FEBRUARY 2014
EUROPEAN COMMISSION, DG MARE

The development of the CISE for the surveillance of the EU maritime domain and the related Impact Assessment

PART 1: INDIVIDUAL ANALYSIS

COWI

COWI

ADDRESS COWI A/S
Parallelvej 2
2800 Kongens Lyngby
Denmark

TEL +45 56 40 00 00
FAX +45 56 40 99 99
WWW cowi.com

FEBRUARY 2014
EUROPEAN COMMISSION, DG MARE

The development of the CISE for the surveillance of the EU maritime domain and the related Impact Assessment

PART 1: INDIVIDUAL ANALYSIS

CONTENTS

1	Introduction	1
2	Methodology	3
2.1	Legal provisions and limitations	3
2.2	Selecting output and impact indicators	5
2.3	Measuring output and impact indicators	9
3	Baseline: risk assessment	15
3.1	Introduction	15
3.2	Risk assessment framework	15
3.3	Risk assessment analysis	19
3.4	Summary	23
4	Baseline: maritime surveillance systems and cooperation	25
4.1	Status and developments at national level	26
4.2	Maritime surveillance systems and information sharing	27
4.3	Status and developments at regional and EU level	36
4.4	Cross-sectorial and cross-border pilot projects, policies and other initiatives	49
4.5	Summary	59
5	Baseline: legal	61
5.1	Legal principles	61
5.2	General legal conditions for maritime surveillance information sharing	61
5.3	Specific conditions governing the sharing of maritime surveillance information	69
5.4	Agreements between EU agencies	81

6 Baseline: economic 83
6.1 Economic risks 83
6.2 Economic indicators 83

7 Baseline: social 95
7.1 Social risks 95
7.2 Social indicators 95

8 Baseline: environmental 105
8.1 Environmental risks 105
8.2 Environmental indicators 107

APPENDICES

Appendix A Literature

Appendix B Abbreviations and definitions

Appendix C Risk assessment

Appendix D Legal analysis

1 Introduction

Purpose of Part 1

The purpose of Part 1 of the reporting of the Impact Assessment study is to present the background for assessing the likely impacts of establishing a Common Information Sharing Environment (CISE) for the surveillance of the EU maritime domain. Hence, Part 1 presents the baseline that has been used as the starting point for the analysis, and so it is a comprehensive presentation of the foundation for the analysis of impacts of CISE policy options presented in Part 2 (combined analysis).

Part 1 is thus targeted at the reader who wants to understand and/or make use of the detailed evidence that has been used as foundation for assessing the impacts of CISE.

A solid starting point

From the outset, it is important to emphasise that the Impact Assessment study started from a solid point. Much work has been done and many thoughts have been made regarding the possible value and structure of CISE. This includes development of a CISE architecture vision and a technical costing of this; and a development and analysis of use cases, which are examples of where CISE can help to fulfil operational needs related to across user community and across border maritime surveillance information sharing between seven user communities.

This report does not repeat the findings of this prior and on-going work, but refers to the findings that are directly used and adding value to the Impact Assessment study.

Structure of Part 1

Part 1 is structured as follows:

- Chapter 2 presents the methodology that has been applied to develop the baseline for the Impact Assessment study. This concerns both the selection of the output and impact indicators to measure and how we have measured them in practice in the baseline.
- Chapter 3 then presents an assessment of the current and likely future risks within the maritime domain of the EU waters. This assessment highlights areas where there is a potential for CISE in reducing such risks, and so it sets the scene for the economic, social and environmental benefits that subsequently are analysed.

- Chapter 4 provides the baseline regarding the exiting maritime surveillance systems and the existing cooperation within and in between user communities. The result is an assessment of the exiting gaps regarding access to and sharing of maritime surveillance information, and so it is an initial assessment of the missed benefits from incomplete information sharing and insufficient cooperation – that CISE will try to reap. Focus is thus on technical and cultural limitations, but also on legal limitations.

- Chapter 5 then goes more into detail with the legal baseline. This analysis addresses the EU right to act, i.e. the principles of subsidiarity and proportionality, as well as the legal – but also administrative and cultural – limitations for a well-functioning CISE.

- Chapter 6 presents the economic baseline that looks at maritime surveillance costs and so on efficiency and cost-effectiveness aspects, and that looks at other economic cost and benefit indicators. Note that the analysis of the direct cost implications of establishing CISE – i.e. technical and administrative costs – is presented in Part 2.

- Chapter 7 then presents the social baseline that comprises an analysis of the historical and likely future developments of the selected social indicators.

- Chapter 8 similarly presents the environmental baseline.

2 Methodology

The purpose of this chapter is to briefly introduce the principles of the methodology for developing the baseline described below. The methodology is, however, most likely to be really understood when studying the different elements of the baseline.

2.1 Legal provisions and limitations

A CISE related legal approach

The findings and recommendations of the legal baseline are based on our analysis of EU and international legislation and relevant policy documents. Furthermore, it is also based on a thorough examination of CISE preparatory work undertaken, such as the outcome of the MARSUNO and the BluemassMed projects and the on-going studies performed by the Technical Advisory Group (TAG). The study is not an overall conformity check of all EU legislation involved, but concerns merely the function of the CISE.

The legal analysis that we have applied is a focused legal approach in order to define policy options for the CISE development. Also, such a legal approach allows a distinct focus on the important role of the law for the implementation of CISE; on the legal limitations and the legal initiatives needed in order to steward the CISE process.

The baseline

The analyses provide the legal assessments of the existing situation in order to verify the scope for the EU right to act. It gives an overview and understanding of the current situation (the situational awareness) with regard to user communities, related functions and access rights based upon the principle of "need-to-know and responsibility to share". The study identifies the specific objectives, defines the options, assesses the various impacts and compares the options. These activities identify options and implementing instruments.

Applying a CISE related legal approach also means that we have carefully assessed the relevant legal acts, documents and information available in order to identify and isolate the information relevant for the analysis. We do, however, not attempt to alter any of the findings or analyses of these works. The CISE process is complex, and we find that each and every CISE project and document contributes to sheer insight and perspectives useful for this process.

An EU focus

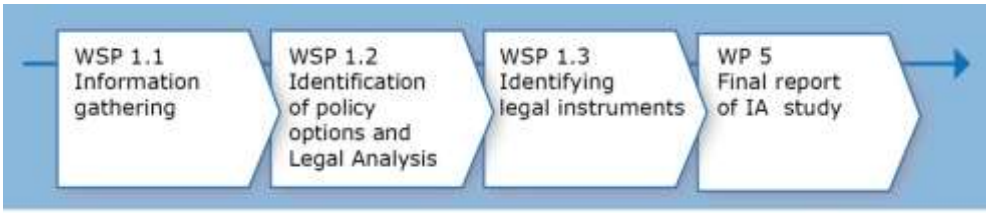
The report addresses the EU level and not directly the national limitations or competences. Such approach makes sense because the transnational nature of the CISE is characterised by the horizontal interaction amongst national administrations driven primarily by the synergies of networking. It also corresponds to the European transnational tendencies in information networking as already employed by the EU agency model and the related information networking. This means that the eventual legal and/or institutional reform of national competences is within the discretion of the Member States themselves. However, these transnational approaches imply also a significant challenge to the Member States for the successful development of the CISE, and as the overview of national responsible authorities within the different functions indicates, many national actors are involved in the CISE operations.

Flowchart of interactive approach

The methodology can be illustrated by the flowchart in Figure 2-1. The chart illustrates the linear progress in Work Package 1 (legal study) of the study evolving from information gathering towards proposing justification for appropriate models and legal instruments. However, although this figure illustrates a rather logical flow, it should be noted that all three subcomponents were implemented at the same time.

In the basic analytical approach, the outcome and lessons learnt from each sub-component feed into the subsequent component. Eventually, the combined results feed into the final report of the IA study (Work Package 5: combined analysis), which presents to the Commission the justification, proposed policy options and related legal instruments for developing CISE.

Figure 2-1 Flow chart WP 1: Towards the Final Report of the IA Study



The interactive approach is useful not only in order to generate knowledge and to consider the likely impacts of proposed options, but also to ensure trans-sectorial alignment and stakeholder perspectives. By taking such interactive approach, it is possible to analyse the impact of different policy options and to identify the selection of a subset of policy options to be analysed in more detail to achieve the full analysis of the impact of the economic, social and environmental dimensions.

The specific approach to WP 1 involves the legal assessment of the EU right to act vis-à-vis policy options and the identification of the appropriate policy options. The approach includes two stages. The first stage involves an initial impact assessment related to the identified policy options. Based on this initial assessment, the second stage identifies the most appropriate policy options, which will be subjected to full impact assessment.

Iterative information gathering

For all activities, the main objective is to develop the functional component of CISE and to identify current shortcomings in the current framework. The mapping of existing legal instruments, the interviews and consultation of stakeholders have addressed the issue of administrative cultures and traditions related to the traditional sectorial legislative thinking. Using a combination of traditional legal desk studies, interviews, stakeholder consultations, we have been able to define appropriate instruments to overcome and facilitate implementation of the functional component of CISE.

Scrutinising the current legislative framework

The study defines and proposes legal options, outline and contents of specific legislation and amendments. The study also includes proposals for specific provisions, where appropriate. However, legal drafting in itself is not part of the study. A legislation and research list, which includes more than 100 relevant legislative acts, has been developed. All relevant acts have been carefully scrutinised in order to identify any possible limitation for information sharing within user communities, across borders and/or across user communities.

Apart from the legislative material, documents and information mentioned above, we keep in mind the extended geographical coverage of the study addressing the EU interests in maritime surveillance. The outcome of the analysis is presented as a list of specific legislative acts for each user community, which could contribute to an efficient implementation of CISE if changed, amended or updated.

Mapping and gap analysis

In the process of finalising the legal assessment, the findings and drafts have been presented to other DGs via inter-service consultation meetings where comments were received and subsequently implemented. Moreover, the findings of the legal desk study assessment have been verified by a comprehensive mapping and gap analysis that includes nine onsite interviews with relevant stakeholders covering a broad range of user communities and a questionnaire distributed to experts in Member States via the Member State Expert sub-Group (MSEsG). Finally, the findings of the legal study have been discussed with the Cooperation Project (WP4 on Access Rights), MSEsG and the TAG.

2.2 Selecting output and impact indicators

2.2.1 Risk assessment

Identifying risk picture …

An assessment of the situations and events that may negatively affect the EU maritime domain in the forthcoming 15 years is central for highlighting whether and where there is a potential for CISE in reducing such risks. Furthermore, the identification of the risk picture is the first step in the elaboration of the baseline scenario.

… via analytical approach developed and implemented by WPI …

The analytical approach for this Impact Assessment study has been developed and implemented by Wise Pens International (WPI), a team of high-level and highly recognised experts in the maritime field. Their approach and preliminary results were presented and discussed at the Technical Advisory Group (TAG) meeting of 2 July 2013. Their analytical approach involves the establishment of a framework for

examining and categorising the risks, as well as by distinguishing the areas of focus (see Appendix C for a full presentation).

… that allows the existence of uncertainty …

Any attempt to estimate the risk picture entails an inherent level of uncertainty. On the one hand, this relates to the fact that a prediction of the future is attempted, which contains an intrinsic level of uncertainty; one that increases along with the timeframe in consideration. On the other hand, any risk is subject to a number of factors (vulnerabilities, source, and probability of occurrence) that further complicate the picture. To the extent that historical data are available, attempts can be made to analyse and understand their development and use that knowledge to extrapolate in the future. However, as history has taught us (from market crashes to terrorist events), previously unforeseen or new factors may play a role. It is therefore these "unknown unknowns" that provide an extra dimension of uncertainty.

… that adopts the Delphi method …

In attempting to estimate (even broadly) the maritime risk picture in the EU, the Delphi method was the core of the approach that was followed. Despite its shortcomings (as any predictive method), the Delphi approach is a widely accepted predictive tool that has been used in numerous studies. In this case, a limited Delphi method was used whereby the WPI expertise was combined with the expertise of EU Agencies. This approach was presented and discussed with the TAG in July 2013.

… and the danger estimation approach

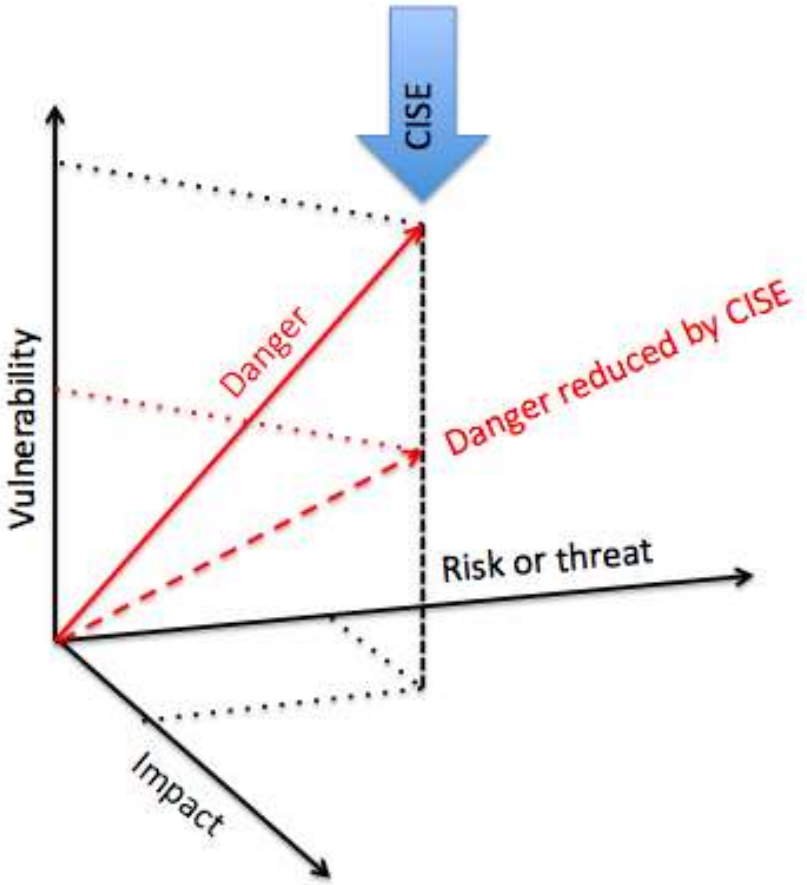
Risks and threats can be viewed similarly whether the event being studied is natural/accidental or man-made. They can be studied individually, and the consequences of incorrect information exchange or action taken in each case isolated, quantified and ranked and regional differences and their status relative to the impact/probability dichotomy taken into account.

Estimating Risk

Risks or threats, vulnerabilities and impact (or consequence) can, as shown in Figure 2-2, also be plotted in a three-dimensional diagram (risks and threats sharing the same axis). *Danger* is plotted as the combination of the three components. While CISE acts mostly by reducing the vulnerabilities, it follows that a consequence of it is the reduction of the overall danger. This is, however, a conceptual diagram, where the relations between the plotted elements do not have to follow the mathematical relations implied by the geometry.

"Risk or threat" and "impact" represent an assessment of the importance of the phenomenon and of its impact on Europe's safety and security. Likewise, "contribution by CISE" represents a judgement on the palliative effects on the vulnerability, and hence to the overall danger, in each specific case if a CISE is achieved. "Danger" is a quantity akin to the mathematical *expected value* of a random success, i.e., the composition of *risk/threat* and *consequence* (assuming a standard vulnerability and reducing the result to a homogeneous scale). "Danger reduced by CISE" is the result of diminishing the "danger" in proportion to the reduction of vulnerability due to the contribution of CISE, and again reducing it to the homogeneous scale. All this follows the logic of the vectors shown in the figure. It is important to note that absolute values have no meaning, the only purpose being to provide a graphical representation of the relative judgements. The analysis is broken down by individual basins as described above.

Figure 2-2 Danger estimation approach



Source: Wise Pens International.

Use of supporting data

An extended effort has been made to identify data sources that can provide an indication of the existing as well as the future risk pictures. However, limitations in the availability of such sources have been uncovered, not least as in many cases risk is linked to security aspects, where publically available information is either limited or restricted. In any case, data sources have been identified and used (to the extent possible) as indicators by the WPI experts, assisting them in making their judgements[1]. Any information gaps have been covered through the individual expert's own knowledge, and they constitute an original analysis.

2.2.2 Outputs and impacts

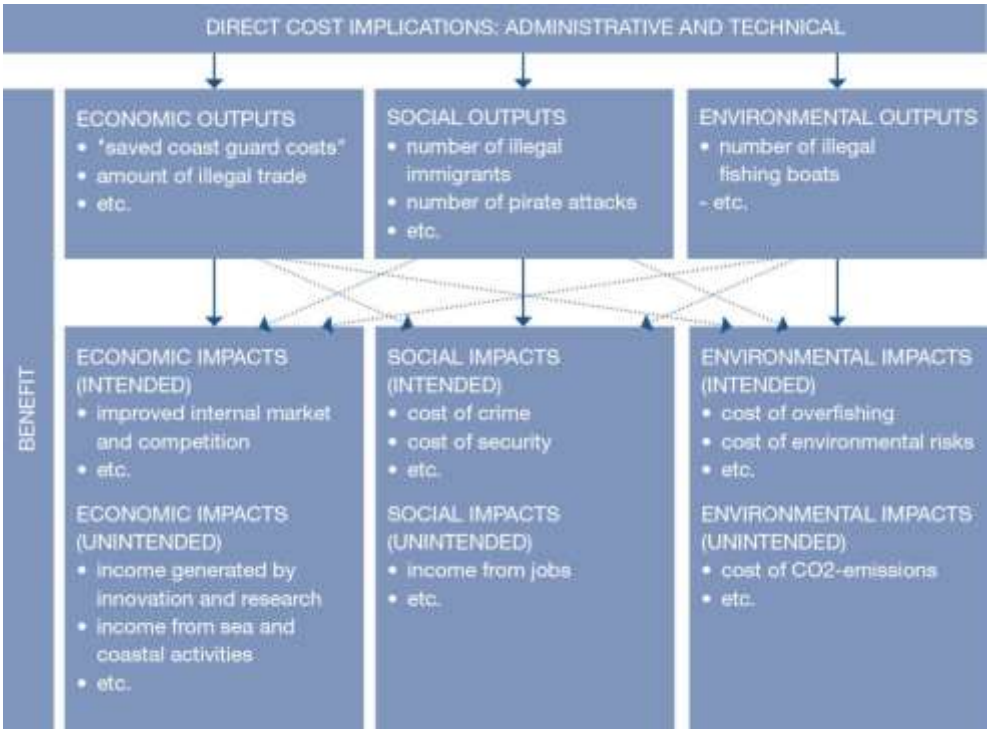
Direct and indirect results of maritime functions

Improvements to maritime surveillance - due to CISE - will imply that the user communities will improve the performance of their maritime functions. This improvement will lead to both direct and indirect results. As described in the following we call these results "outputs" and "impacts" respectively.

[1] Sources and indicators identified are presented in the WPI report in Appendix C

Building upon the above risk assessment the economic, social and environmental output indicators are selected, where the outputs are the changes that may occur as CISE will improve the performance of maritime functions via (i) more, (ii) more adequate, (iii) more relevant, (iv) more reliable, and (v) more timely information. For example, the maritime functions may become better at avoiding: illegal trade (economic dimension), illegal immigration (social dimension), and illegal fishing (environmental dimension). These outputs may lead to impacts such as improved market conditions, lower cost of crime, and lower cost of overfishing. Figure 2-3 serves to illustrate different examples of outputs and impacts.

Figure 2-3 Outputs and impacts



Intended and unintended impacts

Figure 2-3 also shows that we - in line with the EC Impact Assessment guidelines - distinguish between intended and unintended impacts. The intended impacts are those we measure to assess the success in pursuing goals that are closely linked to the EU maritime domain and that are directly affected by the achievement of the outputs. Secondly, we look at the unintended impacts, i.e. (major) indirect positive or negative changes due to the improved maritime functions (surveillance) that should be considered when choosing the CISE policy option.

As indicated in Figure 2-3, we have monetary measures (i.e. Euro) in mind when assessing impacts. This makes them comparable with the cost measures. However as also discussed in more detail below, it is not always feasible to provide monetary impact measures, and so alternative measures are pursued.

Finally, emphasis must be on avoiding double-counting when measuring both, outputs and impacts.

Additional selection criteria

In addition to building upon the risk assessment, a number of other selection criteria have been applied:

- Criterion 1: Manageable number. There has been is a need to delineate the economic, social and environmental dimensions covered by this study, and hence to limit the number of outputs and impacts to be assessed. A first and obvious criterion has been to keep the scope of the assessment manageable within the resources allocated to the present study. This is also in line with the principle of proportionality.

- Criterion 2: Relevance. It is obvious that the economic, social and environmental outputs and impacts we assess must be relevant. With relevance is meant that the values of the output and impact indicators change if the performance of the maritime functions increase, and in particular if this improved performance is due to improved maritime surveillance, and especially if due to improved sharing of information. Hence, this criterion is mainly fulfilled by building upon the above risk assessment.

  Furthermore, the selection of output and impact indicators is guided by the wider EU policy goals. This said, we have not provided precise measures of how improved maritime surveillance contributes to such EU policy goals or to EU internal and external security strategies and cooperation with third countries. The ambition has merely been to highlight how improved maritime surveillance may underpin the EU social agenda and policy goals.

- Criterion 3: Measurability. It is also obvious that the outputs and impacts should be measurable. If not we will not be able to assess the impact of CISE. In this effort, we have tried to avoid the risk of selecting measurable outputs and impacts at the cost of them being less relevant. In other words, we have attempted to strike a balance between relevance and measurability. Furthermore, this criterion implies that the estimates of the cost and benefits will not comprise everything, but be based on the main cost and benefit items.

- Criterion 4: Acceptance. Since the CISE policy option is chosen by the central stakeholders/decision-makers, such as DG MARE, the Steering Group and other stakeholders such as the TAG and the MSEsG, based on its expected economic, social and environmental impacts, they must accept the coverage of the output and impact indicators. Furthermore, since many of the indicator measures and their respective development are associated with much uncertainty. The acceptance of this uncertainty by the central stakeholders/ decision-makers is of outmost importance. We have pursued this acceptance via stakeholder consultation and via establishing the above risk picture – with external assistance from Wise Pens International.

