COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 15.10.2009
COM(2009)538 final

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}

TOWARDS THE INTEGRATION OF MARITIME SURVEILLANCE: A COMMON INFORMATION SHARING ENVIRONMENT FOR THE EU MARITIME DOMAIN

1. INTRODUCTION

In its Communication on the Integrated Maritime Policy for the European Union, the European Commission undertook to "*take steps towards a more interoperable surveillance system to bring together existing monitoring and tracking systems used for maritime safety and security, protection of the marine environment, fisheries control, control of external borders and other law enforcement activities.*"[1]

The General Affairs Council of 8 December 2008, encouraged the Commission to work towards interoperability between national and Community systems so as to increase the cost effectiveness of maritime surveillance operations. This approach towards further integration of maritime surveillance was confirmed in the roadmap for the development of the European Border Surveillance System (EUROSUR), which foresees the gradual creation of a Common Information Sharing Environment for the EU maritime domain,[2] as well as in the recent updating of the Community vessel traffic monitoring and information system[3].

The aim of integrated maritime surveillance is to generate a situational awareness of activities at sea impacting on maritime safety and security, border control, the marine environment, fisheries control, trade and economic interests of the European Union as well as general law enforcement and defence so as to facilitate sound decision making.

Maritime situational awareness is the effective understanding of activity associated with the maritime domain that could impact the security, safety, economy, or environment of the European Union and its Member States. On the basis of clearly defined user needs and rights, it assists the authorities responsible for monitoring and surveillance activities in preventing and managing in a comprehensive way all such situations, events and actions related to the EU maritime domain.

The EU maritime domain encompasses the EU Member States' Territorial waters, Exclusive Economic Zones and Continental Platforms as defined by the 1982 United Nations Convention on Law of the Sea as well as all maritime-related activities carried out therein, on the seabed, subsurface, surface and above the sea such as installations, cargo, small boats and vessels flagged, owned, managed by or bound to the EU. Beyond the above, it also comprises any Search and Rescue Area and any Area of Operations that has been designated for an EU Maritime Operation under civil or military authority.[4]

---

1 COM (2007) 575 final of 10.10.2007

2 COM(2008) 68 final of 13.2.2008, 9.

3 Directive 2009/17/EC amending Directive 2002/59/EC establishing a Community monitoring and information system, OJ L131, 28 5 2009, 101. Equally relevant is Regulation (EC) No 725/2004 of 31 March 2004 on enhancing ship and port facility security, OJ L129, 29.4.2004, 6.

4 While all of the areas included in the 'EU Maritime Domain' have a direct or indirect impact on EU policy and interests, not all of them are subject to EU competence.

There is a clear need to share maritime surveillance information. Different sectoral authorities dealing with monitoring and surveillance of actions at sea gather data and operational information so as to establish the best possible maritime awareness picture for their own use. For many user communities, at present, this picture does not include complementary information gathered by other sectoral users due to the lack of mutual exchange. Developing the necessary means to allow for such data and information exchange should enhance the different users' awareness picture. Such enhanced pictures will increase the efficiency of Member States' authorities and improve cost effectiveness.

The objective of this Communication is to set out guiding principles for the development of a common information sharing environment for the EU maritime domain and to launch a process towards its establishment. To achieve this, enhanced coordination and coherence between the European Commission, the Member States and those interlocutors whom the European defence community may indicate for this purpose, should be established.

2. CHALLENGES

The following challenges are currently being faced with regard to the development of a common information sharing environment for the EU maritime domain:

Diverse user and operator communities: Both at national level and at EU level, national authorities responsible for defence, border control, customs, marine pollution, fisheries control, maritime safety and security, vessel traffic management, accident and disaster response, search and rescue as well as law enforcement are collecting information for their own purposes.

While the technological means exist to share this information in a meaningful manner, most of the information needed to build up this maritime situational awareness is still being collected by numerous sectoral systems at national, EU and international level.

While in some cases the involved authorities are unaware that similar information is collected by other authorities and systems, in other cases they are aware but unable to share this information with one another because information sharing standards, agreements, policies regarding information exchange processes currently exist only in certain user communities.

