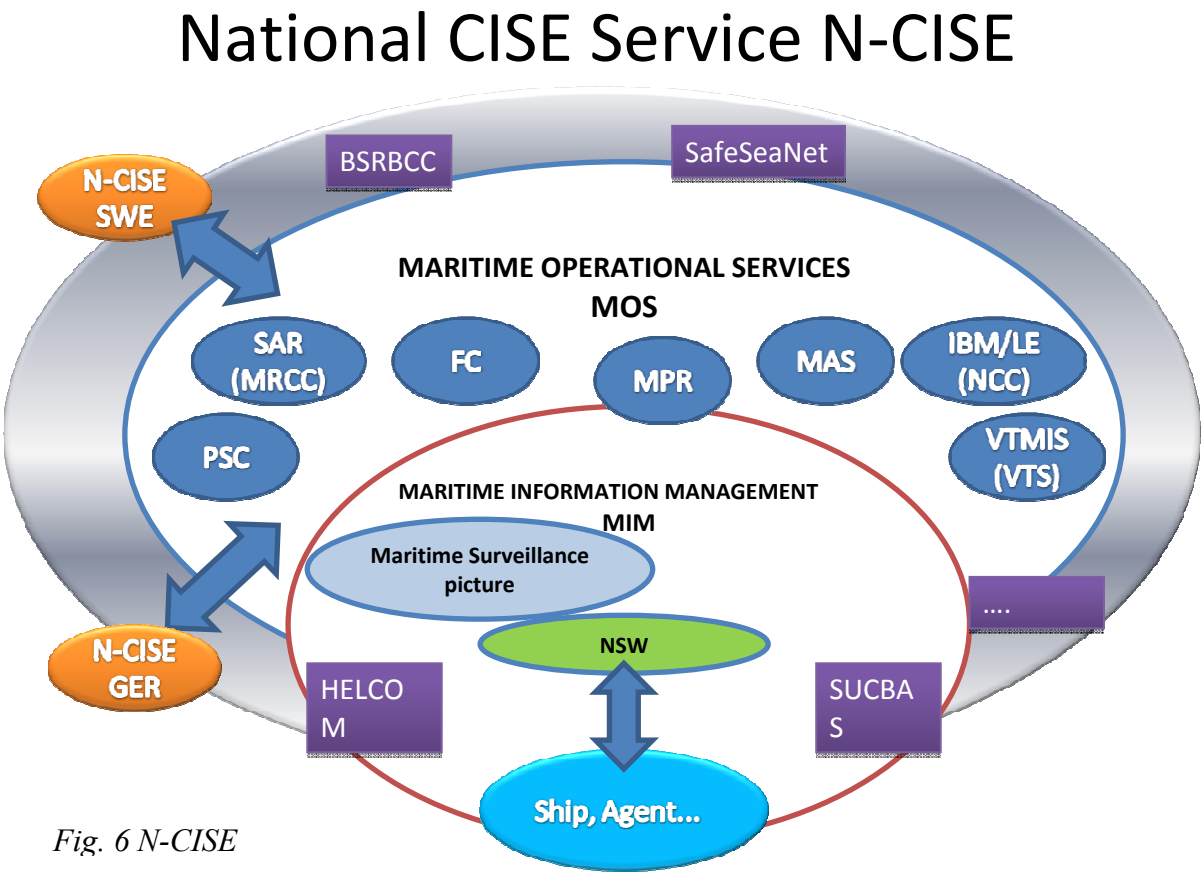


Fig. 6 N-CISE

4. Identification of Administrative, Legal and Technical obstacles that may hinder exchange of information in a long term perspective + Best practice and solutions to overcome identified obstacles (Objective 4 & 5)

To identify the legal, administrative, technical obstacles that may hinder the exchange of the above mentioned information on a long-term basis. To identify on the basis of the acquired experience in exchanging the information, best practices and/or legal adjustments needed to overcome the obstacles identified.

This chapter will focus on the MARSUNO Layers work of identifying and describing the administrative, legal and technical obstacles and to some extent the possible solutions or possible ways forward. All obstacles will not be described but the most important cross-layer obstacles will be summarised and analysed for the fulfilment of the MARSUNO tasks.

In order to achieve higher or full interoperability between existing systems cross sector and cross border, certain obstacles have been identified in MARSUNO and they need to be solved or at least thoroughly addressed in the continued CISE development.

When it comes to interoperability it has to be sustainable, meet the end users' requirements and follow the established CISE roadmap. Interoperability as defined in MARSUNO is also about the sharing of technical functionalities, not only at national and agency level, but also at an individual level.

Co-Financed under European Integrated Maritime Policy

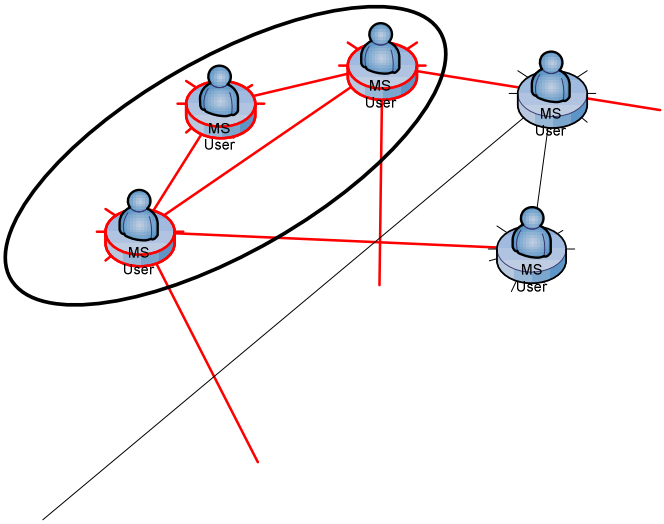


Fig. 7 Functional network connecting individuals and facilitating information sharing.

The line between administrative, technical and legal obstacles is sometimes thin and therefore some obstacles will be addressed in more than one aspect - the administrative, technical or in the legal subchapter, however with different approaches to the three aspects.

Some examples of this are the identified obstacles with accessing or obtaining information from military databases, which is in many ways a matter of legal constraints and in some cases technical, but in this also makes cultural/administrative constraints that need to be addressed. Another is the exchange of personal data to enable more efficient allocation of resources from the legal subchapter. This could be regarded as a national legal obstacle but consists of large elements of administrative or operational assessments.

There does not seem to be any insurmountable obstacles to exchange information within each sector cross border, as long as the purpose with the information stays the same. A possible way forward to enhance sectoral information exchange even further in a common environment is to look at the whole issue of gaining information from another agency as a question of granting authorisation to another agency.

The combination of cross-sector and cross-border information exchange is more difficult. This specific topic will be examined more thoroughly (see Section 4.4).

4.1 Experience from cross-sector workshop: Cross-sector information exchange related to all layers

4.1.1 Capability gaps and possible solutions for enhanced information exchange

The MARSUNO cross-sector workshop 15-17 March 2011 focused on identification of capability gaps and how to find possible solution paths to fill those gaps, aiming at an enhanced maritime information exchange and better coordination between authorities.

The workshop was based on three different cases for the participants to discuss during two Game Days. The workshop's ultimate objectives were twofold:

1) Identify technical, legal and administrative capability gaps and barriers for information exchange in the area of Maritime Situational Awareness and recommend potential solutions to overcome any such obstacles,
2) Strengthen international and inter-organisational relationships, and enhance data sharing efforts among cross-agency, cross-border and cross-sector Maritime Situational Awareness stakeholders

During the workshop, identification of gaps and inconsistencies in fields where cooperation between civil and military assets exist was also part of the discussions and valid for all work groups.

4.1.2 Results and recommended solution paths

Solutions with technical/administrative implications

- One of the central issues from the workshop was the recommendation of using CISE functionality in each Member State or Third Country. The advantage would be an easier ability to establish a common maritime picture. Efforts should also be put on creating solutions for maritime actors to share information in a continuous/automatic way and in a cross-sectoral way. A shared common maritime picture should be updated in real time (exchange of real-time traffic image).
- An increase of research and development of new technical solutions would be beneficial to the whole EU community.
- Authorities and international bodies needing information on the sea traffic situation should have permanent online access to VMS information from all countries.

Solutions with administrative implications

- Harmonisation of reporting burdens
- It would be an advantage to use common definitions/terminology in all communities e.g. based on regional agreements. Also to create solutions for maritime actors to have a good knowledge of available data in a cross-sectoral way (common definitions, standards, information sharing system, etc.).

Solutions with administrative/operative solutions

- Standardised international training and exercises should be promoted. Common operational procedures and agreements on e.g. Mass Rescue Operation and Aircraft Coordination matters and SAR combined with chemical or fire onboard situations are some examples of this.
- A common European system on storing and for availability of SAR Cooperation Plans for passenger ships has been requested. Amendments of EU Monitoring Directives with regard to responsibility areas correlating to Search and Rescue Regions (SRR) is another example.
- Create cooperative tools to assist in managing crises (virtual crisis room).

- The involvement of Third Countries should be improved and also improved exchange of information with private sector (e.g. shipping companies, ports, oil companies, and media).

Regional approaches

- Existing sub-regional/regional cross sectoral initiatives should be cornerstones in a system for managing crises.
- Russia has stated its willingness to exchange information within CISE, at a regional level.

4.2 Experience from Civil-military Seminar; Cross-sector information exchange related to civil-military sectors

4.2.1 Background

Gaps and inconsistencies in fields where cooperation between civil and military assets exist or where they could be developed or enhanced in the future have been analysed during the project time. One of several interesting questions has been to look into how to obtain or improve the conditions for cooperation between the sectors. This is also interesting from the perspective of civil operations with military support and vice versa military operations with civil support.

The civil-military seminar was an attempt to gather speakers with extensive experience of the present ongoing development within different projects in an EU context. Since one of the MARSUNO tasks is to investigate how decentralised network solutions might be connected between Member States, different sector system owners were invited to the seminar[22] to show how the information exchange is working in that context, both civil and military.

4.2.2 Civil-military aspects addressed during the seminar

Interesting aspects were shared during the seminar, of which several are supported by MARSUNO. Some items that were discussed were:

1. The importance of establishing links with Third Countries was emphasised. Comprehensive information exchange taking place between Member States provide a degree of security, but appropriate agreements must be in place with neighbouring countries as well. This is consistent with the discussions performed within MARSUNO.

2. The Wise Pen Team (WPT) emphasised the influence of TEU's Article 42, and in particular, Article 222, the Solidarity Clause, since the articles impose certain obligations on Member States, and both articles promote civilian-military cooperation.

3. The issue regarding lack of knowledge was discussed; "they don't know what they don't know". Such a lack of awareness is widespread amongst the naval, law enforcement, border surveillance, environmental protection, navigational safety and fishery control communities.

[22] Speakers from e.g. European Maritime Safety Agency (EMSA) and Frontex.

This has been one of the major findings of the WPT, that most security relevant information is available and being used within Europe, but is not shared with all the interested stakeholders. WPT recommends evolving from a 'need to know', through a 'need to share' to a 'responsibility to share' mentality. The relevant authorities need to be questioned as to why they are not sharing vital information. This is not only an appropriate question for military authorities, but also for civilian authorities and commercial companies such as ship owners.

3. Operation ATALANTA has been mentioned as a good example of creating effectiveness through establishing civil-military cooperation and coordination both ashore and at sea. WPT promotes the idea of establishing virtual civil–military headquarters with all stakeholders to be represented there. Stakeholders should then carry out information exchange and cooperation there in order to get to know each other and to build mutual trust and confidence. CISE experts should also be working together to find appropriate and affordable system solutions to interoperability problems.

4. The importance of connecting the CISE with transnational approaches proposed by the North Atlantic Coast Guard Forum and to link the coastguards of Russia, Norway, Iceland, the United States and Canada to the EU Member States.

5. The security arena lacks agreed definitions and operating concepts for security tasks which can only be solved by building trust and confidence. Operation ATALANTA might be used as a good example of how to build such trust at all levels – tactical, operational and, equally important, the political level in Brussels. When the political will exists, technical interoperability soon follows. The issue on building trust and confidence to strengthen the exchange of information is described in detail in Thematic Report Layer 1.

6. The MARSUR Network features are of interest and connect to the MARSUNO perspective. Features as:

- open architecture ,
- decentralised system layout,
- inter-agency as a national responsibility,
- legal aspects treated as critical, and
- the will to enable the exchange of unclassified and subsequently classified data.

The technical solutions used and developed within the MARSUR are based on open software, and this will also be the recommendation made by MARSUNO. The experience from MARSUR is that there comes a great challenge in sharing information, especially concerning the willingness to share, mainly defined as a cultural question (see above, point 5).

The MARSUR Network has been built to allow seamless compatibility with other sectors, and as such can be seen as a good example of best practice by other projects.

7. A lot of data is 'over-classified' and there is a need for downgrading classification levels. This might best be achieved by building trust and confidence. Therefore a 'step by step' development for achieving acceptance would be the appropriate way.

8. WPT supports the idea of keeping the responsibility at a national level. The CISE should be used for putting pressure on Member States to make additional contributions internally.

9. Direct communication between the civil and military communities is hard to obtain, and that friction is felt very clearly in some of the Member States. At EU level, relations are good between relevant agencies, however there are political obstacles preventing practical cooperation, and this needs to be addressed at a higher level. More aspects on how to overcome these obstacles will be elaborated further on in this chapter.

10. A panel discussion concluded the seminar where it was agreed that there is a need for stronger political guidance from the political level. A clearer maritime security strategy would be helpful for all parties involved. At the same time responsibility needs to be kept at a national level. Coordination activities at an EU level also need to be strengthened. The issue concerning use of social networks was discussed, where different opinions were reflected by the panel members. At a technical level, the use of more open networks would be helpful.

It has been mentioned by the WPT that one way forward in civil-military cooperation is the establishment of a joint centre. A joint civil-military HQ is no doubt a pragmatic and solution-driven approach. Civil shipping organisations could also be involved in this centre. This centre does not have to be a physical one; it could perhaps be a virtual centre, two or more nodes connected to each other via links. An open question to be discussed further is the idea of intelligence and fusion centres which could be a recommendation directed to EUROPOL to establish a desk for maritime matters in this sense. Policy making is a matter for the EU Commission/DG MARE.

4.3 Administrative obstacles (cross border/cross sector)

Different language and working methods have been identified as an obstacle by Layers 1, 3, 4 and 6 and tend to be the most obvious administrative obstacle. This is also a general and larger issue that, in order to be solved, has to be broken down into smaller parts. One large part of this is the identified need for common standards.

The need for common standards for operational procedures, language and working methods are clearly highlighted by several layers. Common standards for routine work and information exchange within the common environment are identified as of great importance. However each sector/layer will most certainly keep and develop specific sector standards for nomenclature, working methods and operational procedures. Within the CISE there will be need for several different common standards depending on the purpose of the exchange of information.