2.3 Measuring output and impact indicators

The selected output and impact indicators have for the baseline and also for the impact analysis in Part 2 been measured. We have in this context gathered information from different angles – that each has its strengths and weaknesses.

2.3.1 Official information sources

Official statistics

Since CISE is an EU-wide initiative, its impacts on the EU as a whole are in focus. This emphasises the strength of Eurostat - e.g. via its online database[2]. The main weakness is that only few of the data series in the database are directly linked to maritime functions. Moreover, Eurostat only covers developments that are easily measurable - which is not always the case for the indicators we are looking for.

Hence, our method was to take a starting point in the Eurostat database for the baseline description of a given output or impact indicator - e.g. a rough baseline that might be refined by using other information sources.

For more specific maritime functions data - with links to maritime surveillance - we looked into what is immediately available from international organisations and EU agencies with relevance for maritime surveillance (see Table 2-1).

Table 2-1 International organisations and EU agencies with relevance for maritime surveillance

Institution/ agency	Key areas of responsibility	Information systems that the agency is in charge of	1 Safety and security	2 Fisheries control	3 Environment	4 Customs	5 Border control	6 Law enforcement	7 Defence
DG MARE	Support the EU maritime economy. Secures safe and stable supply of seafood, sustainable fisheries, healthy seas and prosperous coastal communities.	FIDES EMODNet		x	x				
DG TAXUD	Manages, defends and develops the customs union as part of protecting the external borders of the European Union.	E-Customs ECS/ICS/NCTS				x			
EC agency operational management of large-scale IT systems	Ensures effective, secure and continuous operation of the EU IT systems. Ensures security of the systems and the data.	SIS VIS EURODAC	x				x	x	
EDA	Improves the EU's defence capabilities; promote armaments cooperation; strengthen the EU defence industrial and technological base and creates a competitive European defence equipment market.	NEC							x
EEA	Provides sound, independent information on the environment.	SEIS			x				
EMSA	Operational support to oil pollution responses, vessel monitoring, tracking and identification. Support to EU legislation on maritime safety, pollution by ships and maritime security.	CleanSeaNet SafeSeaNet THETIS EU LRIT DC S-AIS	x		x			x	

[2] http://epp.eurostat.ec.europa.eu/portal/page/portal/statistics/search_database

Institution/ agency	Key areas of responsibility	Information systems that the agency is in charge of	1 Safety and security	2 Fisheries control	3 Environment	4 Customs	5 Border control	6 Law enforcement	7 Defence
ESA	Shapes development of Europe's space capability. Ensures that investment in space benefits the citizens of Europe and the world.	Earth Observation Systems S-AIS	x		x			x	
Europol	Prevents and combats all forms of serious international organised crime and terrorism.	SIENA				x	x	x	
FRONTEX	Develops and operates information systems that enable data exchange on situational awareness for border control authorities in the EU.	EUROSUR	x				x	x	
DG ECHO/MIC	Supports the mobilization of emergency assistance in the event of major disasters, disseminated emergency alerts, status and response information.	CECIS	x		x				
NATO	Defence of the NATO territory.	MSSIS MCCIS					x		x
NAVFOR	Protection of vessels. Deterrence, prevention and repression of piracy and armed robbery at sea.	Mercury							x
SatCen (EUSC)	Supports decision-making of the European Union by providing analysis of satellite imagery and collateral data.	SatCen (EUSC)	x						x
SUCBAS	Enhances maritime situational awareness benefiting maritime safety, security, environmental and law enforcement activities in the Baltic Sea.	SUCBAS	x		x			x	X

Source: Based on extracts from the Deloitte Study and own review.

Furthermore, we looked into the coverage of information from the OECD or other international sources - in particular for the need of looking ahead regarding certain baseline developments.

Other official information sources

In addition to data needs there was also a need for other information from official information sources. There was, for example, much relevant information in the reports, websites etc. provided by the different Integrated Maritime Policy (IMP) actions.

Furthermore, we looked for other research findings particularly regarding possible output and impact measures.

2.3.2 Questionnaire survey

Questionnaire

A Member State questionnaire survey was conducted. In this context, a questionnaire was sent to participants of the Member State Expert Group on Maritime Surveillance who, for the purpose of this survey, were identified as contact points for Member States and participating EEA States. They were kindly requested to coordinate with other administrations involved in Maritime

Surveillance in their respective countries and compile the various inputs and responses into one single response per country.

The questionnaire was divided into two parts:

- Part 1: Problem definition, policy options and impacts regarding information sharing as well costs related to maritime surveillance in the Member States. The responses to this section of the survey were used for the present Impact Assessment study.

  Part 1 had four sets of questions. The first set addressed the extent to which barriers may currently limit and/or prevent the sharing of information across sectors and across borders between public authorities acting for the surveillance of the EU maritime domain. The second set of questions addressed the different policy options to enhance information sharing and co-operation across sectors and borders between public authorities involved in maritime surveillance. The third set asked about the expected benefits at EU and Member States levels from enhanced information sharing across sectors and across borders (in terms of efficiency and cost effectiveness gains as well as potential economic, social and environment benefits). The last set focused on resources spent on current surveillance activities in the Member States (in terms of staff and assets).

- Part 2: Existing IT systems and initiatives in support of maritime surveillance, collaboration tools, standards and maritime domain awareness definition and building. The responses to this part of the survey were be used as a basis for documenting available building blocks on which CISE can capitalise with a further view to maximise the benefits and minimise the cost impact on participating administrations. Hence, it provided valuable input to the technical costing study carried out by Gartner.

Response rate

Of the 23 coastal Member States in the EU, a total of 13 responded (Table 2-2). Norway, that was invited to participate, also responded.

Table 2-2 Respondents to the MSEsG survey

Response	No response
Belgium	Bulgaria
Finland	Croatia
France	Cyprus
Germany	Denmark
Greece	Estonia
Ireland	Malta
Italy	Portugal
Latvia	Romania
Lithuania	Slovenia
Netherlands	Sweden
Norway*	
Poland	
Spain	
United Kingdom	

** Not member of the EU*

The fact that 10 Member States did not respond naturally affects the results of the survey. The results should therefore only be taken as providing indications. This caveat is underlined by the fact that not all responding Member States provided full answers to all questions; and some interpreted the questions differently. In an effort to provide comparable and consistent summary statistics, certain assumptions have therefore been applied to some of the answers.

2.3.3 Interviews

Member State interviews and workshops

To support the Impact Assessment study and substantiate the answers provided to the MSEsG survey, we also conducted a number of interviews/workshops with both Member States and EU agencies. The meetings typically took place as full-day focus groups with representatives from all user communities. However, not all user communities were represented in all Member States. The focus group format of the meetings nonetheless led to good discussions between the sectors on the questions that were addressed, and many of the participants knew the other (non-represented) sectors quite well. As regards the baseline, the discussions touched upon many topics of importance; including current national information sharing setup, experienced limitations to information exchange experienced, cost of surveillance, and future trends as regards information sharing environments and initiatives. A total of seven Member States were interviewed (see Table 2-3).

Table 2-3 Member States covered by interviews/workshops

Member State	User communities represented						
	Maritime safety	**Fisheries control**	**Marine pollution**	**Customs**	**Border control**	**General law enforcement**	**Defence**
Finland	**X**	(x)	(x)	(x)	**X**	(x)	**X**
France		**X**		**X**			**X**
Germany	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Portugal		**X**				**X**	(x)
Italy	**X**	(x)	(x)	**X**	**X**	**X**	**X**
United Kingdom	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Spain	**X**	**X**	**X**	**X**	**X**	**X**	**X**

*Note: **X** denotes the presence of one or more user community representatives, and (x) denotes that the user community was partly represented through other authorities.*
Source: COWI.

2.3.4 Public consultation

A public consultation has been carried out by DG MARE, using the Interactive Policy Making (IPM) Tool and was online for 12 weeks and closed on 14 September 2013. The findings and recommendations from the public consultation are presented in the Public Consultation report.

2.3.5 Cooperation Project

Baseline and impact information

Through the involvement of numerous maritime surveillance experts, the Cooperation Project provides a number of use cases where CISE in particular is envisaged to give high benefits by improving sharing of maritime surveillance information. In addition, these use cases have been subject to concrete cost benefit analyses using our guidance (see below), and in this way the Cooperation Project has directly provided estimates of impacts of CISE used in this Impact Assessment study.

Furthermore, specific baselines for the use cases have been elaborated. These take their starting point in the relevant maritime surveillance performance and in a description of maritime surveillance information exchanged/shared at present (or could be so with benefit).

COWI guidance

COWI has provided guidance to the Cooperation Project WP3, the results of which are high-value inputs to the Impact Assessment study. The guidance includes:

- Guideline: the general guidance to calculating costs and benefits of use cases (mainly developed by the Cooperation Project WP2)
- Narrative Note: an example/guidance to further developing the narrative of the WP2 (and possibly other) use cases
- Excel-tool: that follows the step-by-step guide outlined in the "Guideline" along with various descriptions of the information needs (not suitable for inclusion in a Word-document)
- Macro Note: describes the kind of information that would be relevant to gather on a more general level (not specific to the use case); that is, the overall risk picture, and the overall surveillance outcomes and costs.

Furthermore, DG MARE has contributed to the development of the methodology for assessing the benefits of the different CISE policy options.

3 Baseline: risk assessment

3.1 Introduction

Purpose of and approach to risk assessment

As presented in the above methodology chapter, an assessment of the situations and events that may negatively affect the EU maritime domain in the coming 15 years is central for highlighting whether and where there is a potential for CISE in reducing such risks. Furthermore, the identification of the risk picture is the first step in the elaboration of the baseline scenario. Hence, the analysis looks at the areas where CISE can provide added value and establish the basis of the estimation of its impacts. The analysis that follows is based on the latest available information and draws on the experience of recognised experts in the maritime field (Wise Pens International – WPI). Their approach and preliminary results were presented and discussed at the Technical Advisory Group (TAG) meeting of 2 July 2013.

3.2 Risk assessment framework

This risk assessment divides the possible situations and events that can affect the risk picture in the EU waters into challenges, risks, threats and vulnerabilities.

Challenges

In this context, challenges are understood as "tasks or situations that test existing abilities". For the future, the primary challenge will be to protect all elements of the maritime domain in order to maximize a safe and secure use of the EU waters while developing a sustainable maritime economy that takes account of natural resources, biology, minerals, energy and water. These challenges can be affected by internal factors such as:

- Difficulty of creating and sustaining political momentum
- Lack of clarity in the chain of command
- Friction created by different agencies, both at EU and national levels – that makes it difficult to create and implement an open exchange of information, e.g. due to the protection of agencies' competences or interests.

- Absence of a set of political guidelines covering both civilian and military operational units in conflict situations
- Lack of consensus among European stakeholders on basic definitions
- Misunderstandings stemming from linguistic and governance issues.

All these challenges can be summarised into a general difficulty of securing exchange of information as freely as possible at the EU level, and between actors with different maritime responsibilities at national level.

Specific risks and threats

There is a more detailed definition of risk (in contrast to the overall risk assessment) dealing with specific risks. This definition is "*situations likely to result in danger or an unwelcome outcome if certain events turn out in undesired ways*." Threats are here understood to come from "*Actors intent on coercing or directly causing danger or damage*." They are always, therefore, man-made and deliberate. Threats usually have a pre-existing and closely associated risk, as both threats and risks are the *actor* taking advantage of the risky situation, and the *situation* itself, of the same man-made danger of damage. Therefore, for the purpose of this study, risks of man-made dangers or damage are treated together with their associated threat. Risks of accidents or natural catastrophes have been considered independently.

Man-made threats and risks

The man-made activities which pose risks and threats to the EU and its population can be classified as:

- Those directly affecting European territory and citizens from the sea (e.g. illegal immigration, arms trafficking, etc.).
- Those that affect European maritime interests, such as threats to the flow of energy and other strategically important commodities along major trade routes, most notably in geographical chokepoints.
- Those that affect Europe's own resources at sea, such as fisheries and oil or mineral deposits within Member States' exclusive economic zones (EEZs), wind farms, tidal or wave power hubs.

Accidental and natural risks

Risks of unintended accidents or natural catastrophes include:

- Those directly affecting European territory and citizens from the sea, such as tidal aptitudes or tsunamis.
- Those that affect European maritime interests, such as threats to the flow of energy and other strategically important commodities along major trade routes, most notably in geographical chokepoints (e.g. pipelines).
- Those that affect Europe's own resources at sea, such as fisheries and oil or mineral deposits within Member States' EEZs, wind farms, tidal or wave power hubs (e.g. risks to biodiversity, marine accidents, etc.).

All these risks and threats, as well as other criminal or unlawful activities at sea, affect not only Europe but also countries across the globe. For example, today irregular immigration and narcotics trafficking from overseas constitute significant internal threats to the EU. Illegal, unreported and unregulated (IUU) fishing, toxic waste dumping and illegal oil bunkering severely undermine the economic viability and internal stability of African coastal states, while also providing an alibi for the practitioners of piracy. The inability of weak or failed states to control their maritime areas is a contributory factor to destabilization (e.g. Guinea Bissau, Somalia and small island states in the Caribbean). The impact of illegal narcotics in West Africa could also lead to the overthrow of governments and possibly widespread de-stabilization in the near to medium term. Natural disasters, in addition to their initial destructive effects, can often create conditions in which these risks and threats can emerge.

Vulnerabilities

Vulnerabilities are understood to include susceptibilities to harm, either from natural causes, accidental, or man-made. While they pose no immediate harm in the normal course of events, they must nevertheless be minimised in order to prevent an opponent from exploiting them.

For example, an important vulnerability is that all EU Member States, even the landlocked ones, depend on the sea, as they all benefit from maritime trade through European ports and from the supply of minerals, foodstuffs, seafood and energy. Any interruption in these supplies could have a significant impact on the quality of life of the people of the EU.

High probability/ Low impact versus Low probability/ High impact events

All the above classifications have to be viewed under the dual prism of probability and impact. Not all risks have the same probability of appearing neither would they have the same impact if they occur. This in turn is known to affect how the public perceives risks, since this in turn drives the political response. Familiarity or frequent false alarms can create a feeling of complacency, whereas the novel or rare event tends to steal the headlines.

An example to illustrate this effect in relation to the topic under discussion is for instance IUU fishing and irregular immigration that are typically high probability/low impact events, while the *Costa Concordia* grounding represents a low probability/high impact event. The disruption of maritime trade, due to disputes between regional powers, as in the Persian Gulf from 1980 to 1988, or a disaster occurring in an EU harbour due to a ship with explosives or weapons of mass destruction (WMD) are low-probability but potentially high impact events requiring appropriate preventive measures.

Table 3-1 Risk classification overview

Affecting:	Territory and citizens	Maritime interests	Maritime resources
Challenges	• To establish an EU-wide CISE • To promote collaboration between constabulary organisations, both at national and international level.	• To establish an EU-wide CISE • To promote bilateral discussions on sovereignty issues	• To establish an EU-wide CISE • To promote collaboration between national coast guards and SAR organisations.
Man-made Associated Risks	• **Terrorism at sea or using the sea as conduit** • **Use of vessels with explosives or WMD against port facilities** • Irregular immigration and related border crime/human trafficking. • Narcotics trafficking • Arms trafficking	• **Piracy** • **Local wars in the vicinity of chokepoints** • Smuggling • Non-EU claims disputing EU's TTW/EEZ borders • Disputes between regional powers affecting trade	• Environmental degradation. • IUU fishing. • Illegal discharge of oily bilge and ballast water. • Quest for archaeological artefacts and treasure.
Risks of Accidents and Natural Catastrophes	• **Tsunamis and storm surges**	• **Damage to underwater pipelines and communications cables**	• **Collisions, groundings, wrecks, cargo fires or explosions** • Risks to biodiversity • Accidents in offshore oil and gas platforms, and wind, wave and tidal energy farms.
Vulnerabilities	• Easy access from the coast to the heartland • High number of tourists and expatriates • Low lands openness to weather and rising sea level	• Critical dependence on maritime commerce	• High dependence on fishing • Large number of vulnerable offshore oil, gas platforms and wind, wave and tidal infrastructure (with limited experience in the last group)

Note: High impact/Low probability events in **bold**.
Source: Wise Pens International.

Regional differences

In trying to evaluate the relative importance of different negative events, regional perceptions and requirements vary markedly between regions and sea basins. Prominent Mediterranean risks and threats such as irregular immigration could be very rare on Europe's Atlantic coast, whereas pollution from a dense network of oil platforms as in the North Sea would be of less concern in the Mediterranean. As such and for the purpose of this study, the European maritime domain is divided into the following maritime areas:

- Baltic Sea
- North Sea
- Celtic Sea
- Bay of Biscay and Iberian Coast and Islands

- Mediterranean
- Black Sea
- Arctic Ocean
- Overseas regions
- External waters (i.e. the high seas and areas away from Europe).

Generically, these zones are also referred to as *sea basins*[3]. It departs slightly from the European Atlas of the Seas' *sea basins* in ascribing the Azores, Madeira and Canary Islands to the Iberian Coast, rather than to the "Outermost Regions". However, for statistical purposes, the Portuguese and Spanish Atlantic Islands are better treated this way instead of together with the French Overseas Territories.[4]

3.3 Risk assessment analysis

While the detailed risk assessment analysis – based on the Delphi consultation approach – is found in Appendix C, the purpose is here to provide an overview of the situations and events that may negatively affect the EU maritime domain in the coming 15 years. This is central for highlighting whether and where there is a potential for CISE in reducing such risks. This is done risk indicator by risk indicator, and thus provides a central part of the foundation for the selection and analysis of economic, social and environmental indicators.

Terrorism at sea or using the sea as conduit

The contingent nature of terrorism makes predictions extremely risky, as changing political circumstances may change the landscape completely. However, the number of incidents has fallen in recent years, and is expected to remain at such lower level in the years to come.

Within the EU waters, the risk is mainly expected to remain in the Mediterranean and the Black Sea. However, since the impact of a terrorist attack may have particular impact in the Arctic Ocean – this also a sea basin in which CISE may reduce the danger in the future.

[3] See the European Atlas of the Seas, http://ec.europa.eu/maritimeaffairs/atlas/seabasins/index_en.htm

[4] The list of French Overseas Departments and Regions quoted in the European Atlas of the Seas misses Mayotte, as well as a number of French Overseas Territories and Collectivities and Special Collectivities, which are nevertheless relevant for any maritime purpose, irrespective of their individual political status, as they generate extensive EEZs for which France retains responsibility.

Use of vessels with explosives against port facilities	There is no specific data for this form of terrorism and experts have no records[5] of any recent incidents. Furthermore, it is not known whether there have been failed attempts. Hence, the assessment that there is a potential for the reduction of the danger via CISE is made on a very uncertain basis.
Irregular immig-ration/human trafficking	Although there has been a significant decrease in irregular immigration/human trafficking in 2012, it is acknowledged that it is a very volatile data set. Furthermore, the civil war in Syria has already this year meant an increase again in the figures for 2013. The Delphi consultation reveals that the risk is expected to remain high, in particular in the Mediterranean and the Black Sea. These are also the areas where there is an expected added value from CISE in reducing the dangers.
Narcotics trafficking	Although figures in a comprehensive study by UNODC[6] are provided, they are presented in such a way that makes it impossible to produce an analysis based on the means of transport (essential for a maritime security study). However, it is evident that overall narcotics traffic in Europe remains stable. Some narcotics, such as synthetic drugs, seem to be slightly in the ascendant, but this is counterbalanced by a reduction in the consumption of other, more traditional drugs, such as cocaine. Cannabis remains by far the most commonly consumed drug in Europe, an estimated 37,113 kg in 2012. Similar to above, the Delphi consultation point to the Mediterranean and the Black Sea for area where the risk is expected to remain and where there is a potential for CISE to reduce the danger.
Arms trafficking	Arms trafficking spans a range of illegal activity from low-level small arms smuggling for criminal purposes to shipping weapons in sufficient bulk or of sufficient sophistication to conduct a terror campaign or to destabilise a regime. Although the potential utility of CISE according to the Delphi consultation is obvious, the range of effects and paucity of recorded data prevents meaningful quantitative analysis here.
Piracy	Data for Somalia shows a clear downward trend in both the number of attacks and in their relative success (i.e. completed hijacks). But the optimism these figures suggest must be tempered by the observed increase in piracy incidents in the Gulf of Guinea, mostly off the coasts of Nigeria, Benin and Togo, which, according to the IMB[7], have already surpassed those off the coast of Somalia this year.

[5] Apart from the failed attack on USS *The Sullivans* (2000), and the partially successful one on USS *Cole* (2002), while in Aden, Yemen, that didn't affect the harbour facilities.
[6] http://www.unodc.org/unodc/en/data-and-analysis/WDR-2012.html
[7] The discrepancy in the figures provided by the IMB and Operation Atalanta HQ for Somalia can in part be explained by the different definitions used: IMB counts any report of suspicious behaviour as an *incident*, while Atalanta HQ only counts actual attacks. Nevertheless, IMB statistics are very useful to appreciate the relative weight of the

While CISE has a potential for reducing this danger overseas, the risk is considered to remain low within EU waters.

Local wars in the vicinity of chokepoints

The trade routes that link Europe to the key commercial areas of the East are punctuated by chokepoints, several of which have been in the past, and may potentially be in the future, affected by local wars that, while perhaps not directly affecting European political interests, have nevertheless caused the closure of or traffic restrictions in the chokepoint. The entire Europe-Asia trade route is thus affected, and with it European economic interests, requiring expensive diversions and even the construction of new classes of ships.

While it is assessed that there here is a potential for CISE added value, it is also considered to be difficult to quantify this impact.

Smuggling

Smuggling is widespread and is facilitated by the use of containers. This entails mostly counterfeit goods imported from Asia in increasing quantities, to be sold on the roadsides of our cities by immigrants. Even though most EU nations are attempting to deal with this threat, the degree of success is still low, as enforcement takes place mostly ashore, after the goods have been imported, when it is too late.

Also here, the Delphi consultation points to a potential for CISE in reducing smuggling, and again this potential is within EU waters assessed to be highest for the Black Sea and the Mediterranean.