Diverse legal frameworks: The different maritime surveillance activities fall under each of the three pillars of the EU. Surveillance systems have been developed on the basis of sector-specific, international and EU legislation. Regardless of the given EU framework, nothing should prevent the Member States to integrate their maritime surveillance activities.

Cross border threats: Threats faced by Member States in the EU maritime domain often require an improved trans-national and sometimes even a trans-sectoral approach, in particular with regard to the high seas.

Specific legal provisions: International and EU legislation frame maritime surveillance activities on the high seas and with regard to the processing of personal, confidential or classified data.

3. SCOPE

Given the challenges identified above, the definition and implementation process for the establishment of the common information sharing environment can only be successful in full consultation and coordination with all the relevant user and operator communities and in full respect of the principle of subsidiarity. Neighbouring third countries should be involved, whenever deemed appropriate.

The different components of the Common Information Sharing Environment shall be understood as follows:

- '**Common**': As the information is to be shared between the different user communities, data used for this information should be collected only once.

- '**Information**' must enable user-defined situational awareness. Coming from disparate user communities, information should be identifiable, accessible, understandable and usable. Processing such information with the appropriate security safeguards must be ensured.

- '**Sharing**' means that each community receives but also provides information on the basis of previously agreed standards and procedures.

- '**Environment**' refers to interconnected sectoral information systems that allows for users to build up their specific situational awareness pictures, which enable them to identify trends and detect anomalies and threats.

The establishment of the common information sharing environment should ensure:

Interoperability: Ways and means have to be found to enable the exchange of information between sectoral systems both operational[5] and those currently being developed by the European Union and its Member States supported by EU agencies such as EMSA, CFCA, FRONTEX and EDA.[6] This requires that existing and future standards, interconnections, non-technical processes and procedures are developed and established enabling information sharing and the protection of information shared on the basis of agreed access rights. This should also lead to improved interoperability between sectoral systems within a Member State.

Improving situational awareness: The information obtained in this environment should considerably improve the situational awareness within the EU and the Member States.

Efficiency: Furthermore, this environment should also contribute to a unity of effort across entities with maritime interests by avoiding duplications in the collection of information and thereby considerably reducing the financial costs for all actors involved. In time, a multi purpose approach could be envisaged when using surveillance tools and assets from different user communities.

---

5 E.g. SafeSeaNet, CleanseaNet, EU LRIT Data Centre operated by EMSA.

6 A glossary of terms and acronyms is to be found in a Commission Staff working document accompanying this Communication.

Subsidiarity: The vast majority of monitoring and surveillance activities at sea are carried out under the responsibility of Member States. Following the principle of subsidiarity, Member States are responsible for coordinating the collection and verification of information from all their agencies, administrations and national operators, preferably via a single national coordination mechanism. Member States will also, where applicable, manage third party access rights, qualify the information and data security levels, and approve and control the selective dissemination and data security mechanisms.

4. GUIDING PRINCIPLES FOR THE DEVELOPMENT OF A COMMON INFORMATION SHARING ENVIRONMENT FOR THE EU MARITIME DOMAIN

4.1. Principle 1: An approach interlinking all user communities

The common information sharing environment should enable Member States' authorities to make a more efficient use of maritime surveillance information. Common rules and standards should be developed at Community level to optimise the exchange of information between the different user communities. Each of these communities should be given the possibility to provide and/or receive information at national level from international[7], regional[8], Community[9], military[10], and internal security systems and mechanisms[11] on a need-to-know basis, in line with conditions of use and defined user access rights, in order to build up its individual user-defined situational picture.

4.1.1. Issues to be considered

(1) *A flexible information sharing environment:* While the common information sharing environment has to be sufficiently secure, it should also be flexible enough to adapt to new users' needs and situations. This situation points to the need to enable each user community participating in the common information sharing environment to have access to as much information as possible, so as to build up an individual situational picture that meets its operational requirements. Such a need has been identified for instance in the Frontex joint operations to prevent illegal activities at the southern EU external borders.