When exchanging information cross sector the need for an essential/basic level of common standards is vital. There will be a need for essential/basic level of standards within CISE;

- per sector,
- legal,
- technical,
- operational, and
- administrative.

Co-Financed under European Integrated Maritime Policy

In the concept of common standards also includes the ability to communicate and the possibility of communication between people. Several of the identified obstacles can, to some extent, be solved by an enhanced communication cross sector and cross border. If communication is facilitated and improved this could very well be a natural way to overcome some of the obstacles to improving interoperability and information exchange cross border and cross sector in a common environment.

Layers 1 and 6 have identified the need for N-CISEs. The need for this was clearly emphasised and the reasons for it has been developed under Section 3.2 in this report.

This responsibility means that each N-CISE must provide assistance, guidance, advice and such other assistance in full compliance with the national legislation. The questioner should not have to think or find the proper authority in another country. The N-CISE will refer and assist so that the information or question arrives at the competent agency.

Different communication tools can be set up in order to enhance and facilitate communication. During the MARSUNO Demo the need for standardisation of video conference link was highlighted and of great importance. The benefits and added value with such communication system were also clearly identified and the information exchange was facilitated and enriched by use of;

- video link,
- telephone communication, and to arrange
- meetings between people engaged in the maritime domain cross border and cross sector. MARSUNO is a good example of information sharing between cross-sectoral personnel working in different layers.

Layers 2, 3 and 4 all identified that several areas of littoral waters of Northern Europe have declared and established areas in which remedial services such as SAR and MPR are carried out overlap to some extent or do not coincide. This lack of overlapping may result in confusion in a combined SAR and MPR operation and needs to be addressed and solved in order to avoid uncertainties.

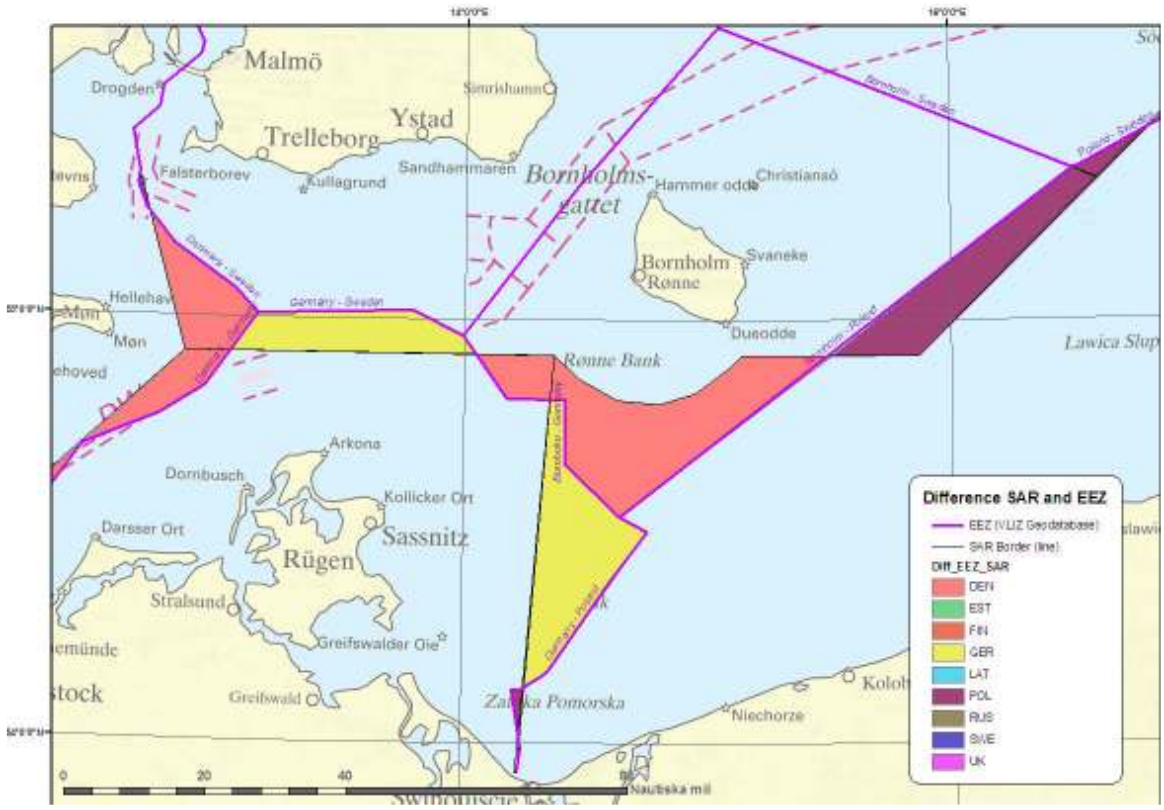


Fig. 8 Example of conflicting SAR and MPR borders from Northern Sea to the Baltic Sea.

The need for better Aircraft Co-ordination and better multi-mission tasks for air surveillance platforms is also well described in the thematic reports from Layers 3 and 4. One example is the challenges concerning joint mass rescue operations. Here is an identified need for improvement of relevant operational procedures. This topic is also of relevance for the other Layers.

The Layer 3 MPR recommends that a common environment makes better use of information gathered, for example connecting satellite images to the VMS signal. This suggestion for improvement is connected to data fusion and will be elaborated on further. It is also a question of improved operational procedures.

The issue of willingness to share information with another agency is identified by Layers 1, 2 and 6 as an obstacle. The information is not always shared even if the information is not under any constraints for sharing and this is a problem both nationally and internationally. Here lays also the problem with over classification of information.

An interesting topic that should be analysed in the aftermath of MARSUNO is the transferring of leadership in a certain case/issue between sectors within a country and cross border. This issue was identified by Layer 1 IBM-LE and needs more attention than a comment in the thematic reports. This could also be beneficial in order to facilitate the implementation and make better use of the possibilities with Joint Investigation Teams (JIT) in different areas, ranging from criminal investigation to accident investigation.

Co-Financed under European Integrated Maritime Policy

Layer 5 FC has identified two obstacles that touch the very nerve of problems concerning information exchange and that is how to obtain relevant and needed information from identified databases and to get knowledge about where the information is to be found. What to share, how, with whom and for what purpose. Another area of improvements that was identified by Layer 5 FC was that the recommendation of how transparency regarding the VMS could be improved. All VMS information should be available for all Member States, not only during the Joint Deployment Plan, JDP.

One obstacle that needs to be solved in order to develop system architecture is that a methodology for the determination of information sharing has to be in place. MARSUNO and the BMM together with the TAG group have started the process but it is imperative that an information sharing methodology is established.

Layers 1 and 6 have identified the need for national Points of Contact (PoC). The need for this was clearly emphasised, but how this PoC should be organised is not so clearly described and could very well differ between countries as long the responsibility at the national level is clearly established. Further on the PoC will be equal to the N-CISE. This responsibility means that each N-CISE must provide assistance, guidance, advice and such other assistance in full compliance with the national legislation. The questioner should not have to think or find the proper authority in another country. The N-CISE will refer and assist so that the information or question arrives at the competent agency. The N-CISE functions should be in focus rather than the organisation so harmonisation of operational procedures could be facilitated. The organisational structure at the national level will most certainly differ among the involved countries, but the functions must be standardised and in place for common work within the CISE.

4.3.1 Best practice

The core question is to find the proper balance between technical and operational requirements, legal framework and financial limitations in relation to the possibilities of added value for the different sectors. Some good examples of information exchange cross border and cross sector already exist. Two of these examples are presented in brief in this subchapter.

Regional cooperation has been proven as a good and reliable way to exchange information. This is well formulated in the Thematic Report from Layer 1.

"Therefore, it can be concluded that regional form and structure is necessary for effective cooperation. By using regional structure it is possible to attain sufficient level of practical contacts and information exchange between counterparts, and consequently good results. It is important to highlight concepts of practical and also operative cooperation which are key elements for counterparts which have the same operational area, common needs and similar goals"[23].

This statement from Layer 1 is applicable on almost every sector. If you then connect the regional networks with each other the chain of cooperation grows and with that hopefully the information between different agencies in different geographical parts of Europe increases.

[23] Thematic Report Layer 1 – IBM-LE

Two examples of regional cooperation are cooperation within the environmental protection and response sector and the second one for law enforcement sector; however the example from law enforcement also contains some elements of cross sector information exchange.

HELCOM
The Convention for the Protection of the Marine Environment of the Baltic Sea Area (Helsinki Convention) has a wide scope and covers pollution from all sources: from land, sea- and airborne. Of relevance to Layer 3 is the co-operation in the field of acute MPR. All nine Baltic Sea States as well as the European Union (represented by the EC, and Maritime Situational Awareness) participate in this work within the HELCOM Response Group. Apart from co-operation in developing response capacities, the HELCOM Response work also covers beach cleaning, aerial surveillance for oil spills, multilateral development and use of a common web based oil drift forecasting and hind casting tool and coordinated use of Maritime Situational Awareness-provided satellite images[24].

Baltic Sea Region Border Control Co-operation, BSRBCC
Cooperation throughout the entire Baltic Sea Region includes combating cross-border criminality (e.g. trafficking, illegal immigration, document forgeries, use of vessels and other watercraft for illegal activities), environmental protection of sea area (e.g. use of joint surveillance and pollution prevention resources, maintenance of situational awareness of entire Baltic Sea Region and working together to investigate crimes detected) as well as technical maritime development projects to foster border security (e.g. exchange of experiences of tools and equipment as well as Coastnet and BALMIS project.

Aspects of cooperation are;
- information exchange,
- surveillance data exchange, and
- common operations.

4.4 Legal obstacles (cross border/cross sector)

4.4.1 Introduction

Core legislation
Within the scope of this Project, i.e. achieve a higher degree of interoperability among existing monitoring and tracking systems – information exchange - in order to improve maritime surveillance, there are a great number of different Regulations and Directives that play a decisive role for the actors implicated. They establish a natural basis for this part of MARSUNO, where the legal conditions are studied in detail, obstacles, gaps and hindrances are identified and finally proposals to overcome these legal obstacles for new and amending legislation in force are presented.

The following Directives form the core of the main problem area:

[24] MARSUNO –Thematic Report Layer 3 Marine Pollution Response (MPR): p 9.

- Directive 95/46/EC on the protection of personal data and on the free movement of such data, Data Protection Directive,
- Directive 2002/59/EC[25] on establishing a vessel traffic monitoring and information system, VTM Directive,
- Council Regulation (EC) No 1224/2009[26] on establishing a control system of the common fisheries policy, Common Fisheries Control Directive,
- Regulation (EU) No 404/2011[27] on detailing rules for the implementation of the Common Fisheries Policy, Fisheries Implementation Regulation,
- Regulation (EC) No 725/2004[28] of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security, ISPS Directive,
- Directive 2005/65/EC[29] on enhancing port security,
- Regulation (EC) No 562/2006[30] on the rules governing the movement of persons across borders, Schengen Border Code.

What is B.A.R.?
The Project has identified, from and for the purpose of the operative level, three categories of information, where the difference is determined by its sensitivity; basic data, additional and restricted. In short it is called as the B.A.R., and is explained in more detail, see Section 2.3.1 above.

Basic data is such data for which the exchange does not entail any constraints and is thus free to transfer. What **A**dditional data is, is a little more diffuse. Firstly, additional data is not the same as restricted data. MARSUNO has concluded that additional data is still to be considered as basic data, but data that is requested to enable a more complete picture and often only accessible from certain selected source or sources. It is important to underline that from a legal perspective there are no legal differences between basic and additional data.

Restricted data is simply data of which the availability is restricted by law.

---

[25] Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC OJ L 208, 5.8.2002, p. 10–27

[26] Council Regulation (EC) No 1224/2009 of 20 November 2009 establishing a Community control system for ensuring compliance with the rules of the common fisheries policy, amending Regulations (EC) No 847/96, (EC) No 2371/2002, (EC) No 811/2004, (EC) No 768/2005, (EC) No 2115/2005, (EC) No 2166/2005, (EC) No 388/2006, (EC) No 509/2007, (EC) No 676/2007, (EC) No 1098/2007, (EC) No 1300/2008, (EC) No 1342/2008 and repealing Regulations (EEC) No 2847/93, (EC) No 1627/94 and (EC) No 1966/2006 OJ L 343, 22.12.2009, p. 1–50

[27] Commission Implementing Regulation (EU) No 404/2011 of 8 April 2011 laying down detailed rules for the implementation of Council Regulation (EC) No 1224/2009 establishing a Community control system for ensuring compliance with the rules of the Common Fisheries Policy, OJ L 112, 30.4.2011, p. 1–153

[28] OJ L 129, 29.4.2004, p. 6–91
[29] OJ L 310, 25.11.2005, p. 28–39
[30] Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code) OJ L 105, 13.4.2006, p. 1–32 and its amending Regulations

Basic principles

The predominant issue at hand is the processing of personal data. Therefore it is important to keep a few points in mind, which establish the very basis for transferring such data. The legislation in place, the Data Protection Directive establishes two principles. It requires that the data must be processed fairly and lawfully. Further it requires that the data may only be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes *(the principle of purpose-limitation*). In addition, personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (*the principle of proportionality*). In addition personal data has to be accurate and necessary and kept up to date.

The civil-military information exchange concept

Furthermore the project has examined the conditions for better exchange of information pertaining to the maritime domain between the civil and military communities. The scope of the cooperation is to enhance security within the Union and its Member States, and outside. A number of strategic statements on Union level have been made; Art. 42 Treaty of the European Union (TEU), Art. 222 Treaty on the Functioning of the European Union (TFEU) and Title V of the TFEU, directly indicating responsibilities, obligations and possibilities and measures for an increased cooperation and efficient resource allocation in cases of need.

The issue on information exchange between the two communities has been subject of earlier studies and Union measures, see Communication from the Commission Com (2009)538[31] and the Roadmap towards establishing the Common Information Sharing Environment (CISE) for the surveillance of the EU maritime domain[32]. Apart from the regular questions at issue such as processing and transferring personal data and handing of confidentiality requirements and professional secrecy matters they also address of course the military data sharing between the communities. The latter is uniquely and closely linked to the question of classification.

The Project has, similar to Commission papers mentioned above, concluded that the processing of personal data for military, state security and criminal law enforcement are matters usually regulated separately from the general legal framework for data protection. The Military data protection is then addressed in specific legal instruments fitted for these fields, both at Community and Member State level.

The general conditions for military authorities for exchanging personal data are very much similar to the ones governing the exchange between civilian authorities. The exchange of personal data should fulfil all the applicable regulations in place without any exception, meaning that the same principles, as stated above, should be upheld. Regarding information that could be subject to confidentiality, the processing and the onward transfer of this type of data will need to ensure that recipients of the data are equally bound by confidentiality and professional secrecy obligations. As mentioned earlier, the purely military data falls outside of the regular framework and is treated in custom fit legislation. This type of data seems to be of

[31] Communication from the Commission to the Council the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain, {SEC(2009) 1341}

[32] Communication from the Commission to the Council the European Parliament on a Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain, COM(2010)584

no material necessity for the accomplishment of the tasks falling under the duties pertaining to maritime safety or law enforcement. For this reason it seems outside of scope for MARSUNO to include this kind of very designated and special data into the assessment of obstacles and the finding of solutions for the better exchange of information between civil and military authorities.