Non-EU claims disputing EU's TTW/EEZ

Non-EU claims disputing EU's TTW/EEZ borders apply mostly in the Mediterranean, where various disputes are still on-going. Notorious examples, but by no means the only ones, are the differences between Turkey and Greece or Cyprus. It is therefore also here where it is expected to be the highest added value from CISE.

Disputes between regional powers affecting trade

Disputes between regional powers affecting trade are still an issue. It should not be forgotten, for instance, that India has militarized the Andaman and Nicobar Islands, facing the Straits of Malacca, and a dispute with China might affect EU trade in the area. Hence, there might be an added value from CISE, but it is difficult to assess.

IUU fishing

IUU is assessed[8] to account for 20% of the global catch and to contribute to economic losses of $10-23 billion, while also threatening 260 million jobs that depend on marine fisheries around the world. For the EU waters, this is also considered to remain a high risk, and an area where there is a potential for added value from CISE.

Somalian piracy against the rest of the world, as the criteria are homogeneous, even if no trend is indicated.

[8] See "The Global Extent of Illegal Fishing", by MRAG.

Illegal discharge of oily bilge and ballast water and other environmental degradations	EMSA gives a figure of illegal discharge of oily bilge and ballast water and other environmental degradations. This figure indicates the size of the problem, although it does not provide information about trends. Despite the accuracy and promptness of the data EMSA provides, the low level of enforcement by nations suggests that the trend is probably negative or stable. During the period 16 April 2007-31 December 2009, 7193 possible spills were detected by EMSA's CleanSeaNet, of which 1997 were verified on site by Member States and 542 were confirmed as being mineral oil. However, even these figures are just the visible part of the problem, as CleanSeaNet cannot detect many other cases of comparatively minor waste dumping that add up to considerable environmental degradation. Hence, the Delphi consultation reveals that there is significant potential for CISE adding value to the detection process carried out by SafeSeaNet, and that this potential is apparent in all EU waters.
Quest for archaeological artefacts and treasure	While plundering of the ocean's riches recently achieved prominence during the protracted and high profile legal battle between the Government of Spain and the US company Odyssey, the judgement against Odyssey has discouraged further exploration by them and other freelance companies without the previous agreement of governments claiming to own the wreck. Odyssey, the most prominent, has since reached agreement with the UK on the exploration of several wrecks. They have also diversified their activities to include exploring for potential seabed mining locations. All this seems to point to a decline in uncontrolled exploitation of archaeological artefacts and treasures, although the capability of divers to reach depths of 50 metres or more is a major cause for concern. Relevant figures are, however, unavailable.
Tsunamis and storm surges	Since tsunamis are intrinsically unpredictable, they are of no help in forecasting, beyond showing where the tsunami prone areas are situated.
Damage to underwater pipelines and communications cables	Whether for reasons of security or otherwise, it is extremely difficult to obtain reliable accurate data for submarine cables and underwater pipeline. The submarine cable map[9] offers some insight into the different cable densities. See also this link[10] which provides indication of their vulnerability. Of the nine sea basins considered here, the Celtic Sea, the Mediterranean and the High Seas have complex networks of cables part of a global network with considerable autonomy. Disruptions to internet connectivity can result from damage to cables by human or natural activities. The submarine cable map illustrates that similar chokepoints exist as for marine traffic with very similar risks and threats. There are no global maps available for underwater pipelines, but they are subject to similar risks but with much more serious results: damage may have an impact on

[9] http://submarine-cable-map-2013.telegeography.com/

[10] http://www.wired.co.uk/news/archive/2013-04/3/vulnerable-undersea-cables

marine resources with a local and a regional reach. The links[11] suggest how risks might be minimised by software and technical means. Pipeline protection is a big but discreet business and so facts and figures are not readily available.

Collisions, groundings, wrecks, cargo fires or explosions

The numbers of these events are likewise very difficult to assess. One important criterion is to measure the intensity of maritime traffic, another is the level of qualification of the ships' crews. There are regional and global maps with current and projected numbers of ships operating in one or more of the sea basins, but very little data about the training standards globally and how to compare them. Most data are not available from open sources. One source for facts and figures could be the ship insurers such as Lloyds of London who also have considerable expertise in ports, container terminals, pipelines and oil platforms. Two major dangers are apparent, the danger to ships' crews or personnel working on maritime infrastructure, and the danger to the wider maritime environment.

Risks to biodiversity

An assessment of the risks and threats to biodiversity can only be based on very general assumptions about many different factors, the major ones are climate change, ecosystem loss or long-term damage and alteration and the invasion of alien species. For further investigation it seems appropriate to study the "Canadian Biodiversity Strategy", to follow the United Nations Convention on Biological Diversity and to pay attention to the European Commission's "Alarm" project, which means "Assessing large-scale environmental risks of biodiversity with tested methods". This study is the best available source for this very complex risk. The complicated nature of the problem and the very different solutions required, demand a broader view and the unrestricted exchange of information between all maritime actors. See the links for additional information[12].

3.4 Summary

A complex picture

One of the main observations is that the risk picture differs both between risk sources but also between basins. Different basins appear (in general) to be affected by different types of risk at varying levels (ranging from low to high). Security related factors appear to show higher diversity, while environment related ones seem more homogenous. At the same time, the same can be said about the possible impact of the risk to the EU, which however tends to be more in the medium range. When using these parameters to estimate "danger" levels, the experts seem to indicate towards a "medium to high" risk picture (with a certain level again of variation by source and basin). "Danger" generally appears more uniform than

[11] http://www.dnv.com/resources/publications/dnv_forum/2005/no_2/theworldslargestunderwaterpipelinesystemprovidingriskstatus.asp.
http://www.industrytap.com/worlds-longest-under-water-gas-pipeline-1166km-giant-serpent/339

[12] http://online.wsj.com/ad/article/execdigest-biodiversity
http://www.biodiversitybc.org/EN/main/why/110.html
https://www.ufz.de/export/data/global/30752_Spangenberg-et-al_Scenarios_GEB-2012.pdf

what is shown in the risk columns. This is explained as in many cases (certainly not always), where "risk" is high, its impact tends to be "low", and vice versa[13].

Contribution of CISE

The Delphi-based expert analysis generally agrees that the contribution of CISE to improving the risk picture is important. However, this is not uniform. This difference can be explained by a number of factors, including the existence of specific methods tools addressing the source already (for example pollution) or the need for CISE to be supplemented by other measures (for example adequate enforcement) in order to bring about the expected results.

[13] For an illustrative example, risk of war in the Skagerrak is very low, and in part because of this, its impact - if it happened - would be immense. Likewise, risk of discharges of oily bilges in the High Seas is naturally very high, but its impact is much lower than in enclosed seas, where it would be more damaging.

4 Baseline: maritime surveillance systems and cooperation

Existing sectorial information setup …

Across the EU, national administrations have been developing their own maritime surveillance systems, data collection procedures, and statistical and analytical tools for a long time. With maritime surveillance being represented by some 400 authorities throughout the EU, this has resulted in a sectorial information setup. With the relevant European agencies developing sectorial surveillance capacities based on centralisation of information owned by the relevant sectorial administrations, much information is available but mostly used within their respective user communities (see FEI, 2012).

… hence information sharing is no "greenfield"

The aim for CISE is particularly to enhance the sharing of information across borders and across user communities. This is a widely recognised need. Despite the sectorial approach to data collection and analysis, many efforts have also been taken to facilitate and stimulate better information sharing; both at national and EU levels, as well as regionally. Hence, the sharing of information across user communities, as well as across borders is no "greenfield", and a significant and evolving information sharing infrastructure is already in place on which the CISE can be built.

Across-user community information exchange mostly nationally

Nationally, many Member States are beginning to focus on integrating information sharing across user communities, and some have already established national coordination centres and information sharing environments. Others are in the process, or plan to do so.

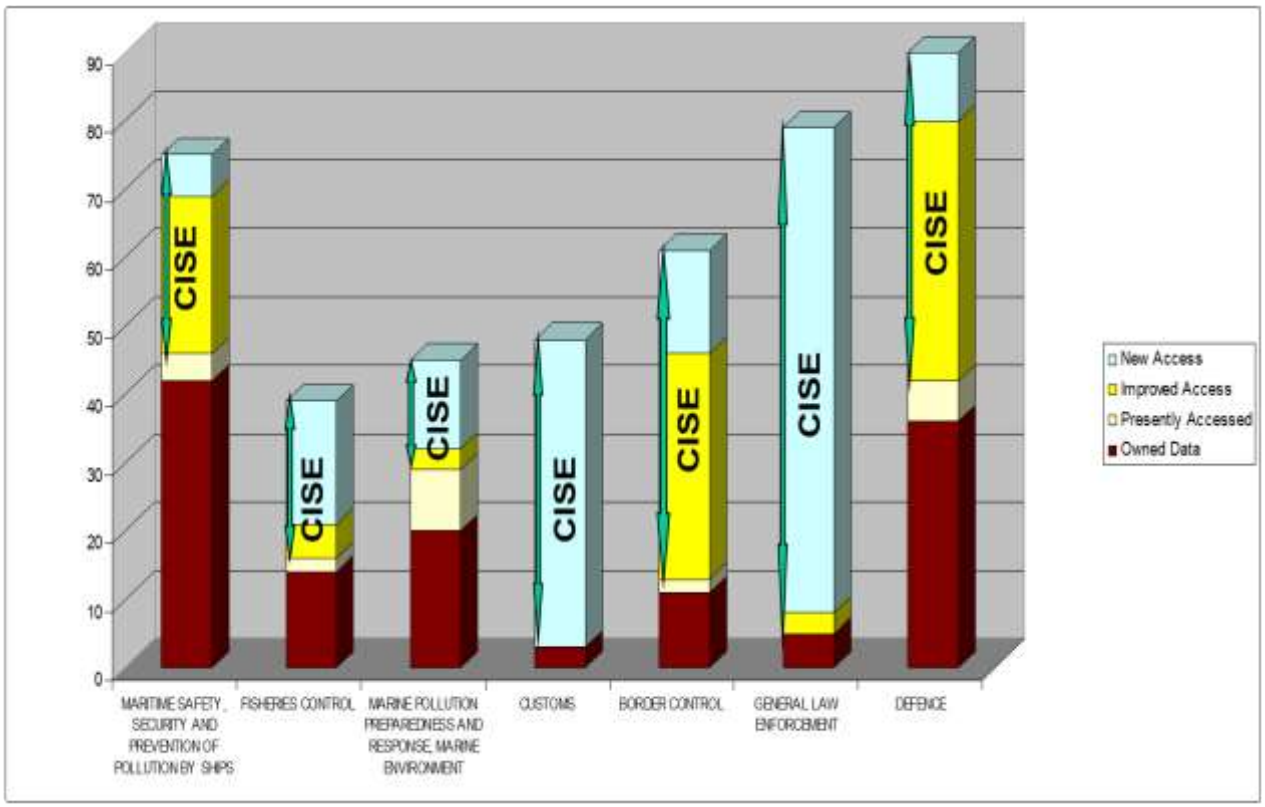
Cross-border information sharing mostly within user communities

At the EU level, several EU systems and platforms for information sharing have been put in place, and many are highly functional and successful. These systems focus primarily on enabling information exchange within single user communities; however, some have started to look at the opportunity for including other user communities.

The following sections provide an overview of the status of and expected future developments in maritime surveillance systems and cooperation initiatives. Highlights are drawn from national, regional and EU initiatives; i.e. with a particular emphasis put on the main information exchange systems and environments that are already in operation, or under development.

However, before turning to the current status as well as development trends in maritime surveillance systems and cooperation initiatives, it is worth briefly emphasising the current data context as it exists in the seven user communities. Such an overview can be obtained by the gap assessment study undertaken by JRC on the basis of inputs from mainly the Technical Advisory Group (TAG). Here, it was found that there is a gap of between 40% and 90% between the supply and the demand for additional data exchange across the various user communities depending on the area, that 45% of the currently collected information is collected by more than one user community, and that about 80% of the existing information is in national ownership. Moreover, almost half of the information that is gathered today is owned by two sectors, namely Defence and Maritime safety, security and prevention of pollution by ships. Finally, it should be emphasised that not all data are exchanged on a regular basis.

Figure 4-1 Overview of data gap assessment



Source: Presentation by JRC (F. Oliveri) to MSEsG.

4.1 Status and developments at national level

This section provides a description of the current situation concerning the extent to which the seven user communities are sharing information and the limitations that are experienced in this regard. The description builds upon results from the questionnaires that were sent out to the Member State Expert sub-Group (MSEsG) members and the workshops/interviews carried out with CISE stakeholders. The information gathered from the workshops/interviews is furthermore used to describe the observations made as regards trends in national maritime surveillance.

As mentioned above, the survey included several questions of relevance for depicting the status and development of maritime surveillance at Member State level. Of particular interest in this connection are the questions related to the *existence of current IT surveillance systems*, including the number of user communities that the systems cover. Likewise, the survey asked Member States about their *experienced limitations to information exchange between sectors and across national borders*. The following provides a summary of the results.

4.2 Maritime surveillance systems and information sharing

4.2.1 Existence and coverage of current national IT surveillance systems

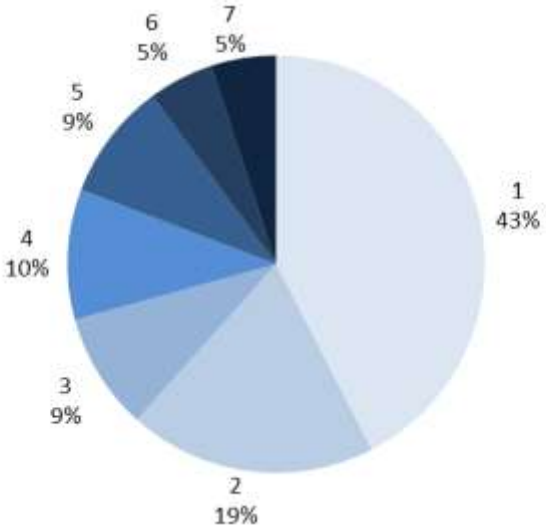
The number of IT systems differs across Member States

Across the 13 Member States who responded to questions on existing IT surveillance systems, a total of 99 national systems were highlighted. On average, each of the responding Member States has thus listed close to eight systems. Looking at the IT systems that cover more than one user community, the average is about four systems. However, there appears to be large variations in the number of listed IT systems across Member States, i.e. with some countries only having very few systems in place while others have many systems. It should nevertheless be kept in mind that not all respondents have listed all their systems and the results should therefore only be seen as indicative.

More than half the IT systems cover more than one user community

Of the 99 national IT systems a total of 42 cover only one single user community whereas the remaining 57 covered more than one. Only 5% of the national IT systems cover all seven user communities. Indeed, on average every IT system registered by the Member States currently covers 2.6 user communities. The distribution of national IT systems in terms of how many user communities they cover is depicted in the below figure.

Figure 4-2 Distribution of national IT systems across the number of covered user communities (1 to 7)

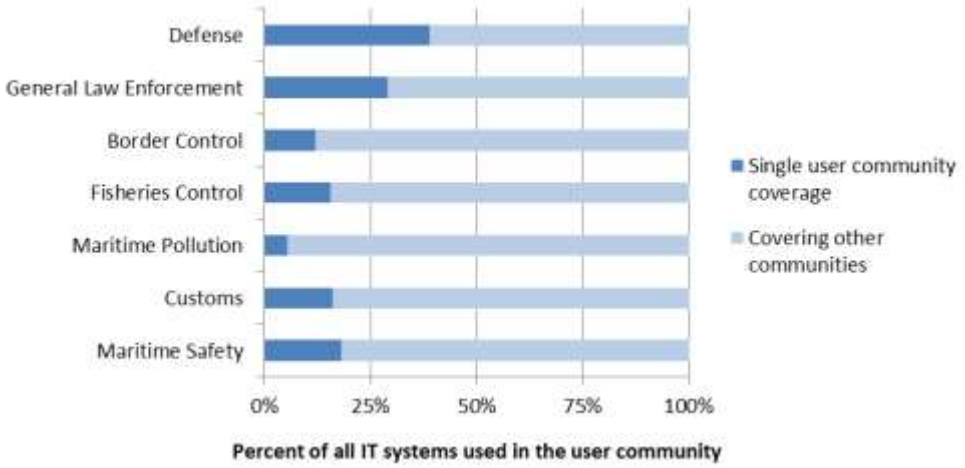


Source: Based on MSEsG survey.

Single-sector systems most prevalent in Defence and General Law Enforcement

The number of IT systems that only cover a single user community (sector) differs largely between user communities. On average across the responding Member States the Defence and General Law Enforcement communities both have a quite high share of IT surveillance systems that only cover their own community. For Defence, the share of such "single user community coverage" systems is particularly high (39%). In the Maritime Pollution community, on the other hand, very few systems are specific to that community. The shares of single sector systems and those systems which cover at least one more community are depicted for each user community in the below figure.

Figure 4-3 Share of single-sector systems and multiple-sector systems used in each of the user communities



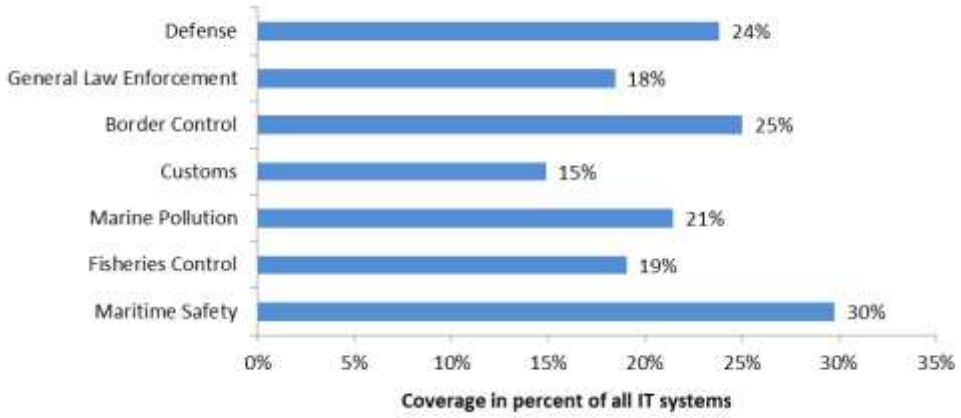
Source: Based on MSEsG survey.

Not all user communities are equally connected

Not all user communities are covered equally by the existing IT surveillance systems. For instance, Maritime Safety, Border Control and the Defence user communities are covered by most systems, while Customs, General Law Enforcement and Fisheries Control are covered the least. The degree to which the

different user communities are covered by the existing IT surveillance systems is depicted in the below figure.

Figure 4-4 User community coverage by national IT systems



Source: Based on MSEsG survey.

4.2.2 Trends in national IT maritime surveillance systems

Member States are moving towards national information sharing environments

From the interviews and workshops that we conducted in the different Member States, it became clear that there is an on-going trend of establishing national cross-sectorial information sharing environments. Some Member States have been engaged in this process for a long time while others, so far, mostly have been discussing it. Also, of those countries which have not yet initiated the process many are on the verge of doing so. In any case, there appears to be consensus that sectorial information sharing delivers benefits.

IT systems are being consolidated within user communities

The above trend also means that existing IT surveillance systems are being consolidated to an increasing extent, and that Member States therefore are moving towards a higher degree of integration of maritime surveillance information across fewer systems. In those Member States that have come farthest in this process, consolidation is now mostly happening across sectors, while other Member States are showing system consolidation mostly within sectors. Indeed, many Member States have a fairly large number of completely separate systems running. The recorded data formats as well as the systems' technical foundation can also differ widely, even within each user community, which makes integration and combination of data cumbersome.

No movement towards one single system

The implementation of national information sharing environments is nevertheless a lengthy process – particularly with respect to establishing the underlying framework, governance models and responsibility structures. The speed at which the consolidation of IT systems is happening is therefore hard to gauge. Also, the consolidation of systems does not imply that Member States are moving towards one single system. Because different authorities have different competences and, accordingly, different information needs they collect information that is very specific to these competences. For this reason separate or single-sector systems are needed; and only parts of the information within these systems will be of benefit for other user communities.

Resource constraints is driving information sharing

The underpinning driver for the above developments has primarily been increasing resource constraints and the objective of seeking efficiency gains. Lately, however, with the increase in the willingness to share information across user communities, and growing cross-sectorial cooperation, there has been a growing awareness of the potentials that information sharing could offer.

From response-oriented to predictive surveillance

For those Member States which have been engaged in information sharing for a long time many developments on how to go further are either on-going or being planned. There is also a growing awareness, for example, that the gathering of data and maritime surveillance is entering into a new era. For example, the attention is to a greater extent turning away from response-oriented surveillance and towards more anticipative or predictive surveillance; i.e. becoming better able at predicting risks and events; and allocating resources accordingly to increase response capability and successful outcomes. As worsening resource constraints will continue to force authorities to do "smarter surveillance" it is anticipated that this trend will continue.

Authorities are nevertheless only beginning to understand that they do not have a very good understanding of the drivers of the risks and threats that they face, and therefore also not of how they will be better able to anticipate them. Interest is therefore also growing in fusing/merging data, and sharing experiences and knowledge, preferably through user friendly interfaces. Likewise, there is a growing focus on "data discovery" with the identification of new possible data sources; some which already may be recorded but are not shared, as well as those that are not yet recorded in usable formats for easy sharing and usage.

4.2.3 Limitations to information exchange

Current limitations to information exchange

Despite current developments as regards increasing the information exchange across user communities and between Member States, the user communities can experience limitations to the exchange of information with other user communities. Such limitations can take several forms, and they may be experienced in connection with information exchange both within and between Member States. In the MSEsG survey, Member States were asked to provide answers about the extent of such limitations; including the extent to which the limitations arise from (1) technical limitations; (2) cultural and/or administrative differences; and (3) legal limitations.