(2) *Providing comprehensive information for better decision making:* Improved decision making capacity can only be achieved if all communities contribute. For instance, the information exchange must be two-directional between civilian authorities and defence forces, while respecting information security related rules.

---

7 E.g. AIS, LRIT.
8 E.g. BSRBCC, BSBC.
9 E.g. SafeSeaNet, EU LRIT Data Centre, CleanSeaNet, VMS, EUROSUR.
10 E.g. MSSIS, VR-MTC, SUCBAS.
11 E.g. MAOC-N, CeCLAD, FRONTEX Information System.

4.1.2. Recommendations

(1) *No data duplication:* Traffic monitoring data should be disseminated only once via the Safe-Sea-Net system[12]. This same data could then be made available to all recognized users including the defence community in accordance with the existing legal framework at EU level or though its modification as appropriate.

(2) *Interoperability across EU user communities:* EU military forces' support to civilian led maritime safety and security, including disaster response missions, requires an improvement in interoperability and connectivity of all relevant actors at national level.

(3) *National coordination:* Enhanced governance of maritime surveillance related matters should be achieved first of all at national level. Towards this end, it is recommended that authorities already identified as sectoral information hubs should serve as interfaces in the common information sharing environment.

(4) *International and regional cooperation:* Whilst building up interfaces between the different maritime surveillance systems within the EU, due care should be given to the potential of sharing selected parts of information with third countries. Issues of security and reciprocity of such information should also be considered. The five regional sea basins (Baltic, North, Atlantic, Mediterranean and Black Seas) and the Outermost Regions all represent a wide area with specific threats. Further efforts are needed to adequately respond to these threats.

4.2. Principle 2: Building a technical framework for interoperability and future integration

Building a 'Common Information Sharing Environment' for the EU 'maritime domain' may be best achieved through a non-hierarchical technical framework of maritime monitoring and surveillance systems. Such architecture should be designed as a cost effective interaction of different information layers to enable the improvement of user defined pictures. The system architecture must allow data to be inter alia collected, merged, analysed, disseminated and managed at the appropriate level of decentralisation, depending on security concerns (e.g. intelligence) and in compliance with data protection regulations, international rules and functional requirements. Best use should be made of existing systems.

4.2.1. Issues to be considered

(1) *Interoperability and interconnection of systems:* Instead of putting all the information together into a single database, each user community, should make its data accessible to other user communities who need it and are authorised to receive it. Thus, each user community should become a publisher of its own information as well as a subscriber to the information published by the other user communities on a need-to-know basis. The architecture should make the information usable through common standards,

[12] Council directive 2002/59 as amended by 2009/17 article 22 a

enable all users to trust the information they are receiving, whilst maintaining access to authorised users only.

(2) *Use of a Community based system:* For certain categories of information, it is easier and more cost-efficient to collect and disseminate the data in a centralised manner. The Community system SafeSeaNet should be used by all relevant user communities and be developed further to function as the main platform for information exchange in the EU maritime domain with regard to port arrival and departure notifications, notifications on dangerous goods, maritime security notifications, incident and accident information, AIS, LRIT and pollution monitoring. The management and future evolution of this system is carried out by the Commission, assisted by the SafeSeaNet High Level Steering Group, as defined by Directive 2002/59/EC.