On the other hand, the problems arising during a transferring measure or action of data or information that does not pertain to the purely military area seems to mainly emanate from the classification regime within the military, and security, communities. Security of information is already regulated on Union level[33]. Though, the classification[34] almost inevitably leads to over-classification, even though this is explicitly discouraged in the referred to Council Decision (INFOSEC) referred to. It is understandable to administer the flow and access within the security community, including both civil and military authorities but the effects of such a regime are clearly counterproductive to the efficiency of a system in need of exchanging relevant information and in right time. From a legal point of view there are no valid grounds for amending or adapting the regulation at the Union level. The solution lies in the administration of such a system. MARSUNO would in these situations, where efficient interoperability between the two communities is at stake, advocate for a governance solution taken care of by agreements between the parties, rather than legislating the administration.

4.4.2 Legal obstacles observed

1. Constraints due to protection of personal data.
The two main, and for MARSUNO relevant instruments of EU data protection law, are the Data Protection Directive and the Data Protection Regulation. The Data Protection Directive seeks to enable the free flow of data between Member States, by harmonising national rules, while at the same time ensuring that the fundamental rights of individuals, notably the right to privacy, are protected with regard to the processing of data.

The Data Protection Directive defines the concept of 'personal data' very broadly. Basically it means any information relating to an identified or identifiable natural person. The concept 'identifiable person' is further defined as one who can be identified directly or indirectly by reference to an identification number or one or more factors specific to his physiological, mental, economic, cultural or social identity. Using such broad definitions result in uncertainty concerning particular items of information. For example, may a telephone number, car registration number, social security number or passport number be sufficient to render someone directly or indirectly identifiable and thus may this, in the context of a particular situation, amount to personal data. Furthermore, in certain circumstances information on legal persons may also amount to personal data, for example where the name of a legal person derives from that of a natural person. Consequently while it seems reasonable to conclude that the name of a vessel may not as such be sufficient to directly identify a (natural) person owning the vessel the unique combination of the vessel's name with other data elements, such as a unique vessel registration number, that enable the

[33] Council Decision of 19 March 2001 adopting the Council's security regulations (2001/264/EC), OJ L 101, 11.4.2001, p. 1–66 (INFOSEC)
[34] top secret/secret/confidential/restricted

identification of a single person (vessel owner, captain, crew etc.) may amount to personal data. Furthermore, pictures, including CCTV images and other visual data may also be considered personal data if they permit the identification of a natural person. Taking the above into account, analysis of the maritime monitoring and surveillance data described above leads to the conclusion that they could potentially involve personal data. To take one example, where data concerns a fishing vessel identification number, a licence number or external registration number or other unique identifiers this may lead directly or indirectly to identify a natural person. While in the large majority of cases the owner or agent of a vessel will be a legal person this may not always necessarily be the case. Various references made in the legal instruments described in this Project e.g. Community fisheries legislation, the Port Security Regulation and the Schengen Borders Code, suggest that data protection concerns were taken into account from the outset[35].

In line with what has been described in the Project regarding processing of personal[36] data, it is also necessary to examine the basis for restraining the sharing of such data pursuant to data protection law. The two principles mentioned above, the principle of purpose-limitation and the principle of proportionality, restrict the possibility to exchange personal data.

Purpose-limitation is one of the cornerstones of data protection law; personal data can only be processed for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Following the principle of proportionality, processing of personal data must be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed.

Personal data can therefore, in principle, not be processed for purposes other than the purposes for which they were collected. A clear and precise description of the purposes of data processing is therefore of crucial importance. In the same way, it needs to be clearly defined who is the data controller, i.e. the person responsible for the processing of the data and thus for compliance with data protection law.

From the perspective of data protection law, the processing of personal data needs to remain restricted to the competent authorities or organisations designated for such processing; and the purposes laid down by the relevant legislation allow the processing.

A number of examples of the purpose-limitation of data processing can also be found in the maritime sector legislation described in MARSUNO. The overall effect is that data collected and processed by a certain authority with a specific purpose cannot then be used for a different purpose just by virtue of the different, possibly broader, competence of the receiving authority. In other words the purpose of the processing of data is therefore of crucial importance.

35 Excerpts from European Commission Final Report Legal Aspects of Maritime Monitoring & Surveillance Data, Framework Service Contract, No. FISH/2006/09 – LOT2, p. 94-134. included in this section.

36 Processing is defined by both the Data Protection Directive and the Data Protection Regulation as 'any operation or set of operations which are performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'.

As regards data sharing another important principle of data protection law is that data may not be transmitted to recipients outside the European Economic Area (EEA), Third Countries, which do not ensure an adequate level of protection. Only a few non-EEA countries currently meet these criteria. However data transfers outside the EEA may take place if adequate safeguards are put in place as a result *inter alia* of appropriate contractual arrangements. Data protection law also imposes a duty on controllers of personal data to implement adequate security measures and to keep such data confidential and confers certain rights on data subjects, such as the right to access and consult the data and to request rectification of inaccurate data.

It is also important to note that data protection legislation does not automatically apply to the processing of all personal data. Exceptions include the processing of personal data in the course of an activity that falls outside EU law *e.g.* the common foreign and security policy and police and judicial cooperation in criminal matters, as well as processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law, see above under Section 4.4.1 and below under point 5.

However there are some exceptions which make it possible to exchange personal data. For example if a Member State needs the personal data for their authorities´ work it is possible to exchange personal data but only if the personal data can be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The exchanged personal data must also be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed and the personal data have to be accurate and necessary, and kept up to date.

According to the Data Protection Directive every Member State shall determine more precisely the conditions under which the processing of personal data is lawful. This rule may result that the Member States have different legal solutions which leads to legal obstacles.

The issue of the routine exchange of personal data cross border and cross border/cross sector to Member States and routine exchange of personal data cross border and cross border/cross sector to Third Country also adds another level to the dimension.

The main reason for this conceptual perception of a legal obstacle is based on the actual ‘need’ to acquire the maximum amount of data possible as soon and as easily as possible. In short, it is pure transferring efficiency rather than overcoming any legal embarrassment. From a legal point of view there is basically no difference between giving access to one piece of data compared to transferring data in bulk or in a routine manner. A request for accessing registered data of personal character has always to be assessed before being handed out. The fact is that there are no legal restrictions as such for the routine exchange or the like, at least not at the Union legislation level. The possibility mentioned above for the Member States to further detail the processing and transfer of personal data may though of course entail in a few cases ‘hurdles’ rather than obstacles. A common approach by Member States is to legislate for different sectors separately and by setting requirements to be met by the receiving authority before accepting any transferring of personal data. The basis for admitting transfer of data is commonly that the purposes involved must correspond. When the requirements are met, then the legislative tool used opens either up for transferring for a individual request or enables so-called ‘direct access’ to the database belonging to the data registering authority. It now stands

clear that there are actually no real legal obstacles – access to the data in question is generally not denied for integrity protection reasons, but instead there is an access problem.

The issue whether and how problems occur between Member States is generally easy to answer. As mentioned above, the Union legislation does not involve any restrictions apart from the principles to be applied with. However, at the national level additional requirements or even direct prohibitions may be stated regarding transfer of personal data. However, Member States usually seem to have a common shared view on this. An common positive basis for accepting transfer cross border to an authority in another Member State is that the transferring authority has the right to transfer the data to another national authority with the same purpose, e.g. law enforcement etc. This is considered as a sufficient safeguard of the protection of personal data and that the purposes will be compatible with the purposes for collection.

Considering transfer of personal data to a Third Country is slightly more intricate than the above mentioned intra-Union transfer. The Data Protection Directive states clearly under what circumstances a request may be admitted. As regards data sharing the data may not be transmitted to recipients outside the European Economic Area (EEA) who do not ensure an adequate level of protection. The process in these situations includes an additional assessment as to whether the recipient fulfils the safeguard requirements besides the one that the transfer of the actual data is admissible. In conclusion these circumstances cannot be deemed as legal constraints as such as they are neither contradictory nor inadequate. The criteria are fully in line with the purpose of safeguarding the protection of personal integrity.

2. Constraints due to confidentiality, secrecy and access to documents

Apart from the possibility regarding certain data concerning e.g. ship's name, crew list, ship's port history, ship's route history and so on as so-called personal data and thus falling within the protection measures through the Data Protection Directive this kind of information and the like may also fall under the application of regulations concerning confidentiality, secrecy and access to documents. The restrictive treatment of such data can be a potential barrier to its exchange.

Confidentiality can originate either by law due to the inclusion of express legal provisions to this effect or on the basis of contractual provisions. A number of the legal instruments cited in this report e.g. VTM Directive, Common Fisheries Control Directive contain examples of confidentiality provisions.

For example the various regulations that establish the legal framework for VMS contain references to the confidentiality of VMS data, the requirements for such data to be 'treated in accordance with applicable rules on professional and commercial secrecy of data'. Such provisions do not constitute an obstacle, as such, to the exchange of data between Member State relevant authorities, such as Fisheries Monitoring Centres – FMCs, and the European Commission in accordance with the conditions set out in the regulation. However, recipients of such data are obliged to observe confidentiality and in general terms may not, therefore, disclose it to third parties not specifically mentioned or in accordance with the options given within the relevant legal framework

Co-Financed under European Integrated Maritime Policy

Similar provisions are found in the VTM Directive with the effect that while data must be exchanged between relevant Member State authorities in accordance with the requirements of the directive, all recipients are themselves under a duty to keep the data confidential and thus they may not share such data with non-designated authorities. The applicable grounds for denying the processing, sharing or exchange of such data are mostly for professional and commercial secrecy reasons.

With regard to confidentiality provisions imposed by contract one example is the standard agreement of Lloyds Register Fairplay Limited relating to AIS Live which imposes a duty of confidentiality on users and effectively prohibits unauthorised third party re-use. Similar provisions are to be found in the end-user licence for CleanSeaNet including a purpose limitation, the effect of which is that Member States may use the data solely for the purpose of oil spill monitoring. Typically agreements of this type also include provisions on the protection of the data supplier's intellectual property rights.

Closely connected to this subject, sharing of information which is considered as confidential, is information that is treated as *classified.* Classification is however not the same thing as confidential. Classification may be looked upon more as an administrative solution to access rights to information depending on its sensitivity. The data itself may be considered as 'free' but between agencies it is not available to certain categories of personnel without clearance or level of authority. On top of this, one may take into account the fact that existence of (the variety of) different national classifications in and between Member States regarding the same types of data produces significant hinders for any effective cross-border information exchange. It is quite clear that this is NOT a LEGAL constraint as such, but still it presents the possibility of problems for the authorities in need of information.

Access to documents is exclusively regulated by law, both at the EU and Member State levels, which generally contain grounds for refusal of access to certain data. The relevant laws and regulations which exist at usually contain a number of grounds for refusal of access to certain data. A general conflict is the one where confidentiality or secrecy obligation is invoked by a contract towards an authority and the latter is obliged by law to give access to documents. The information contained in the contract may be the subject of publicity while the intent of the contract obligation, to protect, will – most certainly be set aside - as the law prevails in such situations. Nonetheless, provisions in such public access legislation usually provide sufficient protection limits safeguarding sensitive information and the subject it pertains to.

Finally it should be noted that the main legal instrument at EU level is Regulation 1049/2001 of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, Transparency Regulation[37]. This framework does not seem to be directly relevant to the exchange issue covered by the Project as it applies not only to documents drawn up by the institutions but also to documents received by them, in all areas of activity of the EU. In principle, all documents of the institutions should be accessible to the public. The purpose of the Transparency Regulation is to ensure the best possible access to documents. Furthermore it should be noted the Transparency Regulation recognises that certain public and private interests may need to be protected by way of exception to the general rule. Therefore, the

[37] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, 31.5.2001, p. 43–48

Transparency Regulation lays down a number of exceptions where the institutions may refuse access. In the same way, the Transparency Regulation provides for special treatment of documents with a highly sensitive content. Most important though is that the Transparency Regulation does not prejudice to any existing rights of access to documents for Member States, judicial authorities or investigative bodies. Neither does the Regulation prejudice any rights of public access that would be granted by instruments of international law or by acts of the institutions implementing those instruments

3. Constraints due to data security policies of public authorities.
Every Member State has its own different data security frameworks. This diversity entails difficulties to gain knowledge on how to know which information is possible to exchange and how to execute the actual exchange.

First we have to define what a *data policy* may comprise. A Data Policy can consist of either or both of the following:

- a high level statement of direction or strategy with respect to data quality, security, or internal standards. The statement is defined by the purpose of the business, and agreed to by senior management, in accordance with the current legislation. The policy would usually be submitted for agreement by the Data Governance Council or other designated internal authority, and/or
- a set of measurable rules defined, implemented and enforced as a unit for a set of data elements, in the context of the purpose of the organisation, for the benefit of a business process, irrespective of the parties that provide the data and where the data is stored. Technical rules are defined by technical staff such as IT managers, System Developers and Data Stewards. Work is performed under the guidance of a System Owner, who will ultimately be accountable for monitoring policy compliance.

The authoring of a policy therefore is a joint effort between business and technical staff. Once the policy is approved, it must be shared with those who must comply with the policy, and with those who need the information to better perform their day to day activities.

Data policies can be categorised according to type, for example:

- data protection and secrecy legislation,
- data quality,
- life cycle management,
- security, and
- data model management.

Data policies at European institutions and bodies and authorities within Member States may involve another barrier to data exchange while governing rules of classification of data. Such rules are usually adopted to develop and safeguard activities in areas which require a certain degree of confidentiality. Data security and classification policies may be especially relevant for military authorities.

Of some relevance, the Public Sector Information Directive 2003/98/EC[38] should also be mentioned. The Directive provides for minimum rules applicable in all the Member States as to the re-use of public sector information resources, may potentially be relevant to the sharing of maritime monitoring and surveillance data in cases where bodies involved in the sharing of such data operate under a semi-privatised structure or in situations where public sector bodies themselves act in a commercial sphere.

The main issue regarding this type of problem concept is the innumerable diversity of policy frameworks based on the vast different constructions, both within a Member State, cross-sectoral and consequently cross-border wise, leading to a confusing overview and the ensuing difficulty of management to reach solutions for efficient exchange of information.

4. Exchanging criminal intelligence information.
In principle this kind of information or data is considered as very sensitive. It is sensitive from two points of view; as an integrity protection interest for the person implicated as any uncontrolled dissemination could lead to great losses socially and in other valued areas, and, as a safeguard measure to secure a criminal investigation from interference disturbing and risking a positive outcome.