Differences in limitations between Member States

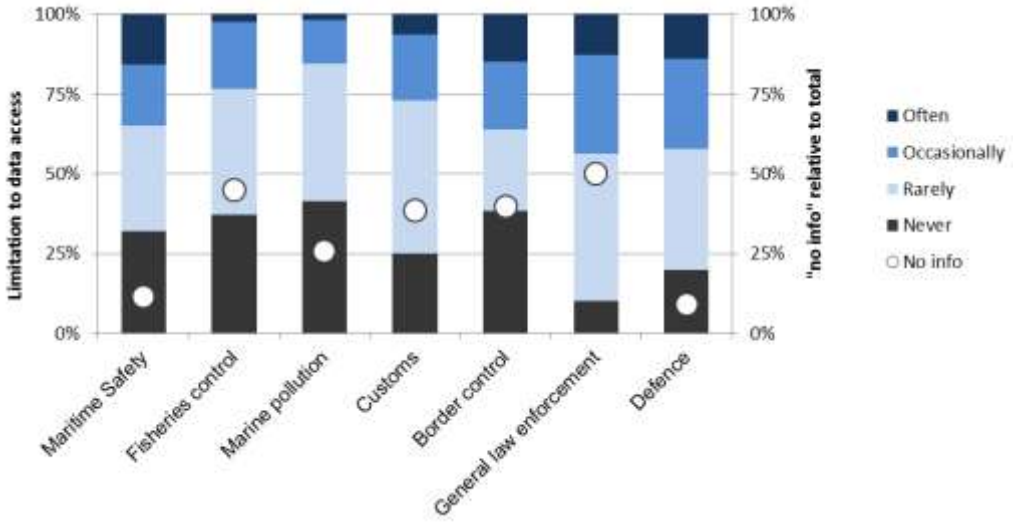
A total of 13 Member States provided answers to experienced limitations in the MSEsG survey. However, some only provided answers for certain user communities. From the answers, it nevertheless appears that there are large differences in the limitations experienced in the different Member States. For example, in some Member States certain sectors never appear to experience limitations to information access, whereas in other Member States such limitations appear to occur quite often.

Differences in limitations between user communities

There are also differences in experienced limitations across the different user communities. This picture can be seen from Figure 4-5 (below), which depicts the percentage of times that a specific user community has registered the experience of

different types of limitations when accessing information from another user community. On average, across all user communities there are about 25% cases of occasional and often experienced limitations to data access in the responding Member States. However, most cases are registered within the General Law Enforcement, Defence, Border Control and Maritime Safety user communities. Marine Pollution and Fisheries Control, on the other hand, appear to be the user communities that experience fewest limitations when accessing data.

Figure 4-5 *Percentage of times that a user community (receiver) experiences limitations to data access from other user communities within Member States*



Source: COWI, based on MSEsG survey responses.

Large uncertainties

As mentioned above, some respondents did not provide answers for all user communities and this naturally introduces uncertainty in the figure. Because the uncertainty can be assumed to correlate with the lack of received answers, the white circle depicts the percentage of answers that were missing relative to what could have been provided. For instance, 12% of the answers related to the limitations experienced by the Maritime Safety community when accessing information from other communities were missing.

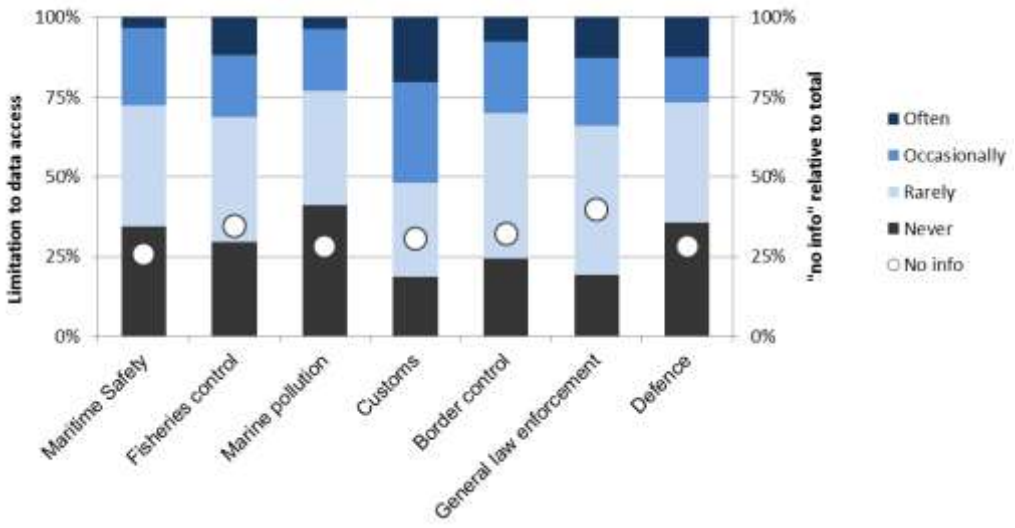
With seven user communities, each Member State could report a total of 42 experiences of limitations to information exchange (6 experiences for each of the 7 user communities). With 13 Member State responses, this totals 78 experiences for each user community. As seen from Figure 4-5, almost all respondents provided answers for the Maritime Safety and the Defence communities. For the rest of the user communities, no information was provided in 25 to 50% of the cases.

Limitations seen from the providing part

While the above figure drew a picture of how each user community experiences limitations to data access from the other user communities, a similar picture can be drawn in terms of how the other user communities on average experience data access limitations from a single other community. In some sense, this can serve to illustrate how the other communities experience limitations in terms of data *provision* from a particular user community. Figure 4-6 provides such a picture. From here it can be seen that only few communities experience limitations to obtaining access from the Maritime Safety and Marine Pollution communities

while data access from General Law Enforcement, Defence, and particularly Customs are experienced as more restrictive and limited. One should however keep in mind that the same caveat mentioned above also applies here.

Figure 4-6 *Percentage of times that other communities experience limitations to data access from a particular community (provider) within Member States*



Source: COWI, based on MSEsG survey responses.

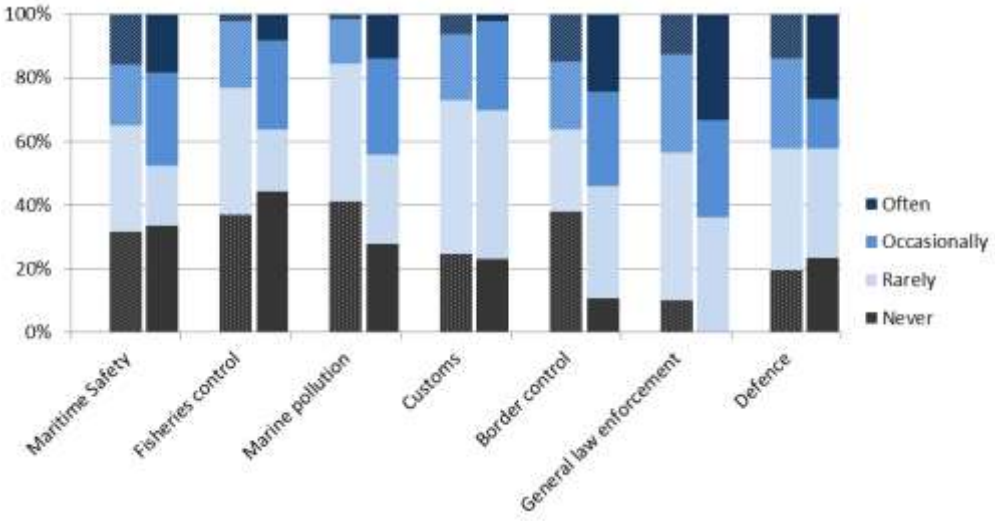
While there are uncertainties about the results it is interesting to note that there are asymmetric experiences to data access limitations across the user communities.

Limitations to data access is larger across Member States

It has already been established, i.e. from the BluemassMed and MARSUNO pilot projects, that the limitations to information exchange across user communities are larger between Member States than within national contexts. This is also the result of the MSEsG survey. For example, in addition to providing answers to cross-sectorial limitations to data access within Member States, respondents also provided answers to such limitations between Member States. From this, similar pictures to the above figures have been drawn.

Figure 4-7 provides a picture of the user communities' experience of cross-sectorial data access limitations between Member States. To better see the difference to the limitations experienced *within* Member States, the figure has been combined with Figure 4-5 above (as slightly dotted bars). The most apparent difference are those seen for General Law Enforcement, Border Control, and Marine Pollution which all appear to experience much larger limitations across borders than they do within national contexts. Customs, on the other than, appear more or less the same where there are only smaller differences in the Defence and Maritime Safety communities. Generally, however, the limitations to cross-sectorial data access are larger across borders than they are within Member States.

Figure 4-7 Percentage of times that a user community (receiver) experience limitations to data access from other user communities across Member States



Source: COWI, based on MSEsG survey.
Note: The slightly dotted bars denote cross-sectorial limitations to data access within Member States, while full colours depict between Member States.

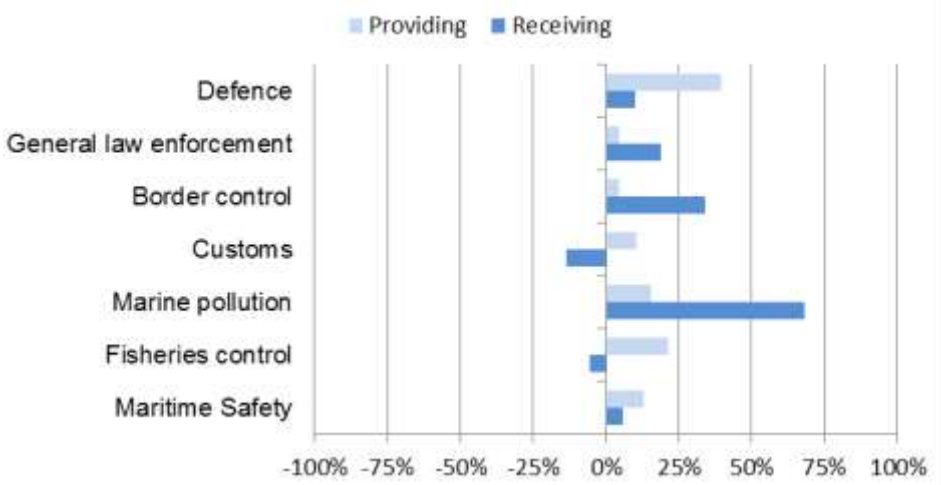
As above, there are large uncertainties with the depicted limitations to data access across countries. Likewise, this can be indicated by depicting the share of information that is missing from the survey. This has nonetheless been left out of the figure as the missing information on limitations across borders more or less corresponds to the missing information on limitations within Member States. It should nevertheless be noted that the uncertainty about cross-sectorial limitations to data access is higher when looking at experiences that go between Member States compared to those that are made within national contexts.

From the above, other sectors appear to be feeling the greatest limitations in terms of provision of data access from General law enforcement, Border control and Defence.

The experienced limitations are generally larger when looking at data exchange between Member States. In terms of receiving data, this is especially the case for Marine pollution, Border control and General law enforcement[14]. When looking at data provision, it is notably Defence where restrictions to data access across borders are felt the most.

[14] The fact that both customs and fisheries control show less limitations to data access across borders should be interpreted carefully due to little information and different interpretations of Member States when filling out the questionnaire.

Figure 4-8 Difference in experienced limitations when receiving and providing data access (between relative to within Member States).

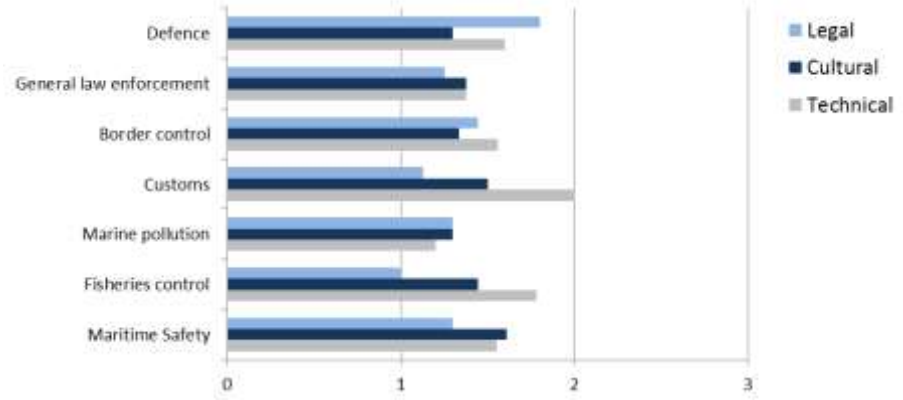


Source: MSEsG survey.

Types of limitations

In terms of the types and significance of limitations to data sharing with respect to the different sectors with Member States, the following picture emerges.

Figure 4-9 Types and significance of data sharing within Member States

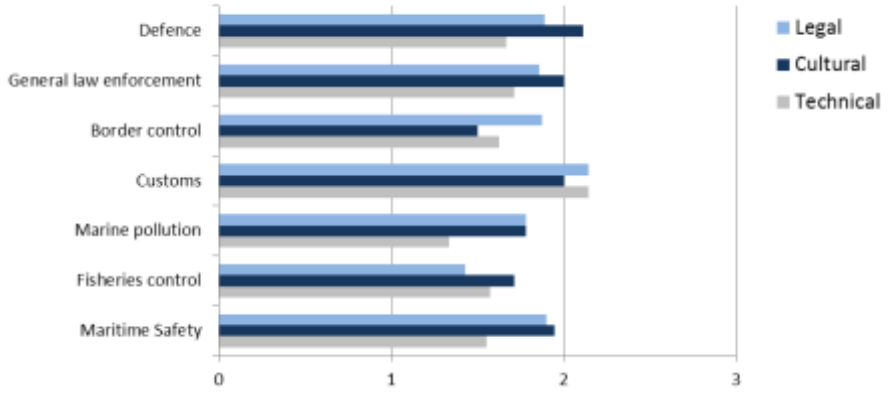


Source: MSEsG survey.
Note: 0: no limitation; 1: minor effect; 2: moderate effect; 3: significant effect

It can be seen that there are differences in the significance that legal, cultural and technical limitations play across the sectors. For Customs, for example, the technical limitations to data sharing appear quite prevalent, which is also the case in several other user communities, whereas legal limitations are more prevalent in the Defence community.

This picture is different when looking at limitations to data sharing across borders. For instance, the relative significance of technical limitations is far smaller than within Member States; thus giving more significance to legal and cultural limitations.

Figure 4-10 Types and significance of data sharing between Member States



Source: MSEsG survey.
Note: 0: no limitation; 1: minor effect; 2: moderate effect; 3: significant effect

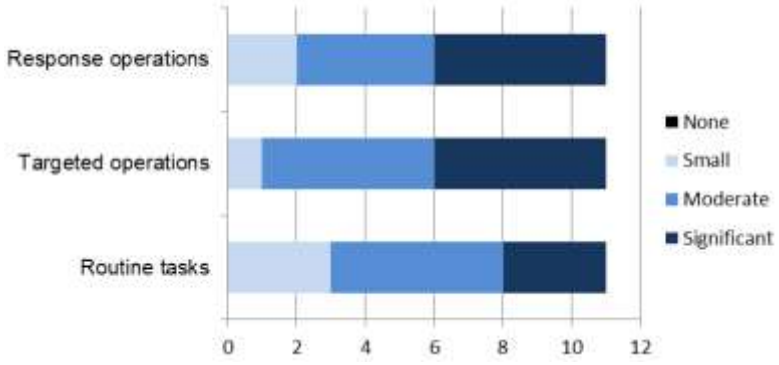
Benefits from better information sharing

Member States were also asked to provide answers to how they see the potential benefits from better information sharing across sectors and across countries, given their current information sharing setup. This part of the survey addressed both potentials regarding surveillance tasks, i.e. routine tasks, targeted operations and response operations, as well as the types of benefits that Member States would regard as most likely to be realised.

Benefits in surveillance tasks

In terms of surveillance tasks, Member States generally see moderate to significant benefits across the board, albeit with targeted operations showing the largest potential.

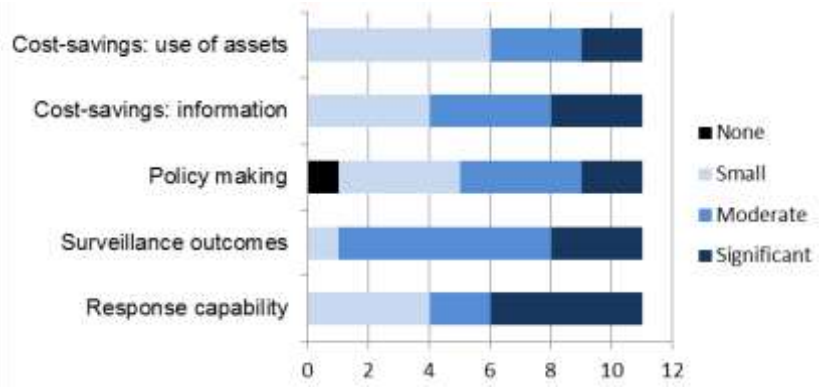
Figure 4-11 Benefits in terms of surveillance tasks (number of answers)



Source: MSEsG survey.

As regards the types of benefits that Member States see the largest potential for realising through better information sharing, surveillance outcomes appear the most consistent answer. Increasing response capacities and achieving cost-savings in terms of information gathering were nevertheless also underlined.

Figure 4-12 Potential types of benefits (number of answers)



Source: MSEsG survey

4.3 Status and developments at regional and EU level

This section highlights the current status and expected developments at regional and EU level with respect to the main information sharing systems/environments used in the seven user communities. Relevant examples include:

Table 4-1 Main EU-level maritime surveillance systems – non exhaustive list

System	Level	Host and organisation	Purpose	How it works
GMES/Copernicus	EU	Coordination and management of the programme is ensured by the European Commission	Uninterrupted provision of accurate and reliable data and information on environmental issues and security matters to users in charge of policy making, implementation and monitoring, in the EU and its Member States	Provides observation data in six Services from satellites and in-situ stations. All information provided free of charge to users
EUROSUR	EU Schengen plus Schengen associates plus Denmark Thus, not including UK and Ireland	Frontex and national coordination centres (NCC) Close cooperation with, EU satellite Centre, EFCA, EMSA	Better situational awareness and reaction capability	Exchange of non-classified, sensitive and classified information Cooperation and information exchange via situational pictures at national, European and pre-frontier area (last two managed by Frontex) Not personal data, but if so: only exchange between neighbouring countries under conditions of Data Protection Rules
SafeSeaNet	EU	EMSA and National Competent authorities Delivers information to EUROSUR under a MoU and for defence and fisheries control	Essential component of the VTM system which aims to enhance the safety and efficiency of maritime traffic; improving the response of authorities to incidents, accidents or potentially dangerous situations at sea, and contributing to a better prevention and detection	SafeSeaNet enables the receipt, storage, retrieval and exchange of information for the purpose of maritime safety, port and maritime security, marine environment protection, and the efficiency of maritime traffic and maritime transport SafeSeaNet information consists of information from ships; AIS derived information

System	Level	Host and organisation	Purpose	How it works
		purposes.	of pollution by ships.	and LRIT information. IMDatE aims to combine the information from SafeSeaNet, THETIS, (port state control) and CleanSeaNet to provide an integrated platform that would also be able to service other user communities
CECIS (Common Information and Emergency System) CIS (Common Information system: on marine pollution)	EU	DG ECHO National focal points (CECIS) National homepages (CIS)	Civil protection and marine pollution Facilitates fast and effective disaster response Facilitates asset sharing	Allows sending and receiving disaster alerts, registering requests for and offers of assistance by States and documenting all actions and information flow during an emergency. It also hosts a database on potentially available assets for assistance, including expertise.
MARSUR	EU except DK	European Defence Agency	Aims at improving the Recognised Maritime Picture (RMP)	Fully decentralised network, linking up existing military maritime networks and fostering the exchange of data, information and knowledge between all (voluntarily) participating Member States
SUCBAS (Sea Surveillance Cooperation Baltic Sea)	Regional	Steering Group with operational and technical boards	Enhances Maritime Situational Awareness benefiting maritime safety, security, environmental and law enforcement activities in the region by sharing relevant maritime data, information and knowledge between the participants	Three levels of co-operation, ranging from exchange of contact points to online automated sharing of maritime situational awareness data
SEAHORSE	Regional Mediterranean	Regionally anchored and coordination with FRONTEX, and on a national level, defence may be involved	Migration monitoring communication systems Reinforcement of cooperation and capacity of third countries to fight irregular migration	Coordinated and joint actions Capacity building Coordination and communication network
PERSEUS	Regional Related to Eurosur Focus on - crime and illegal trafficking - border control and irregular immigration	FP7 project involving 12 countries and validation demonstration projects in the Mediterranean involving EU agencies (e.g. Frontex, EMSA) and EU institutions (ENTR, HOME, MARE, INFSO)	PERSEUS demonstrates and validates recommendation for the European wide integrated maritime border control system, in line with EUROSUR objectives and across all aspects: collaborative, regulatory, technological and trans-national) (see further description below)	System of systems that links existing and upcoming national and regional control centres, supported by ground platforms, and enabled by an upgraded, easy to deploy and low-cost communication network based on secured, protected and extendable Virtual Private Network

Source: COWI, compiled through publically available sources

4.3.1 Maritime safety and security and prevention of pollution caused by ships[15]

The European Maritime Safety Agency (EMSA) is the regulatory agency of the EU in support of maritime safety, security and prevention of pollution caused by ships. The maritime applications of EMSA include[16]:

Table 4-2 Maritime applications of EMSA

Areas that systems receive, process and distribute information on:	**Maritime applications that are used and hosted by EMSA**	
Vessel Traffic Reports	**SafeSeaNet**. The EU coastal system of over 700 shore-based Automatic Identification Systems (AIS) receiving stations, which automatically track all ships navigating within 100 Nautical miles from the EU coastline, and receive and store information concerning the cargo and voyages of vessels	**EU LRIT DC**. The EU Long Range Identification and Tracking Data Centre using communication satellites to track all ships (around 10,000) under EU flags all over the world, as well as any ship, irrespective of its flag, within a maximum of 1,000 Nm from the EU coastline
Satellite monitoring	**CleanSeaNet**. The EU satellite based system for detection of oil spills and vessels at sea using Satellite Aperture Radar images	
Port State Control	**THETIS**. A web-based application providing ship inspection related information and reporting support to all European Port State Control officers.	