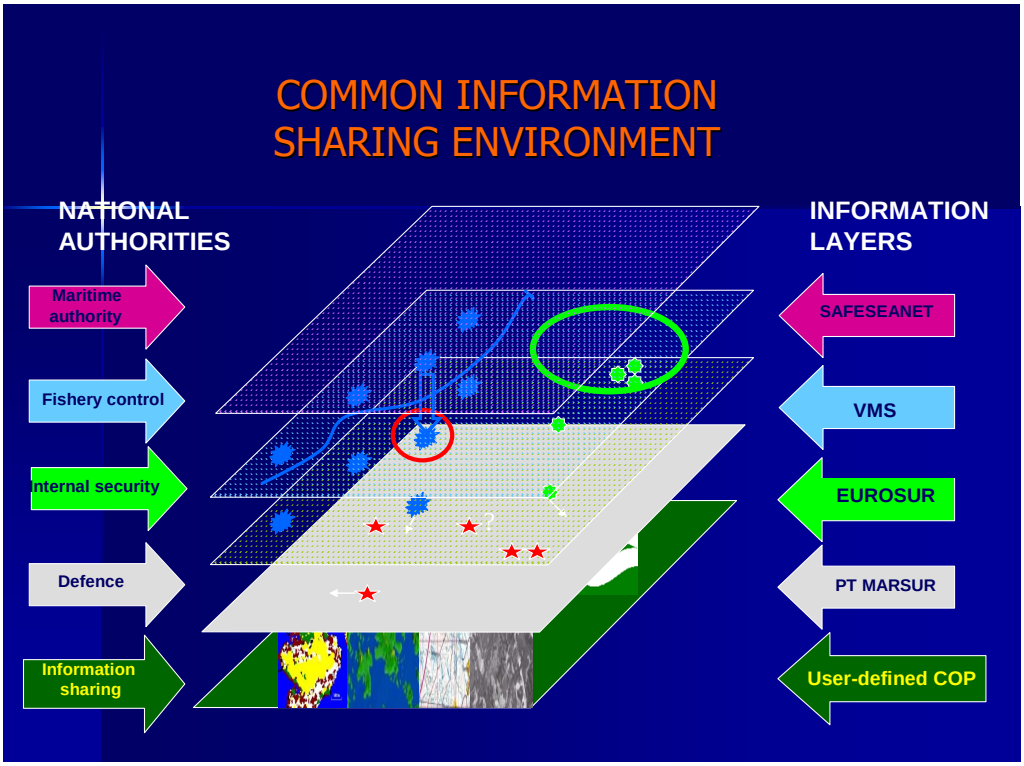
(3) *Use of sectoral systems for the sharing of classified information:* However, for certain categories of information such as classified, security-sensitive data (e.g. intelligence related to internal security and defence), a sectoral approach needs to be pursued to safeguard the security interests of the concerned user communities or recipients. In principle, such information should be exchanged on a need-to-know basis only within the relevant user community. If needed and as appropriate, this information can be shared with other user communities or recipients at national level in accordance with legislation, as well as with other Member States using Community-based systems.

(4) *Regional approaches:* Member States should consider whether to develop a capacity to elaborate a joint situational awareness of legal and illegal activities at sea which would contribute to an improved regional reaction capability.

4.2.2. Recommendations

(1) *Technical framework:* While fully taking into account the competences of national authorities as established by national and Community legislation, such architecture should be designed as a cost effective interconnection of different information layers based on interoperability and common standards. These layers should provide the user with the best technical solution for information access, powerful data mining, correlation processes and harmonised criteria for detection of normal and abnormal patterns. For this purpose, interoperable data models and standards on the handling of data have to be agreed upon, and, secure communication lines have to be established between relevant data users based on pre-defined access rights.

Example of information layers (non-hierarchical):



The collection, fusion, analysis and dissemination of information could be carried out as follows:

– **Collection:** The multiple collection of information to be disseminated, e.g. by military and civil authorities, can be avoided by using the same tools (ground based, satellite, sensors).

– **Fusion:** Fusion of data can fill information gaps and reduce the uncertainty in information received from various sources.

– **Analysis:** Security sensitive analysis should be carried out separately.

– **Dissemination:** The right information should be moved to the right decision maker at the right time. Access to information requires appropriate permissions.

(2) *Interoperability and common standards:* The architecture also calls for the best technical solution for service synchronisation, data quality and standard methodologies for vocabulary and data exchange building-up on best practices. This is of fundamental importance to ensure coherence between EU actions and those undertaken by our neighbours, particularly in shared regional seas.

(3) *EU Agencies:* Relevant EU Agencies play an important supportive and coordinative role within their user community. They could also serve as hubs for the information exchange as appropriate.