Two different issues play a role here, first the general issue of legislation, and secondly when transfer is at hand whether it concerns cross border or cross sector. The latter may also involve a cross border element. Generally speaking criminal intelligence concerns two categories of data; personal data and other data. The latter may in its turn be separated in two blocks; basic and sensitive data.

To begin with the personal data aspect; this area is covered by a general Union legislation, the Data Protection Directive. Member States have possibilities to further determine more far reaching measures when implementing the Directive. This leads to differences between Member States, which will incur compatibility issues when demanding cooperative actions between the cooperating parties. Often in the national legislation transferring of such data is allowed only, or more correctly, restricted, to similar purposes or at least within the similar sector (depending on its definition, case by case). National legislation as a default prohibits any kind of cross-border dissemination of personal data, regardless of the recipient. Exception is made for situations where the receiving State is considered to provide the same level of protection as determined by the Directive. Furthermore, within the Union, the transfer of personal data may be allowed if the transferring authority in the sending Member State has the right to transfer the data to a similarly designated authority within the Member State.

Concerning the other category of data, non-personal data, this seems to be regulated insofar as the Data Protection Directive does not apply. Here it merely seems to be an issue of how to handle data within the public access to documents legislation within each Member State. The different national frameworks lay down a number of exceptions where the registering authority is obligated to refuse access, often based on the assessment of harmfulness due to the sensitivity of the information. Member States choose usually to regulate possibilities for

[38] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information *OJ L 345, 31.12.2003, p. 90–96*

transfer of such sector wise, nationally and internationally. The grounds for admitting transfer show great diversity within and between Member States.

The matter of classifying schedules within the Member States do also apply, but as has been discussed previously, is mainly not a legal problem as such but more a procedural one. Still it presents as an obstacle for transferring information.

A step further down the criminal investigation chain, when court measures have been taken and cooperation is asked for between Member States, there are procedures regulated at Union level.

Below is shown an, non-exhaustive, overview of the main frame works related to information exchange for the purpose of criminal investigations and criminal intelligence operations in the pre-trial phase in the EU:

Work Name	Legal Basis	Objectives
FRONTEX	-Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the external Borders of the Member States of the EU	To coordinate operational cooperation between Member States in the field of managing external borders and carry out risk analyses
SCHENGEN – SIS	-Convention implementing the Schengen Agreement of June 1985; -Council Regulation 1987/2006 of the EP and COUNCIL of 20/12/2006 on the establishment, operation and use of the second generation SIS (SIS II); -Council Decision 2007/533/JHA of 12 June 2007 on establishment, operation and use of the second generation SIS (SIS II); -Commission Decision 2008/334/JHA of 4 March 2008 adopting SIRENE Manual and other Implementing measures for the second generation Schengen Information System (SIS II),	Maintain public order and security, including border control, state security, and to apply the provisions of the Schengen Convention relating movement of persons (article 93)
CUSTOMS INFORMATION SYSTEM (CIS)	-Convention on the use of information technology for customs purposes (CIS Convention-95); -Convention on mutual assistance and cooperation Between customs administrations (Naples II Convention) of 1997, the equivalent instrument for prosecution of offences against Community Law in the Customs sphere, which is the current basis for exchange of information to prevent and detect violations of national customs legislation, Third Pillar matters, and for prosecutions in relation to EC interests, i.e. First Pillar matters	Assist in preventing, investigating and prosecuting serious contraventions of Community Customs or Agricultural legislation or which constitute serious infringements of National law in these or related areas

Co-Financed under European Integrated Maritime Policy

	-Council Regulation (EC) No 515/97 of 13/3-97 on Mutual assistance between the administrative authorities of the MS, as amended; -Council Regulation (EC) No 766/2008 of 9/7-2008 amending Regulation (EC) No 515/97;	
EUROPOL	Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office, which replaces the provisions of the EUROPOL Convention	Support and strengthen action of the Member States in combating organised crime and other forms of serious crime, affecting at least two Member States
Swedish Initiative	Framework Decision 2006/960 JHA on simplifying The exchange of information and intelligence between LEA of the EU Member States	More effective and expeditious exchange of existing information and intelligence for the purpose of conducting criminal investigations or criminal intelligence operations
Prüm Decision	-Council Decision 2008/615/JHA of 23 June 2008 on stepping up of cross-border cooperation, particularly combating terrorism and cross-border crime; -Council Decision 2008/616/JHA on the implementation of the Council Decision 2008/615/JHA	Step up cross-border cooperation and exchange of information between authorities responsible for the prevention and investigation of criminal offences (no collection, storing and supply of personal data)

Furthermore, Eurojust plays an important role where its purpose is to increase the exchange of information between the interested parties, facilitate and strengthen cooperation between national authorities and Eurojust, and strengthen and establish relationships with partners and Third States[39].

An additional framework and legal tool should also be mentioned too, which does not fall within the European framework as such, but plays a significant role in the crime combating arena, and this is INTERPOL[40]. The purpose is to facilitate international police cooperation and the enabling of police in all its member countries to request, submit and access vital data instantly in a secure environment.

The purpose of these different legal frameworks and tools are to facilitate the collection of and sharing information between national authorities and other European players in the area of justice, freedom and security. It is of essential importance to understand that a few of these

[39] In the context of investigations and prosecutions concerning two or more Member States, Eurojust's goal is to stimulate and improve the coordination between the national authorities, taking into account any request emanating from a competent authority of a Member State and any information provided by any body competent by virtue of provisions adopted within the framework of the Treaties (European Judicial Network, Europol, and OLAF).

[40] Its legal basis is: INTERPOL Constitution and General Rules; Implementing rules for the rules on the processing of information for the purposes of international police cooperation; International agreements with states and other organisations

frameworks state policies, and subsequently require implementation to a national level to be fully and efficiently applicable, mainly the Swedish Initiative and the Prüm Decision.

5. Accessing to military databases.

For the civil community the exchange of personal and sensitive data poses the most problems for the military community. In addition problems occur when trying to coordinate the cross-border exchange between military authorities and (cross-sector) authorities in the civil community. However, the military community has though shown considerable cooperation throughout the EU and also internationally, such as SUCBAS, MARSUR, MSSIS, etc

As discussed in the Introduction section above, more or less the same 'problems' occur when considering exchange of personal data and (civil) information subject to confidentiality restraints from or to the military community to or from the civil community. On the other side, regarding data which falls under the responsibility of the military authorities, exchange may be admitted after due assessment based on totally different grounds, such as state security needs. In summary, the Project does not find any specific civil-military legal obstacles hindering the exchange between these communities, at least not more than what is the situation as described and discussed regarding the civil community, see above points 1 and 2.

Besides the common area of processing of personal data, the handling of classified information (non-personal) may also raise an obstacle for exchanging data. Within the EU this has been thoroughly regulated[41] which sets common standards for e.g. classification. Nevertheless it is a common experience that the use of classification routines may incur a certain 'over classification', which may incur hindrance rather than being an obstacle. One, efficient, approach could be to invite the civil and military communities to adopt classification systems adapted to their shared conditions.

6. Difference between Member States legislation and the administrative provisions concerning protection of personal data.

As mentioned above, the Data Protection Directive[42] gives the Member States possibilities to further detail conditions on processing and transferring personal data. This leads inevitably to numerous solutions, which consequently can or cannot be compatible with other similar legislation in another Member State. In addition the procedural solutions differ widely between the Member States, due to constitutional reasons, which then demand time consuming measures for any kind of amendment or adjustment, or simply different legal systems. In any case, these differing conditions are not 'problems' but they are merely the effect of having different answers to the same question(s).

This situation does not only limit itself to transferring of personal data. The VTM Directive and the Common Fisheries Control Directive opens up for a similar differing situation as they both take into account national legislation governing the processing of data falling under confidentiality restrictions. Consequently even in these cases procedure may differ between Member States and raise hinders during the cooperating.

[41] Council Decision of 19 March 2001 adopting the Council's security regulations (2001/264/EC), OJ L 101, 11.4.2001, p. 1

[42] See preambles 7-10

4.4.3 Suggestion for amendments, adjustment and new legislation to overcome the obstacles

The following suggestions are not to be read as alternatives to one another, meaning that either suggestion may solve and meet all types of exchange induced problems, not at all. On the contrary, the Project has identified a number of 'problem sources'. That is why the Project is presenting different solution proposals. Throughout the Project it is clear that all players in the Maritime Situational Awareness arena actually do have access to the bulk of the data registered, at least to the degree where it can be established that access to the (personal) information is not restricted by application of the protection legislation, but that the actual exchange merely is restrained by administering legislation.

Proposals 1 and 2 concern the issues of personal data exchange while the third proposal is about questions of how to solve access problems because of the application of confidentiality and secrecy. These three are purely legal suggestions, where the action is directed towards amending running legislation, changing or even proposing a new one.

Proposal 4 is a more pragmatic position. It advocates a very suitable and experienced tool - the agreement. This 'solution' is more of a recommendation for a way forward. The above mentioned proposals entail time consuming procedures before any change may take place and have an effect. Meanwhile, choosing this option, gives an operative tool using the legislation at hand, with all its benefits and, unfortunately, also its drawbacks. The experience evidenced by MARSUNO shows however that this platform is flexible and opens up for tailor-made solutions.

Proposal 5, a harmonising Policy, is a complex and comprehensive proposal, relying on the concept of sharing common scopes, measures and ways forward. Its core idea is the achievement of implementing harmonised actions on a broad scale based on decisions and official statements

1. Harmonisation by reducing differentiation of national legislation:
Typically the confusing situation concerning exchange of personal data is directly dependent on implementing margin possibilities given to the Member States; see Articles 5 and 13 in the Data Protection Directive, Directive. This possibility leads inevitably to a vast divergence between the national legislative measures. This in turn leads to a lack of compatibility and further establishes hinders for efficient information exchange, if at all possible! The European legislator has openly admitted consciousness of these consequences in the preambles to the Directive[43].

[43] Preamble 9:" Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, *disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community* (highlighted in italics by the Project)"

In order to achieve a high level of harmonised application throughout the European region it is recommended that the diversity because of the implementation option is restricted, where Member States may detail the application of the Directive.

It is clear that for efficiency's sake requirements on safeguarding exchange between authorities and Member States should already be inserted at the level of the Directive, suitably by amending the Directive. Technically the suggested adaption could be performed either as an amendment of Article 13, or by inserting a new provision.

As the description of the action does not cover any inventory and analysis of the different conditions on national basis in the Member States related to the Project, it is at this point not possible to draw any concrete conclusions from the prevailing situation and further present in detail what specific requirements should be incorporated in the Directive.

Regardless of the above mentioned constraints MARSUNO would recommend that at least the following standards and requirements could be subject for incorporation through the amendment of the Directive:

- Full access to non-restricted personal data between corresponding functions designated with the purpose of national security, defence and the prevention, investigation, detection and prosecution of criminal offences within and between Member States,
- Full access to restricted personal data according to the application of the Directive or the relevant national legislation between corresponding functions designated with the purpose of national security, defence and the prevention, investigation, detection and prosecution of criminal offences within and between Member States, under the condition that such data is safeguarded in accordance with the principles of protection of the individual,
- Full access to non-restricted as well as restricted personal data according to the application of the Directive or the relevant national legislation between corresponding functions designated with the purpose of national security, defence and the prevention, investigation, detection and prosecution of criminal offences within a Third Country, under the condition that the requirements set out in articles 25 and 26 in the Directive are met.

2. Harmonisation through legislation by sector at the EU level:
This option is very close to the concept of proposal 1. Instead of dealing specifically within the regulation of the Data Security Directive itself, the Project is here suggesting the idea of altering the conditioning of processing personal data directly in the material legislation. In short the Project suggests that a specific condition would be inserted in the relevant legislation stating that personal data may be transferred to certain enumerated functions, under condition that such data is safeguarded in accordance with the principles of protection of the individual.

The recent development on this specific issue regarding the Common Fisheries Control Directive could serve as an example. The recent development concerning the fisheries control legislation may serve as an example. The former version of the Common Fisheries Control

Directive, 3487/93 (EEC)[44], did not allow any transition of the data collected through the information systems governed and made mandatory for the stakeholders concerned to any other than the Member State fisheries' authorities and the Commissions or the responsible body designated by it. Access to such information was consequently prohibited if you were not part of the authorised community. The current version of the Common Fisheries Control Directive states however (see Art. 12) that data from the collected by systems[45] included in the Regulation may be transmitted to Community agencies and competent authorities of the Member States engaged in surveillance operations for the purpose of maritime safety and security, border control, protection of the marine environment and general law enforcement[46].

The Project recommends consequently that in specific, sectored, Union legislation the legal framework in question should be adapted to the needs for access of necessary information by including provisions regulating the accessibility of certain data to certain designated functions, e.g. law enforcement, customs etc. Following the observation made on the consequences of the applicability of legislation with the purpose of protecting personal integrity, it is advisable to also set requirements facilitating transferring of personal data, e.g. admitting transfer between similar functions or authorities in different Member States if transfer of such information is authorised between similar functions or authorities within the sending Member State. This concept would thus safeguard the protection of the individual and still enable efficient exchange of information in the interest of relevant authorities.

3. Confidentiality and secrecy adapted to sector needs:
This proposal is a direct extension of proposal 2, similar to its construction but with some distinct differences. Firstly it concerns confidentiality and secrecy which are not subject to any general Union legislation as regards protection of individuals, see Data Security Directive. Secondly, the issue is in the majority of the cases exclusively subject to national legislation, meaning that the differences between the Member States are generally significant. Further the data concerns non-personal issues.

Again, the Common Fisheries Control Directive will serve as an example to illustrate how legislation could be altered and adapted to enable the needs by sector for access to relevant information. In the current version of the Regulation it is stated that Member States and the Commission shall take all necessary steps to ensure that the data collected and received within the framework of the Regulation shall be treated in accordance with applicable rules on professional and commercial secrecy of data. Further it states that any use of the data is restricted to the purpose other than that it was provided for in the Regulation (fisheries), unless the provider gives its consent and its use is admitted in the receiving Member State.

[44] Council Regulation (EEC) No 2847/93 of 12 October 1993 establishing a control system applicable to the common fisheries policy, OJ L 261, 20.10.1993, p. 1
[45] E.g. vessel monitoring system, the automatic identification system and the vessel detection system
[46] It should however be noted that the new Regulation further states that it (see Art.112) does not interfere with the application nor affect the level of protection of individuals with regard to the processing of personal data under the provisions of Community and national law, and in particular does not alter either the obligations of Member States relating to their processing of personal data under Directive 95/46/EC or the obligations of the Community institutions and bodies relating to their processing of personal data under Regulation (EC) No 45/2001 when fulfilling their responsibilities. This provision respects Member State legislation on the topic personal data protection. The latter may result in accessibility problems, with similar effect as were the consequences of the former version of the Fisheries Control Regulation.