SafeSeaNet

The main objective of SafeSeaNet is to provide a European platform for maritime data exchange between maritime administrations of the Member States. As indicated in the above table, the system was developed to support the requirements of the VTM (Community Vessel Traffic Monitoring and Information System Directive) Directive. The system is accessible to Member State authorities and the national administrations of the EFTA States.

Following a decision of the High Level Steering Group of the SafeSeaNet from 2011, access to the SafeSeaNet database has been granted e.g. to FRONTEX and EUROPOL. Member States have also been granted European Union Naval Force (EU NAVFOR) access to Long Range Identification and Tracking (LRIT) information to support antipiracy activities.

[15] Unless otherwise stated, this section builds on the contents of the Directive 2002/59/EC as amended by Directive 2009/17/EC, Directive 2009/18/EC and Commission Directive 2011/15/EU.

[16] Source: Presentation by Justino de Sousa, EMSA on 'EMSA's integrated maritime environment – a tool for improved maritime awareness', November 2012 conferences.theiet.org/.../2012/documents/sousa-presentation.cfm

The system aims to (i) enhance the safety and efficiency of maritime traffic; (ii) improve the response of authorities to incidents, accidents or potentially dangerous situations at sea, including SAR (Search And Rescue) operations; and (iii) contribute to a better prevention and detection of pollution by ships. This is done through the provision of information regarding, e.g. the estimated or actual time of arrival and departure at ports, details of dangerous and hazardous goods on board, information on accidents and incidents (including the number of people on board), AIS vessel positions, etc.

Member States are obliged to cooperate to ensure the interconnection and interoperability of the national systems used to manage the information. Data exchange must be electronic and enable messages notified, and the system must allow information to be transmitted 24 hours a day. Member States should be able to send, upon request information on the ship and the dangerous or polluting goods on board to the national and local competent authorities of another Member State without delay.

THETIS

THETIS is the information system that supports the new Port State Control Inspection Regime (NIR). It implements the regime laid down in the Directive 2009/16/EC on Port State Control and its implementing acts (Directive 99/35/EC on ro-ro ferries and high-speed passenger crafts, Directive 2009/17/EC on vessel traffic monitoring (VTM Directive), Directive 2009/15/EC on recognised organisations and Directive 2009/20/EC on insurance for maritime claims and Regulation 2009/392/EC on liability for the carriage of passengers.

The system is linked to the SafeSeaNet system (SafeSeaNet-THETIS interface), and it indicates which of the ships expected at EU MS ports has priority for inspection and allows recording the results of such inspection. The reports are made available to all port state control authorities in the Community and the Paris MOU (The Paris Memorandum of Understanding on Port State Control). Furthermore, THETIS interfaces with a number of maritime safety databases (EU-recognised classification societies, Community and national information systems and other port state control regimes). Inspection results are also available through a public website.[17]

National Single Window – Directive on Reporting formalities

Directive 2010/65/EU on reporting formalities aims at simplifying the reporting formalities by implementing National Single Window systems (NSW). The electronic NSW systems should be implemented before 1 June 2015.

The data to be collected by the NSW can be divided into three categories: (i) information received pursuant to EU legislation (arrival and departure notifications, Hazmat (hazardous material) notifications, waste notifications, ISPS (International Ship and Port Facility Security Code) notifications); (ii) information stemming from IMO (International Maritime Organization)/FAL (Facilitation of International

[17] https://portal.emsa.europa.eu/web/thetis/inspections.

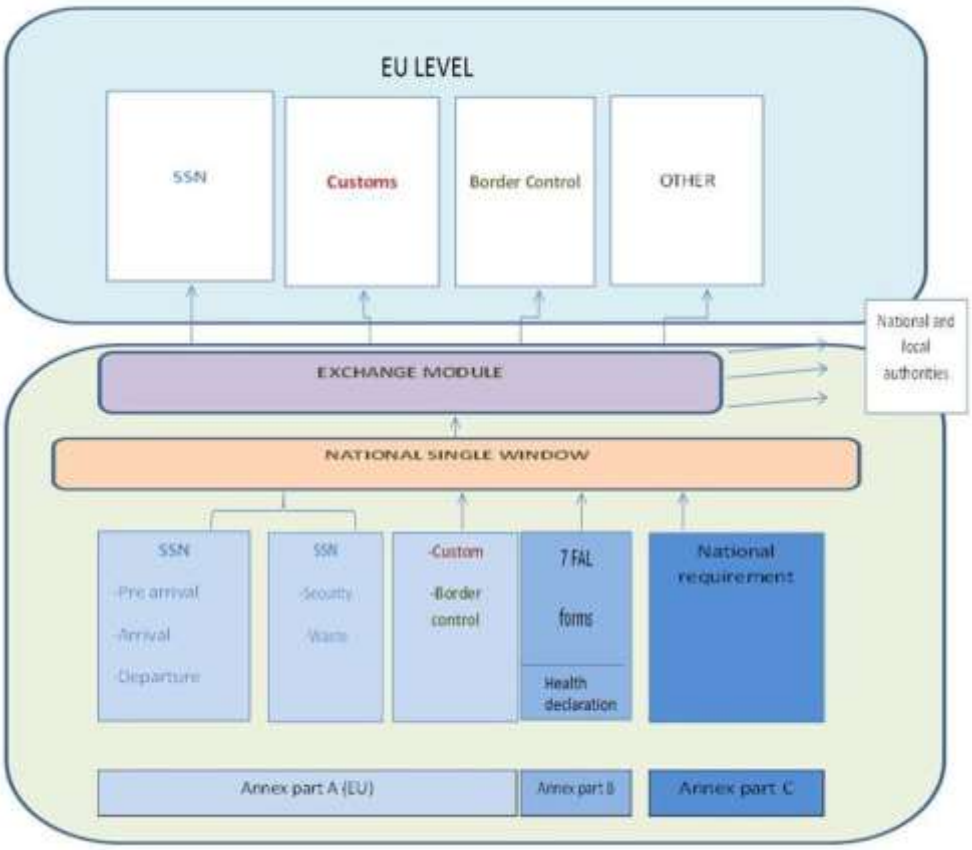
Maritime Traffic) Convention; and (iii) information stemming from national requirements.[18]

EMSA will launch a pilot project, which seeks to help Member States share reporting formalities information via a single window. This includes the development of certain software service components to simulate a National Single Window. This will allow testing different national single window solutions and interfaces to help Member States implement the Reporting Formalities Directive and aid them in the distribution of data to national authorities and in the sharing of information via SafeSeaNet's central system.[19] Some of the key features of the Single Window are summarized below[20]:

All information should be reported only once through a Single Window that links SafeSeaNet, e-Customs and other electronic systems and should be available to relevant authorities of the Member States, such as customs and border control. As such, the scope of the National Single Window is broader and extends beyond the maritime safety and security and prevention of pollution caused by ships user community. The NSW must also be interoperable, accessible and compatible with SafeSeaNet. In addition, Member States should ensure that the information received is available in their SafeSeaNet system and that relevant parts of information are available to other Member States via SafeSeaNet. The below figure provides a graphic illustration of the vision of the Single Window[21]:

[18] Annex to the Directive 2010/65/EU.
[19] EMSA Newsletter No. 98, May 2013.
[20] The EU eMaritime initiative, Single Window, with a view to the near future, Logius Workshop, 10 November 2010 – Rotterdam, EC - DG MOVE (Maritime transport policy: Ports & Inland waterways)
[21] Presentation by Finnish Transport Agency, 23 May 2013, http://itemsk.blob.core.windows.net/cmsroot/www_transrussia/files/5e/5e9e8ec5-db89-481c-bb55-51cc14f9bf49.pdf

Figure 4-13 National Single Window overview



The European Union Long Range Identification and Tracking Data Centre (EU LRIT)

The requirements concerning LRIT stem from Chapter V, Regulation 19-1 of the SOLAS (Safety of Life at Sea) Convention. Paragraph 8-1 of the Regulation 19-1 provides that the Contracting States' governments should be able to receive LRIT data about ships for security and other purposes. Such other purposes cover, e.g. search and rescue, maritime safety in general and maritime environment purposes.

IMDatE

The Integrated Maritime Data Environment (IMDatE)[22] is a technical framework that collects and combines data from EMSA's maritime applications (SafeSeaNet, CleanSeaNet, Thetis and LRIT) and other external sources (e.g. VMS) to provide more comprehensive and configurable services. It also supports the relay of data between the maritime applications themselves, based on existing access rights. A pilot phase of the project ran from March until October 2013. Six Member States are participating in the pilot project (France, Italy, Netherlands, Portugal, Spain and the United Kingdom). Additionally, IMDatE provides services to the European

[22] The revised Regulation (EC) No 1406/2002 establishing a European Maritime Safety Agency requires EMSA to provide operational assistance to Member States and the Commission (Art. 2). This includes e.g. implementing policies and projects in the area of the 'European Maritime Transport Space without Barriers' (the Blue Belt Project, Motorways of the Sea) by exploring additional functionalities to the SafeSeaNet.

Fisheries Control Agency (EFCA) and to EUNAVOR (for anti-piracy activities off the coast of Somalia).

IMDatE envisages that users who combine functions, for example vessel traffic monitoring and marine pollution control having the necessary access rights, will benefit from being able to obtain an integrated overview of maritime activity in their area of interest. Such data should be delivered via a web interface or distributed automatically to authorised external systems in accordance with the access rights. The results of the project will be discussed with the Member States at the next IMDatE User Consultation meeting in November 2013.

4.3.2 Fisheries control

Fisheries control at the EU level is administered by EFCA. EFCA's role is to encourage better coordination, closer collaboration and the exchange of best practice; joining forces from the different Member States and the Commission.

VMS – Vessel Monitoring System

The VMS system is used to assist the coordination of all Joint Development Plans (JDPs), i.e. Cod in Baltic, Cod in North Sea, Small Pelagic in Western Waters, the Northwest Atlantic Fisheries Organisation (NAFO), the North East Atlantic Fisheries Commission (NEAFC) and Bluefin tuna in the Mediterranean Sea. EFCA receives VMS positions from all Member States that participate in the JDPs, as well as regional fisheries management organisations (RFMOs) for non-EU countries. EFCA has been working on enhancing the system and to reinforce user access rights and security in the data exchange[23].

ERS – Electronic Reporting System

The ERS system supports the exchange of data such as electronic fishing logbooks, landing declarations, and sales notes, between inspection authorities that are involved JDP operations[24]. The facilitating application was developed during 2012 and was operational for real time data exchange between Member States by the end of 2012. Today, the system allows EFCA to receive and parse ERS messages, and to exchange them with stakeholders involved in JDP operations. Data quality, integrity and reliability are ensured through a number of validation operations. Users are also provided with a set of web-powered tools to view, search, analyse and produce statistics and reports based on specific criteria[25].

EIR – Electronic Inspection Report

Following the results of a recent study by MRAG and LAMANS[26] that looks into the Member States' national information systems for supporting fisheries management and controls, the Member States and EFCA have identified a potential area of cooperation, namely, the joint development and exchange of Electronic Inspection Reports. On this basis, EFCA organised two workshops with the aim to establish a common understanding by all Member States of all items that need to be

[23] *EFCA (2012; 2013) Annual Report, for 2011 and 2012*
[24] *EFCA (2012; 2013) Annual Report, for 2011 and 2012*
[25] *EFCA (2012) Annual Report for 2011*
[26] LAMANS (2011) Study on information systems supporting fisheries control in the European Union, CFCA/2010/B/02.

registered and in order to create a common exchange format to facilitate the exchange of this type information. The outcome of these two workshops was a working document containing a common definition for each item and a reference to existing elements in the ERS definition.

FishNet

The aim of FishNet will be to provide a virtual coordination platform providing JDP stakeholders with collaboration tools (e.g. sharing data and documents, exchange information, teleconferencing) to support decision making, planning, operational coordination, and assessment of joint control operations, and to promote remote collaboration to support these coordination activities.[27] The aim is that the platform will provide users the necessary tools to enable JDP campaign coordination tasks—as if they worked in a virtual coordination centre.

4.3.3 Marine pollution

CleanSeaNet

CleanSeaNet is a satellite-based oil spill monitoring and vessel detection service operated by EMSA. It provides aggregated data on possible oil spill, pollution alerts and related information. The vessel traffic information is available on CleanSeaNet and this allows detecting and identifying vessels that are discharging. The core of the CleanSeaNet structure is the CleanSeaNet Data Centre, which receives, manages and distributes the CleanSeaNet information.

EMODnet

The European Marine Observation and Data Network (EMODnet) will be a network of existing and developing European observation systems, linked by a data management structure covering all European coastal waters, shelf seas and surrounding ocean basins, accessible to everyone. EMODnet aims to provide the link between observations in different European waters and European environmental information, which can then be assessed by scientists and the general public. This will create a large number of marine services in the field of monitoring, forecasting and marine safety. It will provide an end-to-end system linking the modules “Sensors & Platforms”, “Surveys”, “Communication Systems”, “Data Management” and “Information Tools”.

Currently, a prototype of EMODnet is operating as “ur-EMODnet”. A decision on EMODnet will be taken in 2013, once evidence has been accumulated through ur-EMODnet. Preparatory actions for the establishment of EMODnet started in May 2009. The prototype ur-EMODnet was set up to identify gaps and to receive feedback on experiences. Lessons learned in operating and using the ur-EMODnet will be taken into account in setting up the subsequent operational EMODnet.

CECIS

CECIS (Common Emergency Communication and Information System) is a tool managed by the Commission that enables real time communication in a secure and reliable way between the Monitoring and Information Centre (MIC) in the Commission, contact points of the Participating States in the EU Civil Protection Mechanism (28 EU Member States and EEA countries) and EMSA. Participating

[27] EFCA (2012, 2013) Annual report of the EFCA, for 2011 and 2012

States may opt to appoint different contacts for civil protection and marine pollution. CECIS allows sending and receiving disaster alerts, registering requests for and offers of assistance by States and documenting all actions and information flow during an emergency. It also hosts a database on potentially available assets for assistance, including expertise. CECIS addresses major emergencies, i.e. natural, technological, radiological or environmental accidents occurring inside or outside the EU, including accidental or deliberate marine pollution.

SEIS

SEIS (Shared Environmental Information System) provides decision-makers at all levels (local to European) with real-time environmental data, thus allowing them to make immediate and life-saving decisions. It aims to improve collaboration between organisations and facilitating interaction with civil society at large. It implements the INSPIRE (Infrastructure for Spatial Information in the European Community) principles and contributes to formation of marine component in Water Information System for Europe (WISE).

4.3.4 Customs

CRMS and AFIS

TAXUD is the directorate-general of the Commission for support managing, defending and developing the customs union as a part of protecting the external borders of the EU. Moreover, the European anti-fraud Office's (OLAF) conducts external administrative investigations for the purpose of strengthening the fights against fraud, corruption and any other illegal activity adversely affecting the EU's financial interests, as well as any other activity by operators in breach of Community provisions.

The main ways for customs to exchange information is through CRMS (Customs Risk Management System) regarding the dealing with routine control concerns and the AFIS (Anti-Fraud Information System), managed by OLAF, that provides a user-friendly interface for data exchange.

e-Customs

The e-customs initiative was started with the aim to replace paper format customs procedures with electronic ones in order to creating a more efficient and modern customs environment. The initiative comprises several systems that are currently being developed and deployed; expected to be fully operational in 2020.[28]

e-Customs is a secure, integrated, interoperable, and accessible customs computerised system that facilitates import/export procedures, coordination control of goods, improvement in clearance times, and that enables seamless data flow between export/import countries and customs authorities. The system consists of several modules, namely: Import Control System (ICS), Export Control System (ECS), New Computerized Transit System (NCTS), Electronic Operator System (EOS).

[28] EC (2012) Electronic Customs Multi-Annual Strategic Plan: 2012 Revision

The e-Customs system will be designed and implemented using a service-oriented architecture, which favours the emergence of flexible, modular, easy to change, IT systems that benefit from the reuse of existing functionality in another Member State or in the Commission[29]. By enabling this architecture, e-Customs will provide an interoperable infrastructure that offers authorities to access services independently of their location, and which is also backwards compatible with existing customs systems.[30]

The Blue Belt Policy

Initially, the Blue Belt Pilot Project (BBPP) was set up to explore new ways to promote and facilitate short sea shipping in the EU by reducing the administrative burden for intra-Community trade by providing the customs authorities with the data regarding the vessels, which move directly between EU ports. The operational phase of the project was launched in May 2011 and was concluded in November 2011.

The project aimed, on the one hand, at allowing faster processing of goods through Customs when arriving at a port and, on the other hand, at providing the EU customs authorities with verified, reliable information on the current and past voyages of specified vessels in order to carry out risk assessments and to prioritise customs controls.

The notification report included information about the vessel, its recent ports of call and the last voyage detail and a screen shop indicating the Blue Belt ship track toward the destination port, plotted on a nautical chart. Later in the project, additional features were introduced. These included the integration of satellite AIS position data and information on vessel behaviour (e.g. encounter at sea, failure to report, etc.)

The findings of the evaluation concluded that the project has successfully demonstrated that the information delivered through the Blue Belt service to the customs authorities can provide them with useful information about a ship's current and past voyages and help create reassurances that goods remain under constant customs supervision.[31]

In October 2012, Blue Belt was identified as a key action in the Commission's Communication "Single Market Act II, Together for the new growth".[32] The new Blue Belt policy consists of a package of both legislative and non-legislative initiatives to reduce the administrative burden for intra-EU maritime transport. These measures include an enhancement of the Regular Shipping Service scheme and a facilitation mechanism for vessels that call also in third-country ports. The implementation of the Blue Belt concept will be supported by the planned revision

[29] EC (2012) Electronic Customs Multi-Annual Strategic Plan: 2012 Revision
[30] EC (2012) Electronic Customs Multi-Annual Strategic Plan: 2012 Revision
[31] Blue Belt Service Pilot Project Evaluation report, 4 May 2012
[32] COM(2012) 573 final.

of the Directive 2002/59/EC on Vessel Traffic Monitoring and the implementation of the Reporting Formalities Directive.[33]

4.3.5 Border control

FRONTEX is the European Agency for the management of Operational Cooperation at the External Borders of the Member States. The main system of maritime border control interest is the European Border Surveillance System (EUROSUR).

EUROSUR[34]

The objective of EUROSUR is to improve surveillance effectiveness concerning irregular migration, cross-border crime and the saving of lives of migrants at external land and maritime borders. As such, the system applies to the surveillance of both land and sea external borders of the Member States. It includes measures for monitoring, detection, identification, tracking, prevention and interception of illegal border crossing; with the aim to provide national authorities and FRONTEX with infrastructure and tools to improve situational awareness and reaction capability.

FRONTEX and associated National Coordination Centres (NCC) form the backbone of EUROSUR. Communication between those actors takes place through the communication network, which allows for the exchange of both non-classified as well as classified information. Situational pictures are an essential outcome and means of coordination. Such situational pictures are established at national, European and pre-frontier level.

The initial design of EUROSUR was approved by the six participating Member States. The first node was subsequently created and replicated in the six Member States. After that, 12 additional nodes were created (+ 1 FRONTEX NODE). As of 19 December 2011, real data were exchanged. The system does not have any central database, and there is no central communication component. Only non-classified and non-personal data are exchanged, but this will change when the new legislation is adopted.

The NCCs coordinate and exchange information between all relevant authorities: nationally; vis-à-vis other NCCs; and the Agency. The NCC is the single point of contact and should guarantee the availability, confidentiality and integrity of the information to be exchanged at national and European level. The same applies at the European level of information exchange to FRONTEX.

EUROSUR builds upon the Schengen acquis, and hence UK is not bound by it, whereas it involves Iceland, Norway, Switzerland and Liechtenstein. The implementation is staged in two phases: By 1 October 2013, it applies to all

[33] Communication from the Commission COM(2013) 510 final.
[34] This section is based on information derived from Proposal for a Regulation (COM 2011 873 final, 2011/0427(COD)) and Accompanying Impact Assessment. A EUROSUR handbook has been prepared (in alignment with Article 19) but it is not publicly available.

Member States located at the southern sea and eastern land external borders, and by 1 October 2014 to all remaining Member States with external borders. In that regard, it is worth mentioning that an assessment of the external borders made by FRONTEX in October 2009 as part of the preparatory steps of EUROSUR pointed to a number of maritime borders as being ones that would benefit from setting up permanent surveillance systems in certain areas. These are Greece (maritime borders in Aegean and Mediterranean Sea), Italy (islands of Sicily, Sardinia and Pelagic Islands (Lampedusa, Linosa and Lampione), Spain (coast between Alicante and Cadiz, Canary Islands), Malta, Black Sea Coasts of Romania and Bulgaria.

In terms of future developments, there is close coordination by FRONTEX with Europol, the Maritime Analysis and Operations Centre (MAOC-N), and the Mediterranean area anti-drug enforcement coordination centre (CeCLAD-M) to exchange information on cross-border crime; and with the European Satellite Centre, EFCA and EMSA when providing the common application of surveillance tools. Such coordination aims to ensure that the best possible use is made of existing information and systems in other EU agencies. It is moreover envisaged that maritime traffic data will be provided by SafeSeaNet, which will then make such information available for purposes other than those related to maritime safety and security and marine environment protection[35]. On 17 May 2013, the three-year 'Interagency agreement to enhance situational awareness at Europe's maritime borders' entered into force.

Within the framework of EUROSUR, which is not only a technical platform, but also cooperation between NCC and Member States and with an R&D aspect, there is a cooperation agreement with EMSA. The agreement facilitates information exchange in the maritime domain. FRONTEX is interested in the commercial shipping picture (satellite based AIS, LRIT and VMS) and FRONTEX is now starting the cooperation envisaging gradual implementation. FRONTEX also provides information to EMSA. For example, when in the context of joint operations there are sightings of oil pollution, this information is shared with EMSA.

4.3.6 General law enforcement[36]

Europol is the European Union's law enforcement agency whose main goal is to help achieve a safer Europe to the benefit of all EU citizens. Europol supports EU law enforcement authorities in gathering, analysing and disseminating information and coordinating operations. Security threats monitored by Europol include terrorism, international drug trafficking and money laundering, organised fraud, counterfeiting of the Euro currency and people smuggling; and systems for information exchange include SIENA and Europol Information Systems (EIS).