4.3. Principle 3: Information exchange between civilian and military authorities

Surveillance information should be shared between civilian and military authorities to avoid duplications and to be cost effective. Whilst recognising their distinct purposes and underlying mandates, this requires common standards and procedures for access to and use of the relevant information to allow for a two-directional information exchange.

4.3.1. Issues to be considered

(1) In respect of the missions and competences of national, regional or international authorities as established by national and Community legislation, the support of Member States' military forces to civilian-led maritime safety and internal security missions is important and requires improved interoperability and connectivity between all relevant actors. Similarly, civilian generated data can be of assistance to military operations.

(2) The enforcement of national and Community legislation requires rules and capabilities to operate on the High Seas. Technology such as the gathering and analysis of high resolution satellite images, air patrolling, the operation of unmanned platforms, the detection and analysis of underwater sounds, which so far are typical defence capabilities, are increasingly perceived as being valuable for civilian use. Conversely, civilian user communities can provide the defence community with a large contribution of relevant information on the basis of the Common Information Sharing Environment to the Recognized Maritime Picture.

4.3.2. Recommendations

(1) Enhanced coordination: To achieve the afore-mentioned goals in developing the common information sharing environment, a close coordination between the European Commission, the Member States and those interlocutors whom the European defense community may indicate for this purpose, should be established. Translating this enhanced coordination into policy orientations will be done in full respect of each user community's legal framework.

(2) Better use of surveillance tools across communities: Authorised civilian and military users should be enabled to task and to receive data from European surveillance tools for the purpose of maritime surveillance. At the technical level, this requires common rules to share, compile and present this information to individual users, as necessary.

(3) Space generated data: Europe is committed to the development of its own operational capability for Earth observation through the Global Monitoring for Environment and Security program (GMES). Improvement of maritime situational awareness using space assets can support operations carried out by civilian and military authorities such as monitoring of maritime traffic, sea pollution and the fight against illegal activities at sea. Already today, the use of space observation for monitoring marine pollution is part of the CleanSeaNet system operated by EMSA. These issues are also being addressed by GMES, contributing to security applications in the fields of surveillance of EU maritime external borders and support to EU external action.

4.4. Principle 4: Specific legal provisions

Obstacles to the exchange of monitoring and surveillance data for the purpose of setting up a common information sharing environment should be identified in EU and national legislation. In removing these obstacles, due consideration must be given inter alia to the respect of data confidentiality, intellectual property rights issues and the protection of personal data as well as ownership of data in accordance with national and international law.

4.4.1. Issues to be considered

(1) Processing of personal data: The different activities referred to in the previous sections may involve the processing of personal data. The principles of personal data protection law applicable in the European Union are to be observed in the framework of the common information sharing environment[13]. Personal data should be collected for a legitimate purpose, used and transferred for a purpose that is compatible with the initial purpose of collection.

(2) Confidentiality requirements: It appears that a significant amount of maritime reporting and surveillance data is qualified and/or has to be treated as (commercially) confidential. As regards confidentiality, the basic obstacle is the explicit nature of the confidentiality provisions in some of the key instruments relevant to monitoring and surveillance. As a consequence, 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 is the case with the current provisions for LRIT.

(3) Civil/military data sharing: With regard to a possible information and data exchange between different authorities (including military authorities), it has to be further examined how the integrity of classified information, confidential business data, information related to criminal investigations and the protection of personal data can be guaranteed.

4.4.2. Recommendations:

(1) For the sake of the legal security of all the actors involved, it is proposed that any mechanism aiming at the cross-border exchange of data from various existing databases is made subject to a clear legal framework on a need-to-know basis, defining at least the nature of the data involved, the capability of the data providers, the purposes (and the methods) of the exchange and the potential recipients of the data, as well as incorporating the necessary safeguards with regard to the confidentiality and security of (certain) data and the protection of personal data, where this may be

13 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, 31) and national provisions implementing it; Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, (OJ L 8, 12.1.2001, 1); Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data of 28 January 1981 (ETS 108). The Convention is supplemented by the Additional Protocol to the Convention regarding supervisory authorities and trans-border data flows (ETS 181, 8 November 2001) and the Council of Europe Recommendation No. R(87) 15 of 17 September 1987 regulating the use of personal data in the police sector.

relevant and taking into account existing legal provisions and operational systems at EU level.