While this approach respects the national measures it builds up an impenetrable cluster of diverse legislation. To avoid this obvious obstacle the Project suggests that Union specific legislation should include provisions where transfer of such data, collected and received within the framework of the framework in question, should be admitted without any other restrictions than that transfer is made between similar functions or authorities, within and between Member States.

4. Agreement as a general option:
Pending the adoption of necessary general or specific Union legal measures it is highly advisable that Members States, or their authorities, continue to enter into agreements bilaterally, multilaterally or regionally to enable, preferably direct, access to pertinent information.

It has to be clearly established that entering into agreement does not effectively lead to any material change of the law(s) covering the subjects for the action. This solution is merely a convenient way to find a quick (!) fix to a deep need.

The inevitable source of constraint is the different legislations in place admitting at various levels the eventual transferring of information. And this determines the efficiency of the contract. In the agreements the parties involved determine in detail which data, how and when such data should be transferred and to whom. Such a practice will of course entail a great number of various agreements and the overview will by necessity be hampered by its number. At the same time it will ensure the direct delivery and to administrate for the parties. This solution enables also that any amendment or adjustment to changes, legal or practical or for any other reason, can swiftly be carried out.

As it is necessary to limit the multitude of agreement solutions and increase efficiency of the use of agreements a high level of standardisation should be sought. It is obvious for the Project that contracts consist of significant number of elementary parts, and that the remaining terms basically can be assembled within a few different categories. The task to develop suitable template contracts to be used within the Maritime Domain area could be give to any relevant competent international body, preferably within the Union.

5. Quasi-legislative proposal – Policy for Harmonising Maritime Related Information
The various suggestions for solutions to satisfy the needs for the right information at the right time are complex and require significant investments from the user community. Every player is dependent on the other to eventually achieve the CISE. One overarching requirement to achieve an efficient CISE situation is to create a harmonised legal playing field. For this purpose the Project proposes a designated Policy for Harmonising Maritime Related Information.

Amongst the arguments for choosing such an alternative is its ability to reach and make participation possible for countries outside of the Union as well. Further the Policy will offer well founded decisions taken on a broad basis which will give immediate and direct impact within the sectors concerned. Another specific advantage with the Policy is that the solutions produced will have direct impact within the sectors concerned, regardless of whether they may be of legal content or other measures with similar effects. The Policy will further

facilitate the necessary implementation of the decisions to be effectuated as simultaneously as possible.

The Policy is founded on a few basic cornerstones, as follows.

Determine the framework for the joint efforts
The framework for the Policy would consist of all the relevant legal functions within the maritime sector. This will cover e.g. the national defence, safety and security functions together with surveillance, law enforcement, customs, border guard, maritime safety, SAR and pollution response as well as fisheries control functions and all other functions connected to the maritime arena. The policy is intended to go beyond the Union borders to include Third Countries such as the Russian Federation and Norway, to begin with.

Setting scopes and objectives
The scope of the Policy will be the coherent and comprehensive adaptation of the legal frameworks within the maritime information related sectors to meet the user community needs while respecting the protection of the individual and integrity including the relevant interests of the stakeholders involved. The Policy will have to include all relevant legislation from the national to the Union level, as the agreements, bilateral, multilateral and regional. The specific objectives will have to be set due to the sectoral needs corresponding to the user communities involved. The Project has identified a number of high priority changes, i.e. secure access of non-restricted data, personal as well as non-personal within the maritime sector.

Promoting procedures for achieving the objectives
The Policy structure, see below concerning responsible bodies, will, taking into account the results from the Project, adopt recommended measures in order to reach necessary alterations of the differing legislation and other hampering frameworks within the sectors. The measures needed have to be chosen according to the regional circumstances or to the type of framework(s) that are in question. Where feasible a unified measure may be promoted, in other situations different solutions may guarantee a positive outcome. A flexible approach should be supported towards the choice of solutions in order to accomplish the best results to attain harmonised maritime related information.

Establishing joint work platforms
Efficiency is a key factor in reaching substantial results. The Project advocates that the different user communities would be organised in working pools to produce common 'gap-and-solution' proposals in accordance with the objectives set out for the different sectors or communities concerned. These proposals would in their turn be stepping stones for further development in cooperation with the other special groups such as TAG, JAG, AAG and others involved in the MARSUNO realm.

Distribution of responsibility to perform
Subsidiarity is one of the crucial foundations of the Union, meaning that decisions and measures are to be taken as closely as possible to the people and areas affected, as well as the use of existing expertise in taking decisions. To this must also be taken into account the need for efficiency and conformity. The question is who shall take the lead in this effort and assume responsibility to join and safeguard the process ahead which includes the Union itself

as well as reaching outside its borders. The Project finds that the European Commission is well fitted to take on the role of facilitator and also has the ability to act as an integrator.

Adopting development approaches
Society is changing relentlessly. Today's solutions are already obsolete tomorrow. To avoid any new situation where legislative development creates disparate provisioning concerning the shared maritime information environment it is essential that the Policy includes approaches for continuous follow-up measures within the cooperation.

4.4.4 Summary

The key approach for achieving a functional, efficient and performing CISE is to create a stable, foreseeable and accessible basis for exchange of information. The essential wording is 'harmonisation of legal conditions'.

Respect for the fundamental rights of people includes rights of privacy and consequently also protection of personal data. The right to process such information is well-balanced to serve society's needs for information in order to ensure its development at all levels and for the protection of peace, liberty and democracy. Any further enlargement of the possibilities to transfer personal data has to ensure the protection of this fundamental right. The majority of data/information relevant to the needs within the maritime community, regardless of wether it is personal or non-personal, is, from a legal point of view, already fully accessible at any moment for the stakeholders involved. Most reasons for accessibility constraints are due to administrative procedures and technical barriers. Nonetheless, some obstacles of a legal nature have been identified. Some are of such nature that a solution would need a material adaptation of the running legislation, i.e. positive change of the rule itself, e.g. change from a prohibition to a (complete or partial) permission. Some obstacles could be removed by a simple structural change of the legislation in place. Some problems are not purely legal as such, but result from a policy approach. Changing the policy approach would consequently also change the grounds for the legal framework and its content.

The prevailing conclusion on the concept of information exchange problem is due to incompatibility because of the disparity of national legislation given within the margins of manoeuvre provided for by the applicable European legislation. A conclusive approach for a solution may then focus on harmonising legislation, either directly detailing the provisions on European legislation level or directing further the implementing margins.

In addition, as changes of legislation on the EU level are time consuming procedures, and at the same time the need for the right information at the right time is noted, the only viable solution at hand is to get all stakeholders to act in the rather simple and efficient procedure of entering into agreements with each other while the more formalistic and political alternatives are proceeding.

Lastly, to ensure the necessary adaptations over time and implementation of the results on a broad scale as simultaneously as possible to satisfy the needs for relevant information within the user communities involved it will be required that the alterations are well founded throughout the communities, inside and outside the Union. Such conditions call for political involvement, while the development procedures should be carried out in close cooperation by

the stakeholders. This demands a program-like procedure, which could be harnessed by a policy, monitored and lead by the European Commission.

4.5 Technical obstacles (cross border/cross sector)

4.5.1 National and agency tools

The general understanding is that each nation has its own unique situation with respect to existing national administrations, responsibility for distribution among those administrations and demands rising from each responsibility with respect to the actual geographical and infrastructure situation. This implies that each Member State's national administration should decide on the use and development of the tools needed.

The development of tools to be used within the CISE is judged to benefit from the situation of a mix between national and EU agency tools connected to the CISE.

Data fusion method
Information/data that will be accessible in the CISE must be used in an optimal way. To succeed in getting quality assured analysis and intelligence could lead to operational benefits of participating agencies. A well defined method of fusing data in order to make best use of the available data must be established. This data fusion task could be carried out at the national or agency level. The fusion function would be for the common environment but resides in tools connected to the environment.

4.5.2 Technical functions needed to support/facilitate theCISE

In order to facilitate, at the EU level, an efficient (i.e. cost effective, promoting data quality, broad readiness to connect), national implementation of interfaces to the CISE technical environment the following requirements have been identified:

Common and agreed standards/methods for sharing data between systems
For the automated sharing functions there is a requirement to establish a 'set' of communication schemes. In order to facilitate basic sharing techniques (that may be the first to be used) as well as more advanced sharing techniques (that may be required as the national systems are further developed) the set of communication schemes must not be too limited. In other words there should be communication schemes for different types of use in the CISE. It is foreseen that there will be a need for a maintenance organisation for the CISE.

There should be common and agreed:

- Network that is to be used.
- Security classification levels for the data to be exchanged. (This is very closely related to legal and administrative needs).
- Methods and procedures on how to assign access rights to information (data) shared.

Technical measures on how to protect of each security classification level of data.
Functions for at least the following principal methods of sharing data;

- Pull (the entity to receive the data puts a request and sets up the connection)
    - Single request - Single transfer of data (Single response according to specified search criteria's in the request)
    - Single request – Multiple transfer of data (Multiple responses according to specified search criteria and time interval in the request with multiple replies as specified).
    - Streaming data – Continuous updating of the specific information agreed

- Push (the entity that owns the data sets up the connection)
    - Connection request – Single transfer of data
    - Connection request – Multiple transfers of data

Agreed common standards and methods for information/data to be exchanged in the CISE:

- Information model.
    - The information model may be designed as a basic part (common for all sectors) and sub-parts (for each sector).
    - The information model should comprise an unambiguous definition of each data type (parameter) making up the model.
    - The information model should comprise an unambiguous coding of each data type.
    - The information model should comprise the relation between the subgroups of information.
    - The information model should identify the subgroups of information that shall be possible to use to transferring data.
    - Network(s) that are to be used.
    - Standard to be used to establish a videoconference between multiple operators /operational centres cross sector and cross border.
    - Standard to be used to establish a chat group (social media group) between multiple operators /operational centres cross sector and cross border.
    - Standard to be used to communicate via email between multiple operators/operational centres cross sector and cross border.

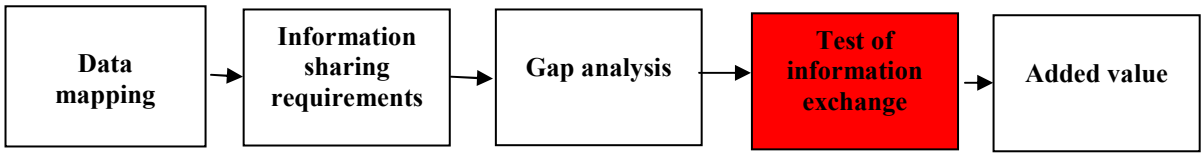
Remarks

All technical systems have a need for a maintenance function. This is also true for the common and agreed standards that could be established for CISE. Hence all the technical facts established will be subject to improvement and corrections and will demand a 'maintenance organisation' that will be an integral part of the CISE.

Before a CISE common standard can be established it is important that existing international (IMO, IALA, UN) standards have been considered and where possible used. One obvious example is regional cooperation between Member States and Third Countries.

5. Test of joint maritime surveillance operational procedures between law enforcement authorities and other sectors - Objective 2

To test joint maritime surveillance operational procedures between law enforcement authorities (i.e. customs and border control, fisheries control, maritime safety, vessel traffic management, search and rescue, maritime assistance service, marine pollution response, maritime security of ships and ports, prevention and suppression of criminal activities).



During the project development, two demonstrations of information exchange have been performed. One was carried out on a cross-border and cross-sector basis, while the other one was performed in relation to information exchange within the VTMIS sector. These two demonstrations are described in this chapter.

5.1 Experience from MARSUNO DEMO

Cross-sector information exchange related to MPR, SAR, IBM-LE, VTMIS and FC

The purpose of the MARSUNO Demo[47] was to study the needs and examine possible gains from improved information exchange, regarding both available and required data/information. The information exchanged during the demo was defined through the project work, and divided into basic data, additional data and restricted data.

The demo corresponds to the second and third objectives in the Grant Agreement;

- To test joint maritime surveillance operational procedures between different sectors within MARSUNO.
- To determine the extent to which project partners are potentially able to set up an exchange of information mechanism at a cross-sectoral and cross-border level that is viable and durable in time as well as, finding gaps between civil and military information exchange.

[47] www.marsuno.eu/Reports

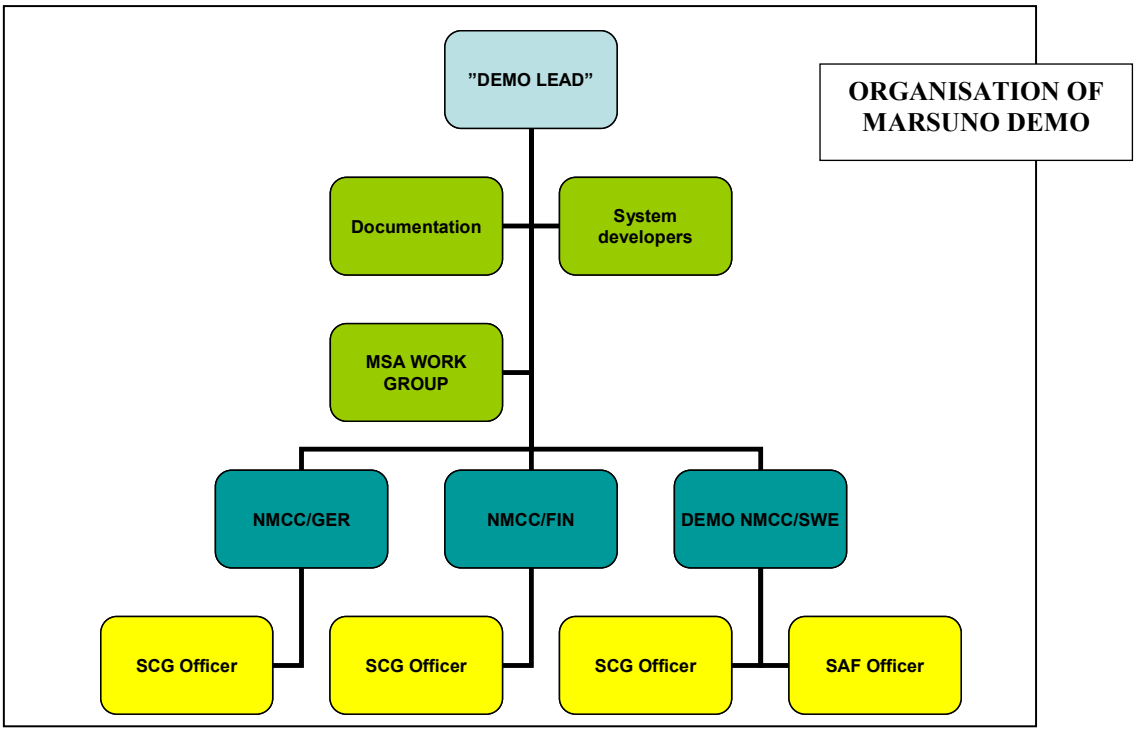


Fig. 9 Organisation of MARSUNO Demo

The MARSUNO DEMO consisted of different activities:

- Demonstration of MARSUNO Demo platform (MD)
- Sector information (additional data, links etc)
- Workshop discussions, template questions
- Two scenarios with simulated information as well as real time situational information with cross-border/cross-sector cooperation by (in the demo) so-called National Coordination Centre (NMCC) in Finland, Germany and Sweden.
- Discussions, conclusions with the aim to agree upon a draft demo document during the last demo day

3.1.1 MARSUNO DEMO Platform

The platform offered the following information services:

- 'Ship' database added with intelligence data.
- 'Harbour' notification database added with safety notifications and crew list.
- Sea information service.
- Real time situation, vessels.
- Real time weather observations.
- Weather forecasts.
- Sea Chart/ land map information.
- Protected areas, fishery zones, protected zones.