SIENA

Europol has established the Secure Information Exchange Network Application (SIENA) to support the Law Enforcement Community, as an extension of their

[35] According to Explanatory Memorandum

[36] This section relies on Europol webpage and various reports of the agency

previous information system Info-Ex. SIENA enables secure communication and exchange of operational and strategic crime-related information and intelligence between Europol, Member States and third parties that have cooperation agreements with Europol. In addition, other designated/authorized law enforcement authorities in the EU Member States may also be connected to run queries.

Information deposited in this application by relevant law enforcement authorities is made available to other EU investigators and is automatically compared with information deposited by other Member States. The purpose of this is to look for matches with a view to enhancing intelligence and providing new leads for further investigation.

Since SIENA was put into effect in 2009, information exchange has improved. SIENA has been rolled out to Australia, Norway, Croatia and Iceland with an operational agreement. In addition, regional platforms in West Africa (Accra, Ghana and Dakar, Senegal) as well as the European Union Rule of Law Mission in Kosovo (EULEX) currently have SIENA remote access facilities. Albania, Bosnia and Herzegovina, Montenegro, Serbia, Turkey and Switzerland were signed up for access in 2012. In 2012, 29% of new cases of data exchanged related to drugs, followed by fraud and swindling (15%), robbery (11%), money laundering (9%) and illegal immigration (8%). By the end of the year, 373 competent authorities were configured in SIENA.

Moreover, Europol and FRONTEX have entered into agreement to enhance their cooperation, in particular through the exchange of strategic and technical information. The aim of this cooperation agreement is to avoid the duplication of activities and efforts[37]. Work on the next release, SIENA 2.1, is on-going.

Europol Information Systems (EIS)

The EIS is Europol's reference system for offences, involved individuals and related data. It is used by the Agency, the Member States, and Europol partners in their work to stop criminal activities, including organised crime, terrorism, and other forms of serious crimes.[38]

Over the years, the quality of the EIS has improved through a number of developments; i.e. involving a change in how data are transmitted to the system by Member States, which allows for cross-matching various types of data entities, as well as through a growing interest by national law enforcement authorities in sharing and comparing their data with the EIS.

In an effort to combat more effectively cross-border crime, actions are also being taken to increase the volume of data and the use of EIS by extending access to the system to all relevant law enforcement units. Also, the use of EIS in investigations is being promoted; and mechanisms for more systematic and automated usage of the system are being put in place.

---

[37] https://www.europol.europa.eu/sites/default/files/flags/Frontex.pdf

[38] https://www.europol.europa.eu/content/page/europol-information-system-eis-1850

4.3.7 Defence

The European Defence Agency (EDA) is the European Agency for defence cooperation among the EU Member States (except Denmark, which has opted out of the Common Foreign and Security Policy).[39] The main environment, or network, for exchanging defence related information and facilitate cooperation is the MARSUR network. Yet, regional environments also exist, such as SUCBAS for the Baltic regions.

MARSUR

The MARSUR (Maritime Surveillance project) network was originally developed to support maritime operations by contributing to a recognised maritime picture. The network is marked to be the cross-border information exchange network for Defence within the CISE environment.

The MARSUR network is fully decentralised, and it has been developed to be easily expanded; i.e. building on an open architecture. The network has been built to allow seamless compatibility with other sectors, and can be seen as a good example of best practice by other projects and initiatives.[40] As such, the network is deemed to be well equipped for connecting with other systems within the CISE environment. The network has also demonstrated a willingness to exchange unclassified and subsequently classified data; i.e. facilitated by paying critical attention to the legal aspects of information sharing.

Other systems

The defence community utilizes systems such as MCCIS (Maritime Command, Control and Information System), Mercury, NEC (Network Enabled Capability) and V-RMTC (Virtual Regional Maritime Traffic Centre) in its efforts to build defence capability. Many of these are for example used in support of the EU's anti-piracy efforts through the EU NAVFOR Operation Atalanta.

4.4 Cross-sectorial and cross-border pilot projects, policies and other initiatives

In addition to the information sharing platforms and systems described in the above sections, a number of pilot projects with the aim to facilitate cross-border and cross-sector sharing of information have also been undertaken. The same goes for other information sharing and collaboration initiatives. This section provides an overview of the BluemassMed and MARSUNO projects[41], their results and identification of limitations to information exchange.

4.4.1 BluemassMed

Project background

The BluemassMed pilot project was launched in early 2010 and finalised in 2012 and can in some sense be denoted as a front-runner pilot project for CISE. It

[39] http://www.eda.europa.eu

[40] EC (2011) MARSUNO Final Report, p. 30

[41] The legal aspects of the MARSUNO and the BlueMassMed pilot projects have been analysed in detail in Annex 2 of the First Interim Report.

brought together 37 agencies responsible for maritime surveillance across all the seven user communities in six Member States (Portugal, Spain, France, Italy, Greece, and Malta). The project focused specifically on enhancing the maritime surveillance effectiveness through increased information sharing, collaboration and identification of areas for better cooperation/coordination.[42]

Results

The act of bringing 37 cross-sectorial partners together; including both military and civil user communities from six Member States has been quite an achievement in itself. For instance, despite initial reservations among the user communities to engage in exchange of information, the project has demonstrated an increasing willingness for collaboration and thus built an important basis for future cooperation and information exchange.

In fact, during the project it was found that the participating authorities were very willing to open and share information; including sensitive information, with selected partners (on the basis of control and security rules).[43] It was also clear that authorities wanted to decide when information should be shared or not. On this basis, the cooperation was greatly improved - also between civilian and defence agencies - and a growing openness towards the "responsibility to share" principle was demonstrated.

Even if the BluemassMed project did not quantify the benefits of cross-sectorial and cross-border information sharing, there is agreement among the participating partners that such information sharing has the potential to better control maritime surveillance expenditures, i.e. from an enhanced awareness picture and better collaboration between partners.[44]

Data exchange limitations

Despite the willingness to exchange sensitive data,[45] certain limitations to such sharing were also encountered, and the limited time frame of the pilot project was not enough to overcome those. Limitations to information exchange of sensitive data were particularly the case when the involved partners' area of competences were not aligned, or if one partner had law enforcement status with access to sensitive data, such as border control agencies, whereas the other partner did not have such privileges. In these cases, sharing was exchanged, but only for testing purposes and mostly using "fake" data. These limitations also meant that some of the agencies participated in the BluemassMed project without their main information exchange systems.[46]

Other limitations to information sharing were also felt among the participating Member States, e.g. due to differences in organisational setups of maritime surveillance administrations. For instance, while cross-sectorial sharing of

[42] FEI (2012) BluemassMed Final Report
[43] FEI (2012) BluemassMed Final Report
[44] FEI (2012) BluemassMed Final Report
[45] BlueMassMed project identified several different categories of data: basic, personal, commercial, sensitive, confidential. FEI (2012) BluemassMed Final Report, p. 30.
[46] Italy workshop (17 June, 2013)

information worked well between some Member States, the existence of organisational complexity within some Member States made information sharing more difficult here.[47]

Generally, however, there was a very positive effect from and attitude towards the BluemassMed project; and even if the participating Member States already showed a high degree of national collaboration, BluemassMed has helped bring more collaboration and a sense of cross-sectorial "community" across borders. One of the key questions that arose in terms of information exchange was what information that should be exchanged, and under which framework and legal conditions.

As such, even if the BluemassMed project uncovered great willingness to share information across user communities, the project's achievements in the area of data exchange policies have been limited. The project therefore also underlined that there is still much work to be done; i.e. in terms of designing the framework for information exchange, including information sharing data policies, access rights, confidential/sensitive information management, detailed and rigorous requirements and specifications - areas that CISE will be addressing.

4.4.2 MARSUNO

Project background

At the same time as the BluemassMed project, which comprised Mediterranean Member States, another CISE frontrunner pilot project was launched in 2010 involving Member States around the Northern European sea basins. MARSUNO brought together 24 authorities across all seven user communities from nine EU Member States (Belgium, Estonia, Latvia, Finland, France, Germany, Lithuania, Poland and Sweden) as well as Norway. Having the same aim as the BluemassMed project, the purpose of MARSUNO was to determine the extent of already on-going information exchanges as well as to establish interoperability between already existing monitoring and tracking systems across user communities, allowing the sharing of information of common interest in the effort to establish an enhanced maritime awareness picture. The project ended in 2011.

Results

Similar to the BluemassMed project, MARSUNO started out by a data mapping exercise, in which the participating authorities would identify a common ground of basic data that would be relevant to exchange. On this basis, they then defined the data and information requirements in terms of data access that would help to improve their own performance. It was found that although requirements differ across authorities there was an overlap in terms of establishing near-real-time situational pictures.[48]

MARSUNO also found, through a number of thematic (sectorial) reports, that a high degree of well-functioning data sharing across borders has already been reached within sectors in the Baltic Sea region. Some Member States have

[47] Italy workshop (17 June, 2013)
[48] EC (2011) MARSUNO Final Report

developed cross-sectorial information exchange systems at the national level, but in other Member States this remains a challenge. Also, the information that is exchanged across borders also tends to stay within the same community; here cooperation also remains a challenge. [49]

The MARSUNO project clearly identified the need for authorities to move from a situation where limiting data and information availability impedes the flow to a more user-defined state of the art exchange. This also concerns the automatic processing and sharing of various events in near real time, which according to the MARSUNO final report would represent a major value added. The reason for this being that various authorities would otherwise be engaging in the same activities in the attempt to obtain information about the event. Coordinated efforts combined with automatic information sharing, however, could potentially speed up the information gathering significantly for all partners and reduce cost. Other examples of potentials for avoiding duplication were also found.[50]

Data exchange limitations

Similar to the BluemassMed project, one of the tasks of the MARSUNO project was to identify administrative, legal as well as technical limitations in the exchange of information between sectors and across borders.

Generally, it was found that there are no apparent limitations to cross-border information exchange. The minor limitations could be overcome without great efforts, in as far as the information exchange took place within the same sector and that the purpose of the information stays the same. However, this property did not hold when looking at cross-sectorial information exchange.

One of the main issues as regards achieving effective cooperation and data sharing identified in the MARSUNO project was related to the lack of cultural understanding for cooperation at the national as well as international cross-sector and cross-border levels. In fact, this was felt throughout the different user communities and demonstrated in both thematic MARSUNO reports and project discussion groups.[51] The source of this issue, it was stated, is mainly due to lack of cross-sectorial information sharing *within* Member States. Overcoming the issue would therefore require that Member States focus on widening national information exchange before broadening it towards international exchange. This would particularly require the building of trust and confidence between the sectors; for which Operation Atalanta has been highlighted as a good example of how to do this; including the tactical, the operational and the political level.[52]

In connection with the above, the MARSUNO project also re-emphasized the issue of lack of knowledge; i.e. “we don’t know that we don’t know”. Such a lack of awareness is widespread within all sectors and may contribute to the lack of information sharing; information that may otherwise be relevant to different

[49] EC (2011) MARSUNO Final Report
[50] EC (2011) MARSUNO Final Report, p. 21
[51] EC (2011) MARSUNO Final Report, p. 19
[52] EC (2011) MARSUNO Final Report, p. 30

authorities. Moreover, much data appeared to be 'over-classified', thus calling for the need to downgrade classification levels; especially with respect to data exchanges between civil and military sectors. Direct communication between civil and military sectors is similarly hard to obtain, and at the EU level there appears to be "political obstacles" preventing practical cooperation even if there are good relations between the different agencies.[53]

The lack of a common language and definitions was also highlighted as a major cultural obstacle since different interpretations of terms and concepts impede cooperation. In particular, common standards for routine work and information exchange were highlighted as being of great importance.

Similar to the BluemassMed project, limitations to data exchange also included differences in organisational structures between administrations as well as differing working methods and political and professional cultures.

From a legal perspective, MARSUNO identified limitations to information exchange as regards the protection of personal data; i.e. pertaining to Data Protection Directive and the Data Protection Regulation. These as well as other legal limitations are described in greater detail in the Legal Study (Chapter 5).

4.4.3 SafeSeaNet-VMS synergies pilot project

Background

In 2011, EMSA launched a pilot project to explore the synergies between the SafeSeaNet system and VMS. The project sought to bring together the fisheries control community and the VTM communities. The background for the project was the amendment of the VTM Directive, which required fishing vessels over 15 metres to be fitted with AIS (Art. 6a). On the other hand, the Common Fisheries Regulation requires vessels above 12 metres to be fitted with VMS equipment ('the blue box'). At the same time, the Regulation requires Member States to use AIS data for cross-checking with other available data (Art.10). As a result, EU fishing vessels are being monitored both by the SafeSeaNet system and by the FMCs in the Member States.

The operational phase of the project started in April 2012 and ran until October 2012. Four Member States participated in the project: Italy, Latvia, Malta and Spain, and EFCA also expressed an interest to be involved.

Information sharing

The participating FMCs identified a limited number of fishing vessels, which were fitted with both AIS and VMS devices. Data were provided in two directions: from FMC to SafeSeaNet for VMS position messages and from SafeSeaNet to FMC for AIS positions messages. Since AIS messages are parsed considerably more frequently than VMS messages, AIS data can increase data rates significantly. The integrated traffic image (VMS and AIS data) was also made available through a web-based interface to the participating FMCs.

---

[53] EC (2011) MARSUNO Final Report, p. 30

Project results

The Final Report, which followed the conclusion of the project[54], discussed, among other things, the constraints following from the sensitive nature of the activities of the fishing vessels, which have a potentially high commercial impact. Consequently, VMS positions are handled in accordance with the applicable confidentiality criteria (Art. 113 of the Common Fisheries Regulation). In this connection, some of the FMCs participating in the pilot project expressed disclosure related concerns and even hesitation about their participation in the pilot project.[55] In response to that, the Report emphasised that the pilot project did not seek to establish a data sharing platform between the participating countries, and that data was provided solely to the relevant FMCs in accordance with the applicable legislation. In the CISE context, this would however be a relevant concern.

Overall, the project participants concluded that the correlation of VMS and AIS data can increase operational capabilities and, in particular, the ability to monitor fishing activities and/or violation of restricted fishing areas, but also provide an important support tool for search and rescue operations.

4.4.4 MARSURV-3/Blue Fin Tuna (BFT) pilot project

The pilot project resulted from the cooperation between EMSA and EFCA. It ran from May until September 2012. It covered areas of the Mediterranean Sea, as identified by EFCA as being of interest with the framework of the BFT JDP.

The aim of the project

The pilot project sought to obtain a real-time, operational maritime awareness picture (via data fusion and the establishment of a vessel register). It aimed to provide for quick and centralised access to information, facilitate cross-checking and correlation of VMS, AIS and visual sightings and thereby support e.g. behaviour analysis, risk assessment or fishing activity assessment.

Information sharing

The main data streams for MARSURV-3 included the VMS data provided by EFCA and VTM data (including SafeSeaNet, LRIT and other sources). The data was supplemented by additional data, such as satellite AIS, which allows tracking AIS vessels that are outside the range of AIS coastal stations. The different data sets were combined and displayed on a nautical chart, which was made available via a restricted web interface. Moreover, fishing vessel activity was observed and visual sightings information was collected during the course of surveillance and inspection activities carried out by the Member States. This data are updated by EFCA on the web interface.

[54] SSN-VMS synergies pilot project, Final Report, 9 November 2012.
[55] Ibid, p. 12.

4.4.5 EMSA and EFCA cooperation in the regulatory area of the Northwest Atlantic Fisheries Organisation

A pilot project between EMSA and EFCA ran from 1 March to 30 April to monitor the regulatory area of the Northwest Atlantic Fisheries Organisation (i.e. a large portion of the Atlantic Ocean including the 200-mile zones of Coastal States' – USA, Canada, St. Pierre et Miquelon and Greenland – jurisdiction). The pilot project aims to assess the added of using correlated vessel activity information for targeting inspections.

Information sharing

The classic behaviour monitoring using maritime position data sets (satellite AIS and vessel targets detected by satellite radar images) is being integrated with fishery-specific information such as fishing licenses and gear type details.

4.4.6 The Paris Memorandum of understanding on Port State Control (Paris MoU)[56]

Background

Regional Port State Control was initiated in 1982. As of today, 27 Maritime Authorities participate in the Paris MoU[57] (including Authorities from Canada, Iceland and Norway; the Commission is not a signatory, but is a member of the MoU's Committee) in order to co-ordinate their Port State inspection. The Paris MoU is a *voluntary agreement* in which the participating authorities have agreed to maintain an effective system of port state control and to carry out a certain number of inspections on merchant ships of certain priority calling at one of its ports of anchorage. Additionally, the authorities have agreed to consult, cooperate and exchange information with the other authorities in order to further the aims of the MoU.

Information sharing

Section 5 of the Memorandum lays down more detailed rules for the sharing of information among authorities. It further provides that when inspection or the detection data contain information about private persons, the Authorities undertake to ensure protection of the privacy of those persons in accordance with applicable laws and regulations, but this protection should not prevent the publication of the company of ships inspected or publication of the names of charterers involved.

The procedure for the sharing of information is specified in detail in Annex 3 of the MoU. The MoU establishes an Information System for the sharing of inspection information. The Paris MoU is supported by a central database THESIS, which is hosted and operated by EMSA. By means of computerised data transmission, the Authorities undertake to provide information on ships inspected in the national ports. The inspection files are updated on a daily basis and should be easily accessible for purposes of consultation and updating.

[56] Within Port State Control see also the Mediterranean MoU and the Black Sea MoU.

[57] The most recent version of the MoU includes the 34rd Amendment and is in force as of 10 May 2012.

The Annex also provides for the possibility to make the data from the Information System available to other organisations (the, so called, 'observers'). With the consent of the Authority, data may on behalf of that authority be submitted to the International Maritime Organisation (IMO) and to the International Labour Organisation (ILO). Moreover, with the consent of the Committee, the Secretariat may conclude data exchange contracts with other organisations. An example of such contract is the agreement with the IMO's Secretariat from 26 March 2012.

Annex 4 provides a list of information related to inspections and detentions, which should be published on the MoU website on a monthly basis. Additionally, inspection results can be consulted on the Equasis website.

Organisational setup

A Committee is established under the MoU, consisting of a representative of each of the participating Maritime Authorities and of the Commission. The tasks of the Committee include the harmonisation of procedures and practices relating to inspection, development and review of guidelines and procedures for carrying out inspection and to share information. Additionally, the MoU Secretariat (the Hague) plays an important role in supporting the work of the Committee (in particular between its sessions) and facilitating the exchange of information.

4.4.7 Interagency cooperation agreement between EMSA, FRONTEX and EFCA

On 25 November 2009, EMSA, FROTEX and EFCA concluded an agreement with a view to cooperating in the field of maritime surveillance. The cooperation should result in an improvement of the control of external maritime borders of the EU, increase of maritime safety and the enhancement of the coordination of fisheries control. The cooperation agreement provides for the exchange of information and data on matters of common interests, exploration of synergies in the use of the maritime surveillance, information systems and the possibilities of joint use of assets and expanding the collaboration between the agencies with respect to coordination of inspections, research, development, etc.

EUROSUR Proposal

The Proposal for a Regulation establishing the European Border Surveillance System (EUROSUR) envisages in its Art. 17 cooperation, in particular, with EUROPOL, EMSA and EFCA, other EU agencies, which can provide relevant information and the Commission. The further use of the data received by the cooperating agencies is limited by their respective legal frameworks and fundamental rights.

4.4.8 Interagency agreement between EMSA and FRONTEX

On 3 May 2013, EMSA and FRONTEX signed an interagency service level agreement to enhance situational awareness of Europe's maritime domain.

Under the agreement, EMSA will develop tailored monitoring services, information products and tools. Data from IMDatE, including ship position reports and satellite images, will be provided to FRONTEX to enable them to construct a more comprehensive overview of activities at Europe's maritime borders. This will

build upon previous pilot project services developed by EMSA for FRONTEX and on the integrated services offered by EMSA to Member States and other EU bodies.

EMSA's services will be provided to FRONTEX in the framework of joint operations at sea and of EUROSUR. By strengthening information exchange between Member State authorities, EUROSUR aims to reduce the number of irregular migrants entering the EU undetected, prevent cross-border crime, as well as to assist search and rescue activities at the external maritime borders of the Union.

4.4.9 EMSA and EFCA cooperation (MARSURV-3/Blue Fin Tuna)

EFCA and EMSA have been collaborating to develop a maritime monitoring service for Blue fin tuna fisheries activities. The cooperation resulted in the MARSURV-3/Blue Fin Tuna pilot project, which is described in more detail above.

4.4.10 EMSA cooperation with EU NAVFOR

Following successful pilot projects in 2009 and 2010, EU NAVFOR requested EMSA to develop an integrated maritime monitoring service for protecting the EU merchant fleet transiting off the Somalia coast. This resulted in the MarSurv service, based on a Service Level Agreement between EU NAVFOR and EMSA. The service integrates and fuses relevant EMSA vessel traffic and satellite information with vessel-related and risk information available from EU NAVFOR and provides an overview of the activity in the defied areas. It was made available through a dedicated user interface and subsequently through the IMDatE platform. Throughout 2013, new data streams and piracy intelligence information will be integrated in the service.

4.4.11 Strategic co-operation agreement between FRONTEX and EUROPOL

With reference to Article 13 of the Regulation 2004/2007/EC establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX Regulation), EUROPOL and FRONTEX concluded a co-operation agreement to enhance the their cooperation on 28 March 2008.

Scope of cooperation

The Agreement seeks, in particular, to enhance the exchange of strategic and technical information between the two agencies, as defined in Article 2 of the Agreement, but does expressly exclude data related to identified or identifiable individuals.

Strategic information include e.g. enforcement actions that might be useful to suppress offences and improve integrated border management, trends and developments in the methods used to commit offences and information regarding

new methods to commit offences, routes and changes in routes used by smugglers and illegal immigrants, prevention strategies, risk analysis, etc. Technical information includes information regarding e.g. working, training and analytical methods.

The information exchanged should relate exclusively to the tasks and activities of the two agencies, and the exchanged data should only be used for the purposes of the Agreement as identified in Art. 1 (Art. 5(3)). A further limitation to the data exchange is included in Arts. 5(5) and 5(6) of the Agreement, which provide that the party providing the information may stipulate conditions on its further use and prohibit the use of the information for purposes other than the purposes for which the information was provided. The information may be transmitted to third parties other than the Member State only upon the prior consent of the providing party. Art. 5(8) of the Agreement lays down the rules for public access to the transmitted information.