(2) The processing of personal data for military, State security and criminal law enforcement currently remains outside of the general legal framework for data protection. However, data protection may be addressed on an ad hoc basis in specific legal instruments in these fields, both at Community and Member State level.[14] As a consequence, additional safeguards will be required in case it would be envisaged to share personal data between authorities falling within the scope of the existing legal framework for data protection (e.g. fisheries authorities) and authorities (currently) falling outside that scope (e.g. military, state security authorities).

5. LOOKING AHEAD

The *Guiding Principles for the development of a common information sharing environment for the EU maritime domain*, as explained above, aim to trigger a reflection process at EU and Member State level. This work will need to encompass all user communities so that their needs, and the policy options necessary to meet such needs, are clearly identified. Towards this end, the Commission's services cooperate with the European Defence Agency's Wise Pen Team in the framework of their mandate to issue a report on maritime surveillance.

It is proposed that in this framework, a permanent and structured cooperation between different EU actors in the civilian and military domains of the Member States should be established to find innovative solutions within the given legal framework. Such coordination could contribute to improved interoperability and connectivity between existing civilian and military systems.

It is proposed that work towards the development of a common information sharing environment should be carried out in the framework of the Commission's Member States Expert Group on Integration of Maritime Surveillance, in compatibility with other ongoing work in sectoral groups and Committees within their respective competences. In particular, the Group would address the system architecture for the information exchange between the different sectoral systems, taking into account the existing legal frameworks and examining procedural, and technological barriers to information sharing.

The building up of the common information sharing environment should not in any way hinder the development of existing and planned sectoral information systems, including their evolution, as long as the need for interoperability enabling an information exchange with other relevant systems is taken into account.

Following an iterative approach, the Guiding Principles may be revised, in particular in light of the outcome of the following three projects, which will be carried out in order to evaluate the ability of users from different Member States and user communities to exchange information:

14 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30/12/2008, p.60.

(1) Pilot project on the integration of maritime surveillance in the Mediterranean Sea and its Atlantic approaches[15]. The purpose of this 2-year project is to test the capacity of six Member States in this region to exchange surveillance information relating to border control, combating of narco-trafficking, fighting terrorism, combating the smuggling of illegal goods and preventing marine pollution. The project is expected to start at the end of 2009.

(2) Pilot project on the integration of maritime surveillance in the Northern European Sea basins[16] with similar objectives and duration as the above mentioned pilot project in the Mediterranean Sea.

(3) Under the 2010 work programme of the 7th Framework Programme for Research and Development (security theme), a call for proposals has been published for a demonstration programme aiming at large scale integration, validation and demonstration of a systems-of-systems solution for maritime border surveillance. The main issues covered are the detection of small craft, fusion of information to detect anomalies, interoperability and affordability. The solution shall be tested in a selected area of the external maritime border, showing – from a technical point of view – the way forward for the development of the common information sharing environment for the EU maritime domain. In addition, as part of the FP 7 Space theme, a call for proposals has been published to develop pre-operational GMES service capabilities for maritime surveillance.

A list of additional EU initiatives relevant for the integration of maritime surveillance is to be found in a Commission Staff working document annexed to this Communication.

6. CONCLUSIONS

An integrated approach to maritime surveillance should improve the effectiveness of the authorities responsible for maritime activities by making available more tools and more information necessary for the performance of their duties. This should result in more efficient operations and reduced operating costs. The potential savings at EU level are significant given the growing need to detect, identify, track and intercept amongst others illegal migration, illegal fishing as well as to prevent accidents at sea, to safeguard the environment and to facilitate trade. The benefits to flow from this process will positively affect national security, maritime security and safety, the protection of the marine environment, border control and, in general, law enforcement.

The Commission therefore invites the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions to:

- Support the objectives presented in this Communication;
- Sustain the proposed approach within their respective areas of responsibility.

[15] Call for proposals MARE/2008/13
[16] Call for proposals MARE/2009/41