Co-Financed under European Integrated Maritime Policy

- Watch functions with alarm, with respect to i.e. area, speed, ETA, vessel type etc.
- Historic replay of surveillance data and other sea information.
- Links.

The MARSUNO Demo Platform was established by using the joint Swedish national maritime surveillance system. This service provides sea information services and is also provider of a common maritime picture for authorities within the maritime responsibility area.

The purpose of the adaption was to have the ability to use the common maritime picture at each NMCC that were participating in the demo. Each NMCC received the same common maritime picture independent of geographic location.

Integrated in the common maritime MARSUNO Demo Platform were MSSIS (AIS data) and other parameters like hydrological and meteorological information. These were examples of some sources that might be used and that cover the responsibility areas.

3.1.2 Use of scenarios

The MARSUNO Demo Platform was adapted to use as many aspects of the common maritime picture as possible and for visualisation, to make full use of the scenarios. Several observations in the two scenarios had been programmed in advance into the Swedish Coast Guard information system. The SUCBAS system was made available for the demo, in a separate connection in the Control Centre in Karlskrona. Video connections were established to the participating 'NMCCs', in Cuxhaven and Turku, creating a virtual common – and cross- sector - information exchange environment. A Swedish Coast Guard officer was located at each NMCC during the demo. A mailbox was temporarily in use during the scenario play, to simulate a common operational log and as a backup function for information flow in addition to regular channels, and for documentation purpose.

The work with the scenarios utilised simulated data together with real time information. To support the work during the scenario development checklists were used with step-by-step comment fields. Notes were made for further analyses of data available/required.

Three platforms were working in parallel; SafeSeaNet-Graphical Interface as situation at sea platform, MARSUNO Demo Platform provided the demo with Schengen related information, weather etc. and the military sector was represented by the SUCBAS system. These three together gave an example of a more comprehensive common maritime surveillance picture. Links to additional information in the MARSUNO Demo Platform enriched the information sources.

5.1.3 Lessons learned from the MARSUNO DEMO

From the scenario part, it was noted that the operators in the demo had good common information and awareness at sea. The operators were capable of tracking vessels, but there was still a lack of integration of systems and information

There is a need for a common standard (technical) to be able to have good communication through audio/visual connections (video link during the MD) - there is also a need for a common environment both for communication and for information exchange.

Information exchange between NMCC operators worked well – but the exact information that it is possible to exchange cross sector might sometimes be difficult to sort out due to legal and operational constraints. As an example, if the information is passed on within sectors, like Coastnet channels these problems are reduced. Coastnet might be considered as a regional precursor to EUROSUR.

In the demo discussions several issues were raised such as;

- Standards are needed.
- The focus is not to have as much information as possible but rather to have selected the information for each user's needs.
- Share all information available (and needed) to enable all actors, better and faster, understanding of the situation.
- Access to information is determined by legislative, security, operational, administrative preconditions.
- Need for Standard Operational Procedures[48] (SOP).
- An important need on the regional level is to have Third Countries participating in the information sharing environment.
- From the SUCBAS cooperation it was reported that "it is not about sharing a compiled picture but to have more frequent contacts in order to be able to share information". Defence community suggests a more open information exchange environment would lead to a better ability to share the best information available in order to achieve better possibilities to prevent risks and handle situations such as the scenarios described.

Proposal for a "roadmap" divided in three steps (see section 7.5.1);
1) Disseminate available information.
2) Extend sharing capabilities
3) Towards value added service sharing

From the workshop activity the conclusions were as follows:
The EU Commission stressed the importance of talking about 'services' – avoid discussions on data – data is of interest when it comes to the technical perspective of sharing.

Basic Maritime Situational Awareness (founded on basic data) should be available for the whole common area but each sector/administration/user/user group etc. must be able to define their own Maritime Situational Awareness independently suited to their own purposes. A common shared Maritime Situational Awareness is not a goal for all communities involved. Maritime Situational Awareness should be available for a limited area in the purpose of dealing with threats, risks or accidents. There would also be a need for national contact points, N-CISEs'.

5.2 Experience from MARDEMO

Cross-sector information exchange related to VTMIS

During April 2011 Poland requested Maritime Situational Awareness for access to the SSN Training site to support the exchange of data between Baltic Sea Member States within the

[48] Precise, defined rules for accomplishing tasks that have been developed to cope with expected situations.

scope of MARSUNO. Maritime Situational Awareness granted access and ensured availability of the SSN Training site. A test period was performed in August and the exercise called MARDEMO[49] was carried out 6-8 September. Authorities from eight different Baltic Member States and Russia were participated in the demo.

5.2.1 Scenario and MSS actions

The Scenario of the exercise was based on the simulation of a passenger vessel (Finnmaid; IMO 9319466) contravening the IMO Resolution MSC.139 (76) Annex 1 (Description of the mandatory ship reporting system in the Gulf of Finland Traffic Area) and afterwards an exchange of non-classified tracking information between Baltic Member States and Russia taking place. The scenario required each Baltic Member States to send an incident notification on SSN Training site when the ship was entering and leaving their EEZ. The existing 'distributed incidents' functionality was used for that purpose.

Maritime Situational Awareness' Maritime Support Services (MSS) ensured an operational helpdesk (administration of user accounts) in the exercise. During the exercise the MSS supported SafeSeaNet registered users in technical or administrative problems related to the use of SSN Training site. A contact person in the Maritime Office in Gdynia was in charge of all operational issues for the MARDEMO exercise.

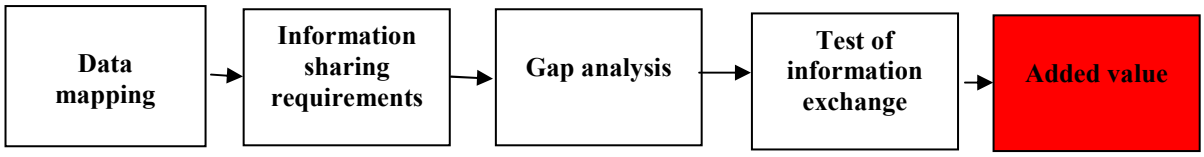
5.2.2 Lessons learned

- Existing SSN tool for distribution of incident reports was initially developed for warning Member States about a vessel posing potential risk and passing along their coasts (in line with Art.16 of the Directive 2002/59/EC). The MARDEMO exercise demonstrated possibility of its use for other purposes e.g. exchanges of tracking/security related information.
- The exercise, based on the preconditions for the specific MARDEMO exercise, also claimed proof that no other existing operational system apart from SafeSeaNet could have been used for acting as 'systems connector' to support the above mentioned exchange of data.
- In operational terms: There should be similar exercises performed regularly.
- In terms of SSN future developments: The Exercise demonstrated that there is a need to implement 'update' functionality for Incident Reports in order to avoid an excessive number of messages related to the same issue[50] (all updates regarding one situation linked to one Incident Report).

[49] MARDEMO Exercise report: Summary material and CISRR report
[50] Due to experiences from recent incidents, it is of the utmost importance to be certain that the Incident Report system has been authorised by all parties involved so that the channels of reporting are completely clear to all.

6. Added value due to cooperation between partners within the Northern Sea Basins and between the sectors that are represented by partner authorities - Objective 6

To determine the extent to which the cooperation between the project partners has resulted in added value – both in qualitative and quantitative terms - in relation to what already exists with regard to cross-border and cross-sectoral cooperation in the geographic area where the pilot project takes place and in relation to the above mentioned domains of surveillance activities.



The MARSUNO project will point out added value and best practice both in relation to what has been mapped in relation to current status as well as for future oriented solutions for how to proceed within the CISE development.

The Added Value concept in CISE the development refers to the linking of national systems by interface solutions in between, which creates a more valuable surrounding by giving access to all available information in comparison to the input value. Suggesting ways to overcome current obstacles, in administrative, technical and legal perspective, the way forward for improving information exchange will strengthen the possibility of improved interoperability between systems and users.

The added value could also be expressed in terms of the gains from better use of cross-border and cross-sector information exchange.

One of the first tasks of the project was to identify the current status of information exchange and it was considered, in general, that the situation is acceptable depending on perspective, for example looking at the cross-border perspective where the information sharing is working rather well but in some cases needs to be improved. Then moving on to the gap analysis combined with definition of requirements for information exchange, the project was able to point out where the weak spots are. The need and the effort in adapting to requested change implies that we can move over to a more optimal position– and create conditions for better knowledge –in other words – creating added value. By implementing the findings and recommendations from the Project we will be able to move from an acceptable position to a position for better knowledge and better capability to adjust to a changing environment. By doing this the users will (see figure 10):

- Gain access to more information (for instance by having access to more information due to expanded authorisation to information)
- The information on demand will be user defined and by this more **relevant** to the user

Co-Financed under European Integrated Maritime Policy

- By gaining access to more information, and also in the sense more relevant information, the ability to make appropriate decisions will increase in relation to operations. In making accurate decisions the efficiency level will increase and this will be promoted by the use of common technical standards and SOP.

Through these three parameters the ability will increase for adapting to dynamics, which in the end is the goal. The CISE should contribute to the possibility of taking action in relation to changes and altered conditions within all sectors in the long run, and this is only possible by offering a flexible but well founded platform for decision making.

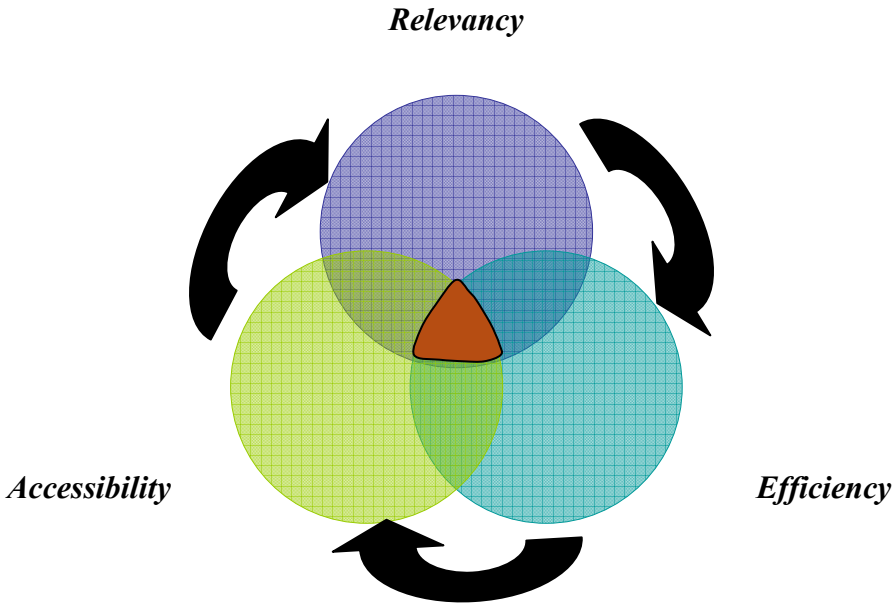


Fig. 10 Adaption to dynamics

6.1 Cooperation and added value

The vision of MARSUNO is stated as to "achieve a higher degree of interoperability among existing monitoring and tracking systems in order to improve maritime surveillance in the Northern Sea Basins". For CISE development this aim is not only limited to the Baltic Sea and the North Sea, but to interconnect several sea basin areas such as the Mediterranean Sea, the Black Sea area and the North Pacific area via the North Eastern Passage. As mentioned before there will be a need for closer cooperation with Third Countries as Norway, Iceland and Russia.

This means supporting following criteria:

- Establishing an Integrated Maritime Surveillance which in the end will be a part of the Common Information Sharing Environment – CISE
- Increase the efficiency of Member States' authorities and improve cost effectiveness

The MARSUNO project will bring added value for the development, compared to current status.

Involvement of Third Countries concerned, i.e. Russia and Norway, in the MARSUNO community gives an added value. That could be interpreted as a promotion of the CISE as such but also an improvement of the Maritime Situational Awareness as well as improving efficiency of existing systems in this vast region.

To enable the cooperation in the intended direction, a rectified administrative structure must be established in the MS, including partner states. There is also a need for:

- Common standards and understanding[51] within the maritime CISE.
- Statement of the fact that (EU) military resources are a necessary support to the CISE and vice versa.
- Responsibility to share information and adapt classification of information – both civil and military.
- Regulations and agreements for cooperation.
- Establishment of a network of N-CISEs.

6.2 Concrete examples of Added value

Many good examples are given in the thematic reports that will lead to added value and cost savings in different ways, direct or indirect, as well as in short terms and long terms perspectives.

During MARSUNO seminars, MARSUNO Demo and permanent discussions within the different layers, numerous ideas and proposals have been scrutinised, in order to identify cost savings and added value as an ongoing part of the process. Rationalising or organisational changes have not been discussed during the process but in a long-term perspective the main part of cost savings ought to be found in these sectors at a national level (see Chapter 6.3 for further analyses).

Some examples of added value:

- 'Single window' system for the merchant shipping industry and fishery industry will be facilitated by the establishment of a well functioning CISE. If the shipping and fishery industries (i.e. ships' owners, shipping companies, masters, ships' agencies, port authorities) can have a constructive feedback of their reports and participation in the exchange of information at their level, they can be encouraged to take more action in the CISE.
- A more efficient cooperation and better understanding between civil and military authorities will lead to avoidance of duplication in many crucial areas and more value for the taxpayers' money. That is also very clear confirmed in the Wise Pen Team Progress Report 'Maritime surveillance in support of CSDP', December 2010.

[51] Understanding, in the sense of " a matter of cultural aspects but also a genuine knowledge of how different cogs fit into the maritime domain as such to form a working operational machinery.