Arts. 7 and 8 govern the confidentiality of the information transmitted pursuant to the agreement. The relevant articles provide that all information processed by or through EUROPOL, except information marked as or clearly recognisable as being public information, should be subject to a basic protection level within EUROPOL as well as in the Member State. The parties to the Agreement are obliged to ensure such a basic protection level. Information requiring additional security measures is subject to a classification level of FRONTEX or EUROPOL (indicated by a specific marking), and each party should ensure that the information receive a level of protection equivalent to the level of protection applied to that information by the other party.

EUROPOL handles **three basic categories of data:** EUROPOL public information, EUROPOL Basic Protection level information (BPL information) and EUROPOL classified information. Four classification levels exist with respect to the final category of data: EUROPOL Restricted, EUROPOL Confidential, EUROPOL Secret and EUROPOL Top Secret.[58] A table of equivalence has been established for all classification levels in each Member State. Tables of equivalence exist also for third parties having a co-operation agreement with EUROPOL.

Following the conclusion of the co-operation agreement, EUROPOL and FRONTEX signed a MoU and a bilateral agreement to allow more active FRONTEX participation in investigations of facilitated illegal immigration and human trafficking. The MoU provides a basis for the establishment of a secure line between the two agencies, and the agreement specifies the details of services and applications available through the secure line, including provisions regarding access to EUROPOL's Secure Information Exchange System (SIENA).

[58] See EUROPOL Information Management, Products and Services, File no. 2510-271.

4.4.12 Cooperation between FRONTEX and CFSD policy

Although the integrated maritime surveillance policy resulted in growing implications of the CFSD policy, in particular in the FRONTEX activities, there are very few examples of cooperation between the FRONTEX and the EU CFSD policy. In December 2008, FRONTEX entered into a working agreement with the EU Joint Situation Centre (SitCen), now integrated in the European External Action Service (EEAS), for risk analysis purposes for the 2009 report on the impact of the global economic crisis on illegal migration to the EU.

Additionally, FRONTEX and the European Defence Agency (EDA) exchange information when supporting the integration and interoperability of maritime surveillance systems and the use of Remotely Piloted Aircraft Systems (RPAS).

4.5 Summary

Current systems work well

Overall, there appear to be agreement among user communities in Member States that existing maritime surveillance and cooperation systems work quite well, at least within their respective sectors. This is both the case within and between countries. The substantial amount of advanced pan-European systems supports this finding; not to mention many of the expected developments within the sectors. This is exemplified by the fact that all the relevant EU Agencies are on their way of upgrading, enhancing, and/or integrating their surveillance systems within their areas of responsibility.

Potential for better sharing across sectors

However, there is agreement that current systems are lacking when it comes to maritime surveillance and cooperation *across different sectors*. This is the case despite a number of system developments and progressive cross-sectorial pilot projects, such as BluemassMed and MARSUNO. From this point of view, much potential therefore exists in establishing an interoperable system or systems that can make it easier to exchange information across sectors.

From the point of view of national cross-sector information sharing, however, several developments have happened, or are in the process. As described, several Member States are on the path of establishing national cross-sector information sharing environments using layouts and architectures that are not unlike what is intended for the CISE. Member States also see an increasing need for pursuing such developments regionally, but establishing such cross-sectorial environments across borders is a major task, and cannot easily be undertaken by Member States alone.

5 Baseline: legal

5.1 Legal principles

Fundamental principles

The legal baseline for CISE starts from the notion that, within the current legislative framework, the rights and responsibilities are subject to a rather fragmented approach, horizontally governed by **fundamental principles** included in the Charter of Fundamental Rights of the EU. These principles include mainly the rules governing the processing of personal data, but also the public right to access documents and documentation originating from public bodies exercising their authority. The principles safeguarding fundamental rights and freedoms of individuals do not constitute legal limitations to the sharing of maritime surveillance information as such, but they impose certain conditions on the sharing.

General principles

Legal principles stemming from overarching horizontal legislation and those that do not stem directly from horizontal legislation, but nonetheless affect potentially all or multiple user communities, are referred to as **general principles**. To the extent such principles constitute conditions to maritime surveillance information sharing across user communities and across borders, they are referred to as **general limitations**.

Responsibility to share and access rights in sectorial legislation

The analysis of specific sectorial legislative acts has furthermore revealed that, on numerous occasions, these acts stipulate **the responsibility to share** maritime surveillance information and **access rights** to such information, but that such responsibility and corresponding access rights are often limited to expressly specified recipients in specified Member States for expressly specified purposes.

5.2 General legal conditions for maritime surveillance information sharing

Four types of legal conditions are addressed in this section:

1 Conditions stemming from the fundamental right of an individual to the protection of personal data

2 Conditions stemming from an obligation to protect the confidentiality of commercially sensitive data

3 Classification of information

4 Contractual limitations.

Protection of personal data

The overall most important legislative acts governing access to and processing of data generally and in the maritime area are the data protection legislation at the EU and national level. The data protection legislation, i.e.:

- the 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 (Data Protection Directive)[59]
- Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Framework Decision)[60]
- the Regulation 45/2001/EC 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 (Regulation 45/2001)
- and horizontally the Charter of Fundamental Rights of the European Union, 2000/C 364/01 protects the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data.

The scope of protection afforded under the data protection legislation

When construing the provisions of the personal data protection in the CISE context, the objective of the rules should be considered: to protect the fundamental rights and freedoms of natural persons, and in particular, their right to privacy. As the Data Protection Working Party emphasises,[61] this is a very important element to be taken into account in the interpretation and application of the personal data protection legislation since it may play a substantive role in determining how to apply the provisions of the Directive to situations where the rights and freedoms of individuals are not at risk and, on the other hand, caution against any interpretation of the rules so as to deprive individuals of protection of their rights.

Moreover, Art. 1(2) of the Data Protection Directive provides that Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1 of Art. 1. Similarly, Art. 1(1) of the Regulation 45/2001 contains the same principle.

[59] Currently under review process, 2012/0011 (COD).
[60] Currently under review process, 2012/0010 (COD).
[61] Art. 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, p. 29.

Furthermore, personal data protection legislation does not apply to all situations of processing of personal data, and the applicable rules, as such, contain a number of exceptions and restrictions and provide a degree of flexibility, so as to strike a *reasonable balance* between the protection of the data subject's rights and the legitimate interests of the data controllers, third parties and the public interest.[62]

The right to the protection of personal data is a binding fundamental right, based on Article 8 of **the Charter of Fundamental Rights of the EU.**[63] Accordingly, the Charter provides overarching binding principles also for the implementation of CISE.[64] Article 8 of the Charter of Fundamental Rights regulates furthermore that personal data must be processed fairly for specified purposes and on the basis of a legislative basis laid down by law.

At the level of secondary law data protection is in particular regulated by the following instruments:

- **Data Protection Directive 95/46/EC:** This directive is the central legislative instrument in the protection of personal data in the EU. It stipulates general rules on the lawfulness of the processing of personal data and the rights of the individuals whose personal data are processed. The Directive does not, however, apply to the processing in the course of activity that falls outside the scope of Community law (Common foreign and security policy) and to processing operations concerning *public security, defence, State security* and the activities of the State in the areas of *judicial cooperation in criminal matters and police cooperation.* It further allows for exemptions and restrictions (Art. 13) of some of its provisions for, for example, *safeguarding national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offence*, resulting in some divergence in implementation of the Directive at national level.[65]

- **Council Framework Decision 2008/977/JHA:** The Decision applies to personal data which for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties are transferred between different Member States (Article 1 (2)(a)), or which, after having been transferred between different Member States are subsequently transferred to a third country or an international organisation (Article 13). It furthermore applies to personal data which are or have been transmitted or made available by Member States to authorities or to information systems established on the basis of the former Title VI of the Treaty on European Union ('Police and judicial cooperation in criminal matters') (Article 1(2)(b)),

---

[62] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136.
[63] 2000/C 364/01.
[64] Compliance with the Charter of Fundamental Rights in Commission legislative proposals, Methodology for systematic and rigorous monitoring, Communication from the Commission, COM(2005) 172 final.
[65] Marsuno, Final Report, p. 48.

or are or have been transmitted or made available to the competent authorities of the Member States by authorities or information systems established on the basis of the former Treaty on European Union or the former TEC.

› **Data Protection Regulation No. 45/2001:** The Regulation applies to the processing of personal data by EU institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of EU law. Art. 20 of the Regulation allows for exceptions and restrictions of some of the provisions of the Regulation in order to safeguard the prevention, investigation, detection and prosecution of criminal offences, an important economic or financial interest of a Member State or of the EU, national security, public security or defence of Member State, etc.

The scope of personal data

The data protection rules contain a broad definition of personal data:[66] it covers *all information which may be linked to an individual*.[67] Accordingly:

› Information relating to **legal persons** is in principle not covered by the data protection legislation unless such information may be considered as "relating to" natural persons. This would be the case, for example, where the name of the legal person derives from that of a natural person. It follows that information on a vessel owned by a legal person will normally not constitute personal data, unless, for example, the name of the legal person derives from the name of an individual who owns that legal person.

› Information relating to **dead individuals** is not considered to constitute personal data subject to the Directive. On the other hand, where the data is used to ascertain whether the person to whom the data relate is still living or may be dead (for example in the context of a search and rescue operation), that data should in principle be treated as being potentially subject to the data protection legislation. As a corollary, data contained, for example, in the marine casualties database EMCIP (Directive 2009/18/EC) would normally not constitute personal data unless combined with data on identified or identifiable living individuals.

The concept of 'personal data' includes data providing *any sort of information.* It includes information regarding whatever type of activity undertaken by the individual and it is not limited to the individual's private and family life.[68] It includes, for example, information regarding working relations, economic and social behaviour.

---

[66] Article 2 (a) of Directive 95/46/EC: 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, mental, economic, cultural or social identity.

[67] COM (90) 314 final, p. 19, COM (92) 422 final p. 10.

[68] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, p. 6.

The crucial point in the analysis is, however, whether particular information **relates to** an individual and whether such an individual is **identified or identifiable.**

Identified or identifiable person

A person may be identified directly or indirectly by name or other data. A person may, for example, be identifiable indirectly when one piece of information combined with other pieces of information (whether the latter is contained by the data controller or not) will allow the individual to be distinguished from others. When determining whether a person is identifiable, account should be taken of "all the means likely reasonably to be used either by the controller or by any other person to identify the said person."[69] Factors to be taken into account when assessing the reasonableness of the means include: cost, the purpose pursued by the data controller in the data processing, the way the processing is structured, the advantage expected by the controller or by any other person, the interests at stake for the individuals, etc.[70]

It follows that e.g. *vessel identification details* may lead to the identification of an individual (e.g. captain or the owner of the vessel, if the owner is a natural person) since such information will normally be available to the national authorities if "all means likely reasonably to be used" are employed to identify such person.

Relates to an individual

Information 'relating' to an individual includes information conveying data about individuals, but *also about objects.*[71] As a rule, information about an object will constitute personal data only if the information is linked to an individual or if there is a reasonable chance that the data will be used to learn something about an individual. Data relate to a particular individual because it is linked to that individual and, as it inform and influence actions or decisions that affect an individual.

The context of the data is important. For example, information about a house is often linked to the owner or resident of the house, and consequently the data about the house will be personal data about that individual. However, data about a house will not, by itself, be personal data. On the other hand, when the data are used in *decisions* about an individual, for example, to determine whether the individual made unlawful alterations to the house and whether action should be taken against that individual, the data on the house become personal.

Accordingly, if there is, for example, a suspicion that a vessel has been involved in unlawful or illegal activities, the data about the vessel may constitute personal data, if they fulfil the requirements of Art. 2(a) of Directive 95/46/EC, i.e. if they relate to an identified or identifiable person. This could be the case, e.g. if the data are or

[69] Recital 26 of the Data Protection Directive 95/46/EC.
[70] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, p. 15.
[71] Data Protection Technical Guidance Determining what is personal data, Information Commissioner's Office, 2012, p. 15.

could be used to determine which actions should be taken against the persons on board or the owner of the vessel (if the owner is a natural person).

Still, where data about objects are not currently processed to provide particular information about an individual, but *could be* processed to provide information about an individual the data *may* constitute personal data. In that connection it must be considered whether the processing of the information has or could have a resulting impact on the individual, even though the content of the data is not directly about that individual, nor is there any intention to process the data for the purpose of determining or influencing the way that person is treated. For example, information from vessels' tracking devices is normally used to establish where the vessel as such is located and not to determine the whereabouts of a particular individual on board. But in situations where the data is used to locate (a) particular person(s) (for example for the purpose of a police operation), this information may constitute personal data.

Combination of data

The most important processing activities in the CISE context would include (original) collection, disclosure and combination of data. CISE envisages the combination of several data sets (typically from different providers) in services, which will then be provided to the recipients for the purpose of performing their maritime surveillance tasks. Combination of data, like any other processing of personal data (see below), requires an appropriate *legal ground* and should *not be incompatible* with the purpose for which these data were collected. Additionally, the collection has to be proportionate to the purposes for which the data are processed.

The combination of data also entails that a single piece of data, which is not personal data for one data controller (e.g. vessel identification details) may become personal data when it is combined with another data or passed on to another controller.

Processing of personal data

Processing of personal data is defined in Article 2 (b) of Directive 95/46/EC. It means any operation or set of operations that 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. Lawful processing of personal data is subject to several conditions. These include, but are not limited to, the "*purpose limitation*" and *proportionality*.

The principle of purpose limitation

The principle requires that personal data are processed for a specified, explicit and legitimate purpose and limits further processing of such personal data to **purposes not incompatible with the purposes as they were originally specified.** The compatibility of purposes has to be assessed on a case-to-case basis.[72] In assessing the compatibility of purposes, the Article 29 Working Party recommends to take

[72] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, p. 21.

into account the following factors: (1) the relationship between the purposes, (2) the context in which the data have been collected, (3) the reasonable expectations of the data subjects, (4) the nature of the data, (5) the impact of the further processing on the data subjects and (6) the safeguards applied by the controller to ensure fair processing and to prevent undue impact on the data subjects.

The final criterion, i.e. the safeguards applied by the controller to ensure fair processing on the data subjects, in particular is worth exploring in the CISE context. Indeed, appropriate additional measures may to some extent compensate for the change of purpose or the lack in the specification of the purpose. Such additional measures may include additional technical and organisational measures to ensure functional separation or possibilities for the data subjects to provide for a specific *consent* to the use of the data for additional specified purposes.[73]

Proportionality

As regards to the principle of proportionality, personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. It should also be emphasised that if personal data are processed for several purposes, all requirements on lawful processing (as provided for example in Article 6 of the Data Protection Directive) apply to each purpose separately. Accordingly, a case-by-case analysis would have to be carried out to ensure, for example, that the data are adequate, relevant and not excessive in relation to the purpose of their processing.

The revision of the data protection legislation

The legislative process for the revision of the personal data protection legislation is still on-going[74] and it is, at this stage, premature to predict and assess the data protection rules agreed in the future data protection legislation.

Confidentiality and commercial secrecy

Information can apart from being within the scope of personal data also be included in legislative acts governing the areas of confidentiality, secrecy and access to documents. The exchange of data within that area can be restricted for these reasons. Confidentiality can originate either from legislation or on the basis of contractual provisions. Unlike the protection of personal data, no harmonisation exists of rules governing commercial and professional secrecy. These continue to be the subject of national legislation and as such, raise an issue of legal complexity for CISE.

At EU and international level, provisions addressing confidentiality and commercial secrecy can be found in several legislative acts governing the maritime area e.g. VMS Directive, VTM, Directive, SOLAS Convention, port security regulations. Such provisions do not necessarily constitute an obstacle to the sharing of information between Member States as such, but establish obligations for the receiving authority to apply the same level of confidentiality as the provider. The

[73] E.g. Annex II to the Directive 2000/59 provides on the standard form for a prior notification consent to the use of the data for "other inspection purposes".
[74] 2012/0011 (COD) and 2012/0010 (COD).

information can therefore not be shared with third parties potentially including other functions.

Classification of information

A commonly detected administrative hindrance is public authorities' classification of information, which gives the information a specific label even though there is no strict legal limitation for access. That is not a legal limitation but can be perceived as such and it could potentially be a challenging issue for the efficient implementation of CISE. In the maritime domain, no common classification levels exist, some guidance is nonetheless provided in the Commission's Provisions on Security[75] and the Council's security regulations.[76]

Contractual limitations

In the CISE context, three types of contracts are relevant:

- Agreements between authorities.
- Procurement contracts with private providers of data and information
- Outsourcing of CISE related tasks.

Contracts are concluded in accordance with standard agreements, national law, or the choice of law among the contract parties. In practical terms, this means that CISE faces a multitude of different contract approaches as national contract law and contract practice vary throughout Europe.

Furthermore, the quality of the contract outcome requires negotiation powers, which depend on resources available for the public CISE actor and the actual bargaining position.

Differentiated approach

This illustrates that contractual limitations vary significant amongst the CISE stakeholders throughout Europe. CISE cannot legally ensure a uniform approach to the conclusion of contracts as this will interfere with national legislation and competences.

Instead, the EU may apply CISE related recommendations directed at CISE national stakeholders when entering contracts governed by private law. The contract, which itself is only binding for the contracting parties, shall safeguard both the private interests and the need for CISE distribution of the data provided. It shall be recalled that the data collected by the public stakeholders may be governed by EU and national legislation, such as data protection legislation and openness. However, a poorly drafted contract concluded with private data providers may restrain the actual public use in that case and thus be a limitation for CISE. This

[75] See Commission's Decision amending its internal Rules of Procedure, C(2001) 3031.
[76] Council decision adopting the Council's security regulations, 2001/246/EC.

may be the case, for instance where the public authority has agreed to an extreme confidentiality clause or use based on a costly license agreement.[77]

Outsourcing

In case a contract allows a private contract party to possess or obtain information that legally is in the domain of the principal contract party, the contract must regulate the use of the information by the private contract party. This concerns typically outsourcing, and is especially important where such use by the private party is not governed by adequate legislation.

5.3 Specific conditions governing the sharing of maritime surveillance information

5.3.1 Analysing sectoral legislation

Sectoral approach to information sharing

The legal conditions for the sharing of maritime surveillance information rely primarily on a sectoral (vertical) approach. The provisions of sectoral legislation relevant to the sharing of information reflect a need-to-know principle and accordingly provide for the sharing of information mostly within the same function or within specified functions.

Relatively few problems are encountered when information is shared within the same function. This is, however, not the case of cross-sectorial information exchange (section 4.2.3). The Member State Survey, the interviews conducted with the CISE stakeholders, the BlueMassMed and the MARSUNO pilot projects, indicated that this is attributable also to legal limitations (Figures 4-9 and 4-10). Crucial in this context is therefore the assessment of the extent to which the current legislative framework allows for the sharing of information with other functions and to which extent legal limitations impede such sharing.

Identifying legal limitations

When identifying the legal limitations in the current legislative acts, we have targeted mainly targets four categories of limitations related to regulatory methods.

› Express legislative limitations **prohibiting** authorities from sharing specific types of information

[77] Such finding corresponds to the examples provided by the MARSUNO final report with regard to confidentiality provisions imposed by contracts. One example is the standard agreement of Lloyds Register Fairplay Limited relating to AIS Live. This standard agreement is not a result of "poorly drafting" but it imposes nevertheless 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 MS 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.

- Specific functions **exempted** from the scope of legislative acts that holds provisions on information sharing. E.g. the exemption of defence related activities from almost all types of legislative acts governing the maritime area

- Some legislative acts open a possibility to share by stating "may be shared" in the text. However, that is naturally not seen as an **obligation** to share and especially not across functions. That can be perceived as a legal limitation; even though it is not necessarily in contradiction to provisions of the legislation

- Some legislative acts hold provisions on reporting from stakeholders but **no specific provisions** on sharing within or between functions. Other pieces of legislation specifically oblige authorities to share specific pieces of information either with the public or with other Member States within the same function, but provide no explicit access rights for the authorities representing other functions.

Defining legal limitations

What is perceived as a specific legal limitation can be subject to divergent interpretations:

On the one hand, provisions governing the sharing of information collected within the framework of sectoral acts provide legal basis for the processing of and the sharing of the information (*access rights*);

On the other hand, such provisions, while positively selecting the receivers of the information, leave the question of the possibility of sharing the information with other CISE functions open to interpretation. Similarly, when the information shall be provided to competent authorities, it is open to interpretation to which extent other CISE functions may be regarded as competent/relevant authorities in the context of the information collected.[78] While provisions of this kind do not clearly amount to express prohibitions to share information across functions, they contribute the preservation of an environment of legal uncertainty and a culture in which cultural, administrative and technical limitations may prevail. Accordingly, the first and the second interim report construed such provisions as cross-sectoral (and in a few cases cross-border) *limitations to information sharing*.

"Legal limitation"

The term "legal limitation" is therefore used throughout the reports as a **neutral term**, identifying, among other things, the situations in which the access to the information is by the provision in question limited and access rights are not expressly provided for the authorities representing all CISE relevant functions. This is done without assessing whether the limitation is justified for example by the need-to-know principle governing the sharing of sensitive information. It follows that the identification of a provision as one containing legal limitation does not entail that the provision has to be amended as this

[78] Internal organisation of the maritime surveillance tasks and responsibilities is within the competence of the Member States and differs largely across EU.

may in many cases not be the most efficient measure for the effective implementation of CISE[79].

The character of specific limitations

Some of the limitations, formally embedded in sectorial legislation, are an expression of overarching horizontal principles (in particular the applicable personal data protection legislation and restrictions justified by the legitimate interests of commercial operators in the confidentiality of commercially sensitive information). This entails that, should the sectorial limitation be targeted in order to improve the conditions for information sharing from a CISE perspective, due consideration has to be given to the general principles from which such sectorial limitations stem.

Improving the conditions for information sharing from a CISE perspective

Although considerable progress has already been achieved through various initiatives pursued on national and EU level (section 4), legal limitations, reinforced by cultural, administrative and technical limitations, continue to impede cross-sectorial and cross-border information exchange (see above).