- A well functioning CISE will in the long-term perspective bring different cultures within the maritime domain together, enabling a more cost- effective use of resources, crisis management and exchange of information. This will also lead to a natural willingness to cross-sector as well as cross-border exchange of additional and restricted levels of information, thus avoiding parts of the administrative obstacles.
- As the maritime domain is global by nature, the involvement of Third Countries is necessary for a well functioning CISE. In the Project, Russia was involved as an 'associated member' at an early stage. Russia has paid a great deal of interest in the project that has led for example to a clear declaration from Russia, through her membership in the different parts of the regional Baltic Sea cooperation, Black Sea cooperation as well as the North Pacific Coast Guard Forum, that it is willing to share information within the Maritime Situational Awareness sector. As shown in the MARSUNO DEMO, this can also lead to an extension of CISE in the north-east passage, connecting the Pacific region with the Northern European Sea basins.
- Consistent with the above, the MARSUNO project proposes that Russia will be invited to a post as observer in the Member States Expert Sub-group (MSEG).
- A common list of acronyms and abbreviations for the maritime domain as exemplified in Annex 8.1 to the final report. Such a list has been proposed in several of the thematic reports and the existence of that reference material will have great impact on different cultures and diversions cross sector as well as cross border.
- Standard Operative Procedures (SOP) already exist in different sectors, for example in MPR operations (Bonn Agreement, HELCOM, Copenhagen Agreement), SAR operations and military operations within EDA/NATO. Many of the thematic reports propose the introduction of SOP in order to facilitate the procedure for the exchange of information especially at the additional and restricted information levels. The use of SOP could give an added value to the civil-military cooperation, but also to certain language difficulties in the operational context.
- SAR operations as well as MPR operations are already very well organised and are performed and conducted in line with IMO conventions, SOLAS conventions and regional agreements and long practical experience. Nevertheless, the thematic reports from these layers confirm the added value of an extended CISE, with admittance to both a basic Maritime Situational Awareness picture as well as an additional situational picture with access to whether conditions and forecasts, common drifting models forecasts, resources available on site, on alert in port or on patrol or from different military resources. Sometimes a connection and exchange of information via CISE with different law enforcement agencies could be of added value when there are operations initiated with suspicions or connections with different criminal activities as for example illegal migration, smuggling, water pollution, sub-standard crews, use of alcohol or other drugs or violation against sea traffic rules and regulations.
- Concerning the added value for IBM/LE it is well described in the thematic report and there are no additional analyses or remarks to be made in the final report. However, the findings in the thematic reports about the need for establishing a network of N-CISEs (former NCC or NMCC) highlights the added

value of having one national contact point designated for all matters related to the maritime domain.

6.3. Potential for cost savings

Potential for cost savings

In relation to the development of a CISE, the EU Commission has declared the importance of creating cost efficient solutions. This might imply shared solutions concerning use of resources but also joint efforts to develop mechanisms for optimal use of the resources. This could for instance be applicable when it comes to crisis management. Establishing a CISE should in the long run save costs, or at least lead to cost avoidance. On the other hand, it is important to keep in mind that the quality of the operational work must be balanced against the cost saving aspects, since the overall goal in the sectors involved in MARSUNO is about providing better quality and to provide security for society.

The MARSUNO project has, due to the Grant Agreement, to clarify some aspects in relation to cost savings. This section will in theory go through some of the components that are important to study to give further recommendations in the aspect for cost savings. The project will not give an account for each sector in relation to cost savings. This would require a new assignment.

The estimation of costs will be relevant to perform in connection with the defined conditions decided in relation to the Technical Feasibility Study within TAG. Only in defining the scope of what needs to be changed (primarily technically), it will be worth the effort to start defining costs. In the second round there will be a need for a thorough cost-benefit analysis for counting gains from the effects of the CISE.

Generally, the cost of shared solutions is less than the total cost of each specific solution. Cooperative agreements should ideally be beneficial. Other aspects that need to be balanced are;

- economy,
- efficiency, and
- effectiveness.

These should be in relation to the benefit, and the need for making better decisions should be valued as well. There will also be a need for performing different cost benefit analyses within each step of the development of CISE. In an overall picture focusing of the benefit for the EU, a meta-model for relating to CISE development should be considered while adjusting each national platform with attached systems, databases etc. The challenges will be related to categories on an inter-agency level, like cost savings in relation to hardware/software costs/ personnel costs/ facility costs/ supply costs etc.

In a larger perspective, there will be of interest in looking into categories like operating costs related to expenses required for the day-to-day running of the system. This includes the maintenance of the system. This will be on an inter-agency level, and also, depending on how the CISE solution turns out, this might be a cost to investigate before implementing different solutions at the regional/federal level.

Development costs incurred during the development of the system, which could be a one-off investment in the short run, but more extensive in the long run. This is relevant both on an inter-agency level as well as looking at the whole CISE development.

Improved performance and minimised processing costs are benefits which will be of essential value both at a national as well as at a regional level.

Both tangible[52] and intangible costs and benefits should be considered in the evaluation process towards CISE development.

Connectivity and standards:
The process of setting standards is largely political and involves many powerful interest groups, such as the private sector industry associations for equipment, federal governments and professional groups of standard institutes[53]. The need for setting standards and improved connectivity will be crucial for getting the CISE development to work and to be accepted. This will be a challenge that will need to be undertaken no matter what the costs will be. But this will probably be of lower cost if there is a political consensus in the decision to adopt a policy.

Direct cost saving impacts suggested within the project:

- The common use of satellite pictures provided by the EU through Maritime Situational Awareness is one example of how integrated solutions of operative cooperation and cost reductions can be solved among MS. The Sea Track Web is another example of how system developments will be open for common use, in this case among all the Baltic States. This could be developed to common systems for drift forecast and environmental atlases stored in 17 different national systems.
- By creating solutions that allow transfer of data between systems, there will only be need to input the data once, which will involve both time and cost savings. There will be a need for efficient interface solutions. A risk will be that costs of the development of interface solutions gets to high compared to the gains of data transfer.
- The adaption of standards (e.g. data formats and language tools) will be a cost saver in the long run for making software more compatible. (Compare with studies performed regarding cost saving within EDI).

Indirect cost saving aspects[54]:
A common shared situational picture, for instance in the Baltic Sea area, will create better opportunities for dividing and planning resources in an efficient way. This will also lead to increased control over action development and resources."

This is about quality in operations and how to make more accurate evaluations for improved performance.

[52] Related to physical/material costs (costs for machinery etc), intangible relates to immaterial costs (ex. value of a patent).
[53] Essentials of Management Information Systems; Laudon & Laudon, p. 237
[54] The highlighted texts in italics refer back to the opinions agreed in the application for call for proposals, by the applicants' consortium.

Regarding security aspects: a shared environment can possibly lead to cost saving by reducing the tap of information and shared costs for security solutions. This will only be relevant if the security solutions chosen by the different nations use the same solutions, or in relation to an agreement that indicates use of same tools.

"In integrating maritime surveillance systems within the Nordic sea basins and creating a higher degree of interoperability, there will be possibilities for cost reductions related to research and development costs, undertaken the conditions that the Member States will be able to – to a certain degree - access data and information from the systems that have been developed."

This might inflict free-rider behaviour by some parties, but as long as the benefit is larger than the lack of benefit this will be an acceptable way of sharing systems solution with other agencies, both cross sector and cross border.

"The public and the private sector will need to be partners in the effort to creating maritime situational awareness. The public sector is dependent on data and critical information from the private sector and the private sector is dependent on the public sector to secure an efficient and reliable flow of, for instance, people and cargo. Easy solutions that will avoid long lead-time in administrative procedures between Member States' and Third Countries will be an incentive for letting the public sector accessing necessary information. This will be cost saving for both parties, and time saving since the decision making process will be faster."

The Single Window solution for the maritime sector will fit in here, to reduce the administrative burden for the private sector.

Cost saving by entering into regional agreements

"In a shared system environment, significant cost savings can be obtained both in a short- and long-perspective due to a reduced need for different licensing agreements. (Based on a degree of database sharing etc.)".

This will only be relevant if there is a cooperation agreement between the parties, to use the same solutions.

"Increased interoperability will also lead to cost saving opportunities for countries with restricted budgetary means to take advantage of countries that have come further in developing and implementing systems."

This could be facilitated by entering into an agreement between parties about what information needs to be exchanged, and what kind of standards are set for the information exchange.

The advantage of using national solutions (connected into regional solutions) as platforms means the risk of competitive advantages for a certain or a limited number of suppliers will be less than for a more centralised solution.

7. Recommendations from MARSUNO for continued Sector specific and CISE development

7.1 Recommendations from thematic reports

Some of the recommendations listed in the thematic reports have been supported by several layers and these items will be discussed below. Some recommendations specifically for cross border dimension as well as cross sector have been listed as well, and these will also be summarised in this section.

Sector specific recommendations

Some of the recommendations are categorised into cross-border and cross-sector recommendations.

Layer 1: Integrated Border Management and Law Enforcement

- Cooperation between Member States and Third Countries is crucial. Regional solutions are needed to involve all states in the maritime domain.
- Regional as well as wider cooperation should be clearly regulated and agreed on in order to ensure quality, reliable and fast information exchange as well as avoiding duplication of work.
- In order to establish a basis for cooperation between sectors it is highly recommended to create common standard operational procedures for all maritime authorities. Definitions, concepts and terminology should be commonly agreed on.
- Common data classification levels and definitions should also be created for avoiding miscalculations between counterparts.
- It is necessary to develop (and maintain) network of national contact points. Common framework could be created and within its limits information could be shared according to the single-window principle.
- Counterparts should know each other as well as possible to increase trust since it can be the most significant mental challenge in creating any cooperation and information exchange environment.
- National cooperation is a fundamental part of the whole cooperation and should be encouraged within all coastal states. A comprehensive approach is essential in this matter.
- To allocate resources efficiently, sea areas should be categorised in a common way, which requires a common risk analysis.

Layer 2: Vessel Traffic Monitoring and Information Systems

- Enhancing the overall safety at sea: Harmonise monitoring and reporting systems to a level where ships' navigators perceive all the systems as one

  - The (Baltic) Harmonisation Working Group has currently no official status, one possible host organisation for the Group could be the Helsinki Commission
- Reduce the amount of reporting required by ships
  - Automatic information sharing between authorities cross sector will be enhanced by the implementation of directive 2010/65/EU (NSW directive)
  - Automatic information exchange between authorities cross border will be further enhanced by the full implementation of directive 2002/59/EC (SSN directive) and related technical systems

Cross-border recommendations

- Complete the national implementation of directive 2002/59/EC, comply with SSN XML messaging (L2)
- Russian Federation joins the SSN
- Use of IALA Recommendation V-145 On the Inter-VTS Exchange Format (IVEF)

Cross-sector recommendations

- Complete the national implementation of directive 2002/59/EC (Vessel Monitoring directive)
- Implementation of directive 2010/65/EU (NSW directive)

Layer 3: Marine Pollution Response

- Introduce pro-active traffic monitoring
  - Need for additional information (CISE might be the solution)
  - Identification of risk vessels (accident prone vessels, risk cargo), risk situations and nature of consequences of an accident
- Regard HELCOM and Bonn Agreement as Best practise
- Further alignment of Operation Manuals
- Same compensation rules within the EU as a whole
- Make AIS info more available
- Secure delivery of satellite images
- Development of 'Oil in ice drift modelling'
- Integration of HELCOM Map Service and BAOAC into MARSUNO
- Ensure Places of Refuge to work within operative timeframes between states and strengthen cooperation in forcing masters to accept the Place of Refuge given.

Cross-border recommendations

- Regional harmonisation of Support Systems.(Maritime Situational Awareness)
  - Environmental Atlases
  - Oil drift modelling

  (Thereafter integration into MARSUNO)
- Integration of MPA-data into STW and Sea bed data into Environmental Atlas and PoR manuals.
- Use of Coastal radars in some areas.
- Joint use of Aerial Surveillance
  - planning
  - performance

Co-Financed under European Integrated Maritime Policy

  - Standing diplomatic clearance
- Regional harmonisation of Support Systems.(Maritime Situational Awareness)
  - Environmental Atlases
  - Oil drift modelling

  (Thereafter integration into MARSUNO)
- Integration of MPA-data into STW and seabed data into Environmental Atlas and PoR manuals.
- Use of Coastal radars in some areas.
- Joint use of Aerial Surveillance
  - planning
  - performance
  - Standing diplomatic clearance

Cross-sector recommendations

- Enhancing the overall safety at sea
  - Harmonise monitoring and reporting systems to a level where ships' navigators perceive all the systems as one
  - Need for formalised and regular cross-border cooperation between VTS/SRS authorities
- Integration of data
  - environmental sensitivity
  - shipping
  - MPR resources
- Drift models
  - Same drift model for MPR and SAR
  - Satellite images(+VMS) for Fishery control
  - Wider use of RS equipment
  - CEPCO routines for other operations
  - Coastal Radar for SAR, Maritime Safety and Border Control

Layer 4: Search and Rescue

- Border and responsibility areas
  - Conflicting areas of responsibility for Member State (-s) and/or national authorities should be investigated and if appropriate, to develop operational procedures and joint cooperative plans to avoid uncertainties or misinterpretations in operations of SAR and MPR simultaneously.

  - Directives and definitions of EC 2002/59 and EC 2009/19 should be amended so that; surveillance and reporting areas will correlate SRR coordinates with the traffic monitored areas and to make information from SSN on vessel traffic management available for SAR and MPR.

- Maritime Organisation and System Concept Recommendations
  - Integrated maritime operational centres or co-location of SAR and other maritime functions would contribute to a more effective information exchange.

Co-Financed under European Integrated Maritime Policy

To be achieved by closer cooperation between the maritime functions SAR, MPR, VTM and, where appropriate also with regard to security, fishery, customs, MSI, ice braking services. Member States should be encouraged to consider to what extent benefits might be achieved by an integrated services.

- Mass Rescue Operation (MRO) Recommendations:
  - Mass rescue needs more resources, good cooperation, interoperability and extended approach in the preparedness and readiness of services. Therefore, Member States should be encouraged to implement MRO plans on local, national or regional basis.
  - Need for improved information exchange
  - Common databases with access and availability on;
    - Resources
    - Weather data
    - Situation reports
    - Contingency plans
  - Guidance on plans and operational procedures
    - Before a SAR operation
    - During a SAR operation
    - After a SAR operation

- Aircraft Co-ordinator (ACO) Recommendations:
  - MS Maritime and Aviation SAR administrations should, if appropriate, be encouraged to adopt the (Baltic) ACO model as main model for flight safety during mass rescue operations.

- Drift Modelling and Search Planning Recommendations:
  - As appropriate, Member States individually or by regional cooperation (including Third Countries), should discuss the development in a common computerised system gathering hydro-meteorological data.

- SAR Mission Coordinator Training Concept Recommendations:
  - Develop a course plan containing as well teacher-led face-to-face training, e-learning and practical parts, which would be seen as a basis for a detailed continuation of such future courses in cooperation between countries in the region.

- SAR Co-operation Plans for Passenger Ships Recommendations:
  - SSN to be used as an interactive platform for creating the SAR cooperation plans and for the reports exchange (SAR areas, coast stations, contacts, SAR exercises, updates on SAR Cooperation Plans, monitoring, verification etc.)
  - EU may if appropriate initiate a demonstration to identify functions of international database as ‘data centre’ (compared to LRIT data) for SAR Cooperation plans. The objective could be to use SSN as a future platform.

Layer 5: Fisheries Control

- VMS information should be available for all Member States at all times and not restricted to JDP campaigns.
- A common database with information needed for fisheries control could be run by for example COCA. Such a database should be available 24/7 and easy to find relevant information in.
- Legal obstacles concerning sharing information need to be solved.
- Intelligence needs to be shared in a better way in order to improve the inspections.
- Technical problems with databases which are too complicated to handle or too slow, need to be solved.
- Databases used on inspection platforms in the field (aircrafts, vessels, cars etc.) need to be better adapted to low bandwidth communication and computers with limited capacity.

Layer 6: Maritime Situational Awareness

- A need for interlinking authorities has been identified within all layers, for instance through NCCs but also outside the law enforcement community (N-CISE)
- There is a need for common standards (technical) to be able to have good communication through audio/visual connections - there is also a need for a common environment both for communication and for information exchange.
- Implement Single Window solution within VTMIS (full implementation of EU directives)
- Simplify the exchange of civil and military data requires legal adjustments - continued joint coordination of operations between civil and military communities (ex. ATALANTA)
- Capability of accessing information and awareness at sea – but lack of integration of systems and information & common definitions and Standard Operational Procedures
- Importance of involving Third Countries
- Give Russia an observer status within Member State Expert Sub-Group (MSEG)

7.2 Recommendations from a Maritime Situational Awareness perspective

7.2.1 Concepts of operations and Operational Procedures

Despite the fact that maritime operations are handled in accordance with international or national conventions and directives, there is still a need for a deeper knowledge of common activities and methods.

For instance, the SAR sector underlined the lack of role descriptions and task specifications with regard to Member States' appointment of tasks. Other sectors have identified needs for continuous monitoring of dangerous areas and risk assessment which requires adaptation of existing procedures and rules.

Efficiency during cross-sector operations in particular require detailed descriptions of operation procedures and Concepts of Operation (CONOPS).

Recent information sharing initiatives like MARSUR and SUCBAS demonstrate the importance of clearly defined CONOPS and operational procedures.

One recommendation of MARSUNO would be to set up a work group in charge of adopting CONOPS and Standard Operational Procedures (SOP). This group would start from existing sources and focus on cross-sector and cross-border maritime events which are not effectively handled now. A practical and pragmatic approach should be encouraged.

7.2.2 Implementing the CISE; setting up common definitions and adopting standards

The need for common definitions is present in all thematic reports. Information exchange is made difficult by the existence of numerous data formats and different definitions for similar events.

Initiatives of standardisation exist in some communities (for instance IVEF for interfacing vessel traffic monitoring systems or basic ACO guidelines which contributes to flight safety during SAR operations) but the effort should be developed at both cross sector and EU level.

Information must be categorised in order to ensure that common definitions are adopted by Member States' administrations. In order to ease information exchange and to propose a coherent framework to potential new partners, a data modelling effort should be encouraged. The aim is not to define the overall and complete data model, which could be time consuming and difficult to manage in the long term, but to agree on common definitions for core information and principles (e.g. technical standard). The modelling effort should focus on essential information to be exchanged during operational activities, especially cross sector.

To safeguard a reliable level of quality of information, Member States should reach agreement on classification levels regarding exchange of information. The Member States should define common security requirements. Exchange at a non-classified level should be encouraged and 'over-classification' of information should be avoided.

With time these standardisation efforts should lead to harmonised European systems based on best practices which will improve the service to end users as well as efficiency during operations. For instance, systems using exchange based on standards will enable users to build their own user defined operational picture. This is a requirement pointed out by many partners being essential due to the diversity of maritime operations and administrations involved.

7.2.3 Common tools

The workshops held during the MARSUNO and the thematic reports underline the need for cooperation between Member States in order to build better common tools like drift modelling system, seabed management or geographic information systems.

Such tools already exist but they need to be technically and semantically harmonised in order to be aggregated in order to be shared by several operators, regardless of national borders.

7.2.4 Encourage regular training sessions to promote willingness and trust

Training is a key point in setting a long-lasting information sharing environment between different countries and administrations. It is a way to overcome cultural differences and different historical backgrounds as well as work culture, by the simple fact by having

operators participate directly within each other's organisations. Combined with analysis of real-world operations, training could be a source of identifying new requirements and give the opportunity to learn new lessons. Recurrent scheduled training sessions could improve efficiency while giving users more confidence in technical solutions adopted by the information sharing environment (which is particularly important regarding security solutions). From a governance point of view, training sessions could be used to evaluate degrees of compliancy of partners regarding common rules and framework.

7.3 Administration of CISE

To establish an effective CISE demands an overall administrative handler function to be established, with clear responsibilities and legal authorisation organised nationally. The architecture of the common environment should be fully applicable to all authorities involved. All involved parties must also consider not only how to exchange information technically but also organisationally (administratively).

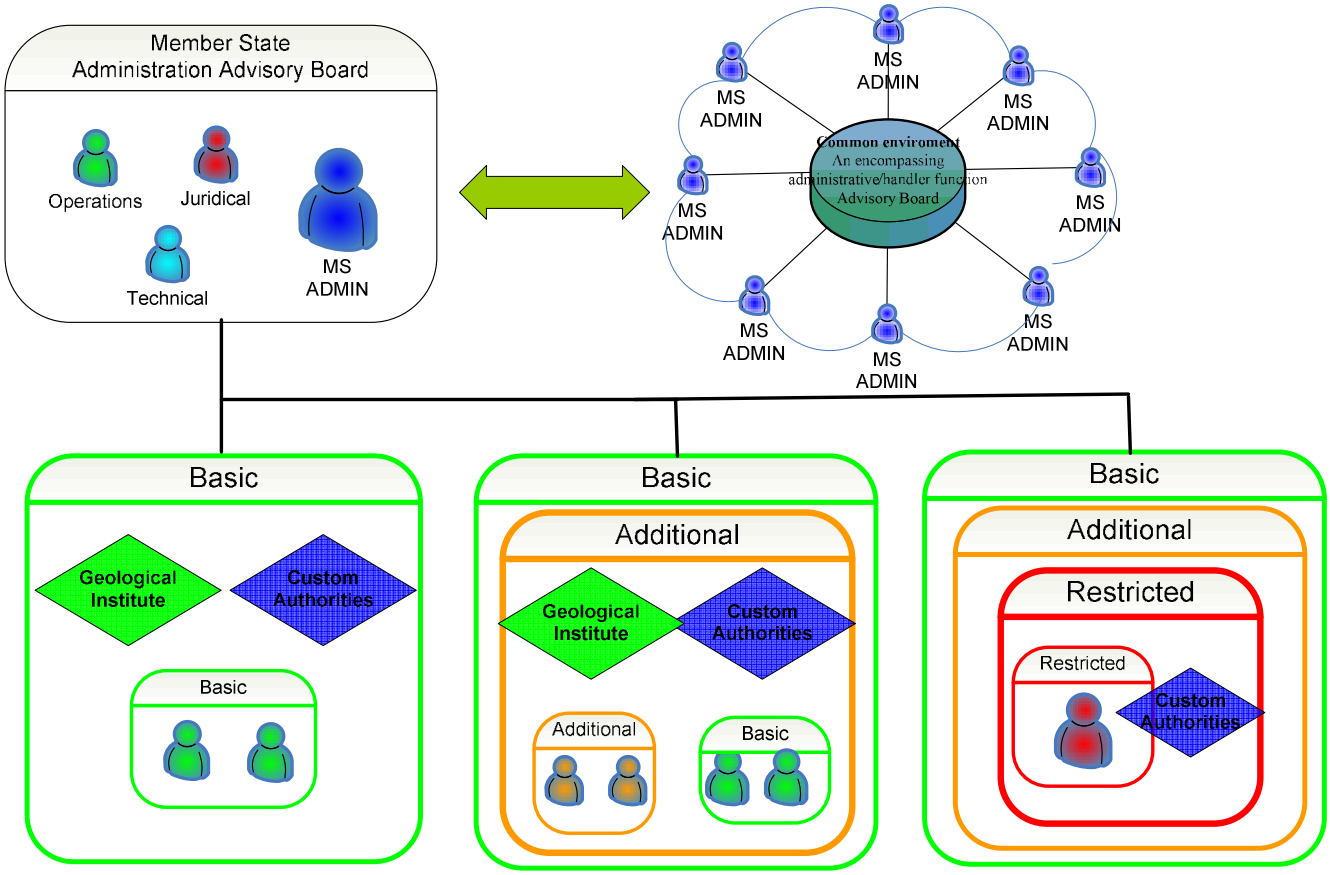


Fig. 11 One example of a nationally organised administration connected to a common environment administration.

The overall encompassing handler function could be set up as an Advisory and Policy Board, (AP Board), with participation from all involved Member States involved, including Third Countries. The national Member States' administrations could absorb the concept of AP Board, inviting relevant authorities to participate. The mission for such a board function

would be to set up and secure the access rights and protocols for authorisation at a national level as well as in required cases also at the individual level. Another major duty for such an AP Board could be to ensure the commitment from the end users and to manage the requirements, needs and ideas from the same end users. Also best practice should be shared both nationally and internationally and this could be handled and distributed by the AP Boards.

Consequently the AP Board as well as the national AP Board should cover the information sharing management aspects and the aspects of system management.

7.4 Administrative Advisory Group for implementation of CISE

To reach the aim of a CISE and facilitate the solution of the administrative obstacles and harmonise the implementation of CISE an Administrative Advisory Group (AAG) should be established by DG Mare. AAG should work in close cooperation with TAG, and future eventual work groups as Legal Advisory Group and Financial Advisory Group. The four advisory groups could together be a solid foundation covering the full spectres of the CISE implementation.

One topic which falls within the administrative scope is the development of common standards for the information exchange and for the operational standards. It is important to safeguard a sectoral specific development of standards and to facilitate and harmonise the equal need for cross-sectoral standards related to information exchange.

7.5 Natural convergence towards an optimised CISE

It would be too much to imagine that creating a new European system could emerge from nothing. Administrations, nations, community of users already have each of them their own organisation, priorities and systems (maritime surveillance systems, data bases, risk analysis tool) and these actually work satisfactorily.

Nevertheless it has been identified that a better interoperability, a better sharing of information, mainly automatic, cross sector and cross border, between administrations in charge of maritime surveillance will enable them to create a better Maritime Situational Awareness and improve their management of risk, their knowledge of maritime events and eventually their efficiency.

A well defined and common framework can be sufficient to entail a natural convergence towards an optimised CISE with time. Indeed, the medium lifetime for an information system is about three years. Each new update can be a step toward a more interoperable system of systems by using:

- the last version of adopted common data model defined at EU level by a cross-sectoral expert group,
- the last version of adopted common standards and rules regarding interfacing between national systems,
- legal environment and if possible legal umbrella at the EU level.

This ‘natural convergence’ will occur only if end users continue to meet regularly;

- at the EU level in expert work group working on EU data model and/or on common technical standards and rules and sectoral services with the assistance of European agencies,
- at regional/national level and cross sectoral in order to develop contacts, confidence, interoperability and synergy (like during MARSUNO project).

7.5.1 Possible roadmap towards enhanced interoperability

The context of information sharing in the maritime world is currently is marked by several existing systems or networks:

- regional information sharing systems (e.g. HELCOM, BSRBCC, SUCBAS),
- sector-based systems (e.g. SafeSeaNet for the safety community, EUROSUR),
- national systems already implemented or are not a single window concept, and
- existing capabilities in the private sector (providers of satellite information or other services).

However, most actors in MARSUNO identified the need for an improvement of information sharing and interoperability among partners.

The Project noted that cross-border exchanges already exist inside sector-based communities. They are usually based on the use of tools and systems developed for the sector determined purpose and users often express their will to keep their actual systems.

Thus an optimised information sharing environment should not replace existing systems but should provide guidelines for their evolution as well as a common interoperability framework in order to improve the global efficiency at a European level and to reduce the cost of new functionalities.

Having this in mind, several steps could be considered;

- enhancing interoperability between stakeholders by disseminating fundamental information for operations across command and situation awareness systems,
- extending sharing capabilities to support restricted data and more complex information sharing patterns, and
- encouraging cooperation effort to develop and to share value-added service.

First step: Disseminate available information

The information exchange matrices gathered during the project illustrate that there are a good number of information communities that are ready to share. Member States demonstrated possibility and will to exchange most types of information, within the legal limitations, such as relating to personal data or intelligence, as well as data from military sources. A first step towards a common information exchange environment could be to develop a common vocabulary and data models for these kinds of information by promoting standards in order to reduce specific interfaces implementations.

In this phase, existing systems mostly adapt their interfaces in order to support this model and thus to enable enhanced information sharing.

According to available technologies and modelling efforts, this goal could be achieved within reasonable time.

The establishment of N-CISEs in each Member State and Third Country is also an important first step to be taken. The N-CISE could be either virtual or an already existing but updated centre. However the most important factor is that this function has to be officially designated in each Member State and Third Country, otherwise the added value could be significantly reduced.

Second step: Extending sharing capabilities

During this phase, partners extend the information model to fulfil requirements for new interaction patterns. For instance, new data sets could be considered while developing cross sector exchanges of information (for instance, the capability to use data collected by an aircraft used for MPR for others cross-sector purposes could lead to new requirements for data modelling).

The common information sharing environment is also updated with new data and technical solutions in order to support classified information as stakeholders get more confident with the system and legislation is adapted to the needs and also appropriate agreements are reached.

Third step: Towards enhancing services sharing

The next step towards a cost effective common information sharing environment could be to adapt the design of existing systems in order to enable enhanced services.

Cooperative effort should be encouraged to develop and to share enhancing services. Regardless which organisation provides a new tool, this authority should be obliged to following commitments within e.g. an agreement to share and make it technically accessible to other operators and partners to use that system The adoption of such a solution should limit functional redundancy.

8. Annexes

8.1 Abbreviations and acronyms

8.2 Partners in the Project

8.3 MARSUNO Stakeholder Analysis

8.4 MARSUNO Action List

Other related documents:

- **Thematic report Layer 1 Integrated Border Management and Law Enforcement**
- **Thematic report Layer 2 Vessel Traffic Monitoring and Information Systems**
- **Thematic report Layer 3 Marine Pollution Response**
- **Thematic report Layer 4 Search and Rescue**
- **Thematic report Layer 5 Fisheries Control**
- **Common Information Sharing Requirements and Recommendations Layer 6 Maritime Situational Awareness**

Co-Financed under European Integrated Maritime Policy