Legal limitations are limitations deriving from legislation and as such may be reduced by legal measures. However, in order to facilitate the interpretation of the provisions in question, there is also a potential to make the use of non-binding measures to reduce the effect of legal limitations. In general, the effectiveness of legal measures in doing so is expected to be higher than of non-binding measures, resulting from their general application and legally binding force. Still, it is fair to assume that a successfully implemented non-binding measure can in principle be equally effective as a legally binding measure.

In order to reduce the effect of legal limitations to improve the conditions for information sharing from a CISE perspective, a **positive formulation of access rights** to the relevant information may be added to the provisions of sectorial legislation governing information sharing. Such provisions would be subjected in particular to the condition of compliance with fundamental rights, including personal data protection requirements, and the protection of legitimate commercial interests.

Since, as indicated above, the internal organisation of the maritime surveillance tasks and responsibilities is within the competence of the Member States, clarification may be provided through e.g. specifying the purposes for which the relevant information may be shared with other CISE functions (e.g. "the information may be provided to competent authorities for the purposes of ..."). The critical point in this connection will be the formulation of the purposes for information sharing, so that these comply with the conditions imposed for example by the personal data protection legislation and the requirements to protect the confidentiality of commercially sensitive information.

Appendix D provides an overview of legal conditions to information sharing in sectorial legislation. The appendix identifies from a CISE perspective potential changes in the legislation, which could improve the conditions for information sharing from a CISE perspective.

5.3.2 Specific limitations

The analysis of sectorial legislation, relevant for the sharing of maritime surveillance information, revealed that such legislation provides numerous access rights to the information collected, but at the same time create – in the sense described above – limitations to information sharing. These limitations relate both to cross-border and, in particular, to cross-sectorial information sharing and fall broadly into several different categories:

1 **The act provides for information sharing, but this sharing is voluntary only** (e.g. Art. 12 of Regulation 1224/2009 establishing a Community control system for ensuring compliance with the rules of the common fisheries policy Art. 13(4) of Regulation (EEC) 2913/92 establishing the Community Customs Code/Art. 47(2) of the Union Customs Code).

2 **Responsibility to share and corresponding access rights are provided for competent authorities within the same function or within specified functions** (e.g. Art. 1 of Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union).

3 **Responsibility to share and corresponding access rights are provided for recipients in specified Member States only (cross-border limitation)** (e.g. Art. 16(2) of Directive 59/2002 establishing a Community vessel traffic monitoring and information system).

4 **Information is provided for specified purposes** (e.g. Art. 116(4) of Regulation 1224/2009 establishing a Community control system for ensuring compliance with the rules of the common fisheries policy) **or under specified circumstances** (e.g. Art. 8 of the Directive 41/98 on the registration of persons sailing on board passenger ships operating to or from ports of the Member States of the Community).

5 **Specific information or function is excluded from the scope of the act** (e.g. the exception for warships, naval auxiliaries and other ships owned and operated by a Member State engaged only in government non-commercial service).

6 **The act provides for a system of ex-post reporting and/or does not provide for an institutionalised framework for information sharing** (e.g. Art. 9(2) of Directive 2009/15/EC on common rules and standards for ship inspection and survey organisations and for the relevant activities of maritime administrations).

The subsequent analysis of sectorial limitations is divided according to sectors.

5.3.3 Fisheries control

Summary of analysis

The analysis of EU sectorial legislation within the fisheries user community revealed that a large amount of maritime surveillance data is collected and may be exchanged both across borders and, in some situations, also across sectors. These data include tracking data from VMS, AIS and VDS systems and other data collected while monitoring compliance with the common fisheries policy (data on fishing activities, catches and surveillance and inspection data).

Art. 12 of the Regulation 1224/2009 establishing a Community control system for ensuring compliance with the rules of common fisheries policy envisages the sharing of the tracking data (AIS, VMS, VDS) across functions (i.e. for the purpose of maritime safety and security, protection of marine environment, general law enforcement and border control). Although such sharing takes place on a voluntary basis only ("may be transmitted"), this provision represents a considerable improvement in comparison to the previous Fisheries Control Regulation 2847/93.

With respect to other information collected in the framework of the Regulation, the responsibility to share and the corresponding access rights are limited to competent authorities of Member States carrying out tasks within the fisheries control community to the purpose of complying with the rules of common fisheries policy.

Detailed analysis

Following a preliminary assessment, the following legal acts (Regulations) were identified as most relevant and, accordingly, studied in more detail:

- Regulation No 1224/2009 establishing a Community control system for ensuring compliance with the rules of the common fisheries policy;
- Commission Implementing Regulation 404/2001 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;
- Regulation (EC) No 768/2005 establishing a Community Fisheries Control Agency.

A detailed analysis of the above mentioned acts is provided in the Annex.

5.3.4 Maritime safety and security

Summary of analysis

The maritime safety and security user community accumulates a large amount of relevant data (regarding the carriage of dangerous or polluting substances, inspections, ships suspected of discharging polluting substances or not complying with the rules for disposing with ship-generated cargo waste, passengers on board, marine casualties and incidents, etc.) and the legal framework governing the community offers the possibility to share such data across borders and, to a limited

extent, also across functions, in particular through the SafeSeaNet system and, once implemented, the National Single Window.

The SafeSeaNet system allows for the exchange of relevant parts of the registered information for the purposes of "maritime safety or security or the protection of the maritime environment" (Art. 14 of the Directive 2002/59/EC). General conditions governing such exchange stem from the applicable personal data protection legislation and the applicable rules on commercial confidentiality.

In addition, the Directive 2010/65 on reporting formalities for ships arriving in and/or departing from ports of the Member States aims to simplify and harmonise the administrative procedures applied to maritime transport by making the electronic transmission of information standard and by rationalizing reporting formalities. The Directive establishes access rights for the relevant authorities (such as customs and border control) with a view to ensuring that the information is shared so that the commercial operators only reports the same information once.

Finally, as far as cross-sectorial information exchange is concerned, legal acts within the maritime safety and security user community often embrace the protection of marine environment within their framework. This entails, in particular, that competent authorities within the marine environment user community will often by EU legislation be granted access to the information collected in the maritime safety and security framework.

Detailed analysis

Following a preliminary assessment, the following legal acts (10 Directives and 2 Regulations) within the maritime safety and security user community were identified as most relevant and, accordingly, studied in more detail

- Directive 2002/59/EC establishing Community vessel traffic monitoring and information system (VTM Directive)
- Directive 2010/65/EU on reporting formalities for ships arriving in and departing from ports of the Member States
- Directive 2009/16/EC on port State control
- Directive 2009/15/EC on common rules and standards for ship inspection and survey organisations and for the relevant activities of maritime administrations
- Directive 2005/35/EC on ship-source pollution and on the introduction of penalties for infringements
- Directive 98/41/EC on the registration of persons on board passenger ships operating to or from ports of the Member States of the Community
- Directive 2009/21/EC on compliance with flag State requirements
- Directive 2000/59/EC on port reception facilities for ship-generated waste and cargo residues

- Directive 2009/18/EC establishing the fundamental principles governing the investigation of accidents in the maritime sector transport
- Directive 2008/106/EC on the minimum level of training of seafarers
- Regulation 2004/789/EC on the transfer of cargo and passenger ships between registers within the Community and repealing Council Regulation (EEC) No 613/91.

Detailed analysis of the acts in question is included in the Annex.

5.3.5 Customs

Summary

The customs user community has a well-established system for information exchange through electronic customs systems established under Decision 70/2008/EC. The system applies for the exchange of data between the customs authorities of the Member States, economic operators, the Commission and other agencies involved in the international movement of goods. The Decision as such does not envisage information sharing across functions. The provisions of the Community Customs Code (Regulation (EEC) 2913/92 laying down the Community Customs Code) on the other hand allow for a limited information exchange with "other competent authorities" (such as veterinary and police authorities) in the context of conducting customs inspections when this is required for the purposes of minimising risk. General conditions to such exchange stem from the applicable rules on commercial secrecy and personal data protection legislation.

The Community Customs Code was to be replaced by the Modernised Customs Code (Regulation (EC) No 450/2008). However, for a number of reasons the Commission decided to amend the Regulation No 450/2008 before it becomes applicable. The Code is now being recast as the Union Customs Code (UCC),[80] which will repeal the provisions of the Modernised Customs Code.

In comparison with the currently applicable Community Customs Code, the UCC provides more detailed rules governing confidentiality of the protection of personal data. Additionally, in the framework of the customs control it will be possible to exchange information not only for the purposes of minimising risk, but also for combating fraud. These amendments do not, however, change the substance of the provisions regarding information sharing and cannot be construed so as to allow for a broader cross-sectorial information sharing.

Detailed analysis

Following a preliminary assessment, the detailed analysis focused on the following acts (1 Decision and 3 Regulations):

- Decision 70/2008/EC on paperless environment for customs and exchange

[80] Position of the European Parliament of 11 September 2013, EP-PE_TC1-COD(2012) 0027.

- Regulation (EEC) 2913/92 laying down the Community Customs Code
- Regulation (EU) No .../2013 of the European Parliament and of the Council laying down the Union Customs Code (Recast)[81]
- Commission Implementing Regulation 2454/93 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code.

The detailed assessment of the above-mentioned acts is included in the Annex.

5.3.6 Marine environment

Summary

The Directive 2003/4/EC on public access to environmental information sets the baseline for the exchange of environmental information. It is based on the underlying principle that environmental information should be available. This principle is subjected to limited exceptions, which reflect legitimate interests of both public and private nature (Art.4). Information falling within the scope of the exceptions should be wherever possible separated from the rest of the information requested.

The majority of legal acts adopted within the area does, however, not provide for real-time information sharing of environmental data (this function is, as described above, to some extent covered by the maritime safety and security user community). Rather, the relevant acts establish systems based on periodical reporting and notifications to the Commission and to other Member States. Environmental data are furthermore exchanged through the Network established by the EEA, although no specific responsibilities to share or corresponding access rights are provided with respect to such exchanges in the Regulation establishing the EEA. Environmental information will furthermore be available through the WISE-Marine information system.

Of relevance is also the Copernicus programme, coordinated and managed by the Commission. It consists of a complex set of systems that collects and provides up-to-date information related to environmental and security issues to policy makers, public authorities and business operators. The programme is based on an intergovernmental agreement between Member States.[82]

Detailed analysis

Following a preliminary assessment, the following acts (4 Directives, 2 Regulations and a Council decision) within the marine environment user community were identified as most relevant and, accordingly, studied in more detail:

- Directive 2003/4/EC on access to environmental information;

[81] Position of the European Parliament from 11.9.2013, EP-PE_TC1-COD(2012)0027.
[82] Intergovernmental agreement on the establishment of an intergovernmental fund for the European Earth monitoring programme (GMES) for the period 2014 to 2020.

- Directive 2008/56/EC establishing a framework for community action in the field of marine environmental policy (Marine Strategy Framework Directive)
- Directive 2000/60/EC of the European Parliament and of the Council establishing a framework for Community action in the field of water policy
- Directive 2008/105/EC of the European Parliament and of the Council of 16 December 2008 on environmental quality standards in the field of water policy
- Regulation (EC) No 401/2009 on the European Environment Agency and the European Environment Information and Observation Network
- Regulation No. 911/2010 on the European Earth monitoring programme (GMES) and its initial operations
- Regulation No. 2099/2002 establishing a Committee on Safe Seas and the Prevention of Pollution from Ships (COSS) and amending the Regulations on maritime safety and the prevention of pollution from ships
- Council Decision No. 779/2007 establishing a Community Civil Protection Mechanism.

The detailed assessment of the above-mentioned acts is included in the Annex.

5.3.7 Border control

Summary

The majority of data collected at present within the border control user community is collected by the individual Member State, and the existing legal framework envisages the exchange of the data in the framework of the FRONTEX Regulation and, in particular, the EUROSUR Regulation. The recently adopted EUROSUR Regulation offers a great potential in the field of border control. It seeks to establish a common framework for the information exchange and cooperation with a view to detect, prevent and combat irregular migration and cross-border crime and to contribute to ensuring the protection and saving the lives of migrants.

The EUROSUR Regulation foresees the possibility to, at national level, exchange information across functions (specifically with search and rescue, law enforcement, asylum and immigration authorities (Art. 5(3)(b)) and, at EU level, cooperate with other Union agencies, offices and agencies and international organisations (Art. 18).

The Regulation emphasises the significance of obtaining complete, and up-to-date information and for that purpose foresees the possibility to cooperate, among others, with the European External Action Service and provides expressly for the inclusion of information on military assets assisting law enforcement missions in the national situational picture (with the access possibly restricted on a need-to-know basis).

Opt-ins and opt-outs from Treaties

Denmark, the UK and Ireland have an opt-out from Title V TFEU (Area of freedom security and justice). In addition to cooperation in border control, this opt-out includes asylum and immigration and judicial cooperation in criminal matters and police cooperation (see below) and in civil matters. The UK and Ireland have the possibility to opt-in in individual matters, and they have done so in most policing and criminal law measures. Denmark, on the other hand, would have such possibility only after giving up its opt-out in accordance with its constitutional requirements.

Denmark has acceded to the Schengen *acquis* (while the UK and Ireland participate only partially with respect to criminal law and policing irregular immigration in accordance with their opt-in prerogative).[83] Regarding the area of freedom, security and justice matters, which build upon the Schengen *acquis*, Denmark has six months to decide whether to apply each such measure in its national law.[84]

As far as the FRONTEX Regulation 2007/2004 is concerned, the UK, Ireland and Denmark do not participate. Arts. 11 and 12 of the Regulation nevertheless envisage the possibility for cooperation with the UK and Ireland. The UK and Ireland are further not bound by the provisions of the Schengen Borders Code (Regulation (EC) 562/2006). Denmark acceded to the Code using its prerogative to opt-in.[85]

Detailed analysis

Following a preliminary assessment the following acts (3 Regulations) within the border control user community were identified as most relevant and, accordingly, studied in more detail:

- Council Regulation (EC) No 2007/2004 on establishing a European Agency for the Management of Operational Cooperation at the External Borders of MS of the European Union
- Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR)[86]
- Regulation (EC) No 562/2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code).

A detailed analysis of the above mentioned acts is included in the Annex.

---

[83] Protocol on the Schengen acquis integrated into the framework of the European Union, Art. 3, Council Decision 2000/365/EC concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis; Council Decision 2002/192/EC concerning Ireland's request to take part in some of the provisions of the Schengen acquis.

[84] Protocol on the position of Denmark, Art. 4.

[85] Udenrigsministeriets underretning til Europaudvalget dateret 16. april 2008 (jf. nr. 400.C.2-0).

[86] European Parliament legislative resolution of 10 October 2013, P7_TA(2013)0000.

5.3.8 General law enforcement

Summary

At European level, the majority of data within the general law enforcement user community is collected by EUROPOL within the framework of the Council Decision 2009/371/JHA. Such data include information on persons suspicious of having committed crimes and data related to investigated criminal offences. Access rights to the data are limited to the competent authorities carrying out tasks within EUROPOL's mandate. These limitations are largely justified by the applicable principles of personal data protection legislation (Council Framework Decision 2008/977/JHA).

Article 22(2) of the (EUROPOL) Council Decision provides that Europol may conclude cooperation agreements or working arrangements with EU bodies for the purposes of establishing cooperative relations as this is relevant to the performance of its tasks. Such agreements may concern the exchange of operational, strategic and technical information, including personal data and classified information.[87] To this effect, EUROPOL concluded, for example, a working arrangement with FRONTEX on 28 March 2008 (analysed above in section 4).

A Proposal for a EUROPOL Regulation[88] is currently in the legislative process. The proposal seeks, among other things, to enhance the supply of information by Member States to EUROPOL. It introduces detailed provisions governing processing of personal data and specifies the purposes for data processing. Specific rules are provided for the sharing of information with OLAF and Eurojust.

Detailed analysis

Following a preliminary assessment, the following acts (Council (Framework) Decisions) within the general law enforcement user community were identified as most relevant and, accordingly, studied in more detail:

- Council Decision 2009/371/JHA on the European Police Office (Europol)
- Council Decision 2009/934/JHA adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information
- Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.

A detailed analysis of the above mentioned acts is included in the Annex.

---

[87] The detailed procedure for concluded such agreements are laid down in Council Decision 2009/934/JHA adopting the implementing rules governing Europol's relations.

[88] Regulation on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, COM(2013) 173 final.

5.3.9 Defence

Summary

The defence user community remains under the discretion of Member States and is subject to specific rules and procedures. The EU common foreign and security policy aims to preserve peace and strengthen international security, to promote international co-operation; and to develop and consolidate democracy and the rule of law and respect for human rights and fundamental freedoms. Based on the general guidelines defined by the European Council, the Council is the institution competent to take the necessary decisions for the implementation of the CFSP, and the High Representative of the Union for Foreign Affairs and Security Policy is mandated to ensure the implementation of the Council's decisions. A major component of CFSP is the Common Security and Defence Policy (CSDP), which includes both military and civilian missions. Civilian missions include areas of police, rule of law, monitoring of borders and peace and EUSR (European Union Special Representative).

Defence activities are exempted from the vast majority of legislation governing the maritime area. There is no tradition for sharing information with other user communities, and there are no legal provisions for doing so. ESDP missions, such as the Atalanta operation, nonetheless provide evidence of the fact that a sharing potential exists even within the military missions of the defence community.

As no legislation is adopted to implement the EU CSDP, the analysis focused on various CSDP operations and documents originating from or governing e.g. the European Defence Agency (EDA)[89] and the European External Action Service (EEAS).

The legal constraints regarding the civil-military cooperation do however not hinder that voluntary initiatives are taken in order to reap the benefits from exchanging relevant information between the communities. Especially the pilot projects BlueMassMed[90], Marsuno[91] and the Maritime Surveillance in Support of CSDP[92] have shown that efficient cooperation and better understanding between civil and military authorities can lead to avoidance of duplication in many crucial areas and thus more value for the taxpayers' money.

Regarding the military surveillance efforts, it can generally be stated that the military community has a higher number of assets than other communities. CISE would therefore benefit significantly from including those assets into the exchange

---

[89] Council Joint action 2004/551/CFSP on establishment of the European Defence Agency.

[90] http://www.bluemassmed.net/index.php?option=com_content&view=section&layout=blog&id=6&Itemid=56

[91] http://www.marsuno.eu/index-8.html

[92] http://www.realinstitutoelcano.org/wps/wcm/connect/3e3e4d8042cc996b98adf95cb2335b49/The_wise_pen_team_final_report_april_2010.pdf?MOD=AJPERES&CACHEID=3e3e4d8042cc996b98adf95cb2335b49

environment. A concrete example is when a military asset detects an irregularity with direct relevance to another community. Here the receiving community would benefit from the exchange of information. The pilot projects mentioned above have found that a key limitation to information exchange concerns the fact that much data is 'over classified' and hence that there is a need for downgrading classification levels. A more operational approach to information classification has the potential for a significant improvement in impact of civil-military cooperation.

5.4 Agreements between EU agencies

The various inter-agency and cooperation agreements concluded between EU agencies have been explored in section 4.4. The assessment contained therein strengthens the baseline by providing an understanding of the scope and content of the existing information sharing arrangements and thereby helps to identify gaps between the baseline and the potential of CISE from a legal perspective.

6 Baseline: economic

6.1 Economic risks

Risks affecting maritime interests

The risk assessment presented above provides a comprehensive overview of the situations and events that may negatively affect the EU maritime domain in the forthcoming years. Regarding the economic domain, the risks affecting maritime interest are of particular relevance. These include the entry of smuggled goods and of counterfeit and pirated goods, but also piracy and disputes between regional powers.

These economic risks have been identified and assessed by maritime experts. This has partly taken place through the risk assessment presented above and partly through the use cases described in Part 2.

Economic risks on the EU agenda

In continuation of this, Part 2 explains how the economic outputs and impacts of CISE to a large extent are assessed using a bottom-up approach – i.e. through use cases. In addition, we check whether or not the economic risks or issues analysed are in line with the EU agenda.

6.2 Economic indicators

6.2.1 Maritime surveillance costs

Cost savings

A direct, expected economic benefit of CISE is cost savings in information gathering and sharing, such as the reduction of data duplication resulting from cross-sectorial information sources. Information already shared may not need to be gathered again by multiple actors). Furthermore, there are expected direct benefits from cost savings in the use of assets.

Hence, information exchange between sectors within Member States or throughout the EU/EEA may in general allow Member States to rationalise their deployment of assets and to save costs if they wish to do so through improved coordination and planning in the deployment of ships, aircrafts, etc. resulting from cross-sectorial information exchange. For instance, an authority receiving enhanced information

from other sectors or countries may be able to optimise the patrolling route for certain assets like ships, planes, helicopters. A border control plane detecting e.g. IUU fishing activities (illegal, unreported and unregulated fishing) or illegal pollution may transmit relevant information to the relevant fisheries/anti-pollution authorities thereby avoiding that the latter need to deploy further assets. Military assets such as satellites detecting illegal immigrants at sea may transmit the latter's position to search and rescue or border control authorities that may in turn carry out a targeted *rescue* operation while avoiding to engage first in a lengthy and thus costly *search* operation potentially involving several assets.

Input from the MSEsG survey

To be able to asses such cost savings, a picture of the potential cost savings is needed. This picture is partly drawn by analysing the current (and expected) maritime surveillance costs in the EU. It is, however, not straightforward to create such picture. For instance, the MSEsG survey included questions looking into the cost of current maritime surveillance, but it is difficult to provide a comprehensive overview of costs from this source of information.

Of the 14 respondents, six Member States provided no information on operational costs while nine did not provide information on investment costs. Moreover, many of the respondents who did provide information only included figures for one or a few of the relevant user communities. Hence, the cost information from the MSEsG survey cannot be regarded as accurate and is likely to underestimate actual costs. Also, the large differences that exist between the costs as reported by Member States suggest other differences. Some of these could perhaps be explained by the fact that some respondents have included cost of personnel in their figures while others have not. In conclusion, providing an accurate overall estimate on the cost of maritime surveillance based on the MSEsG survey is not possible.

That being said, it may be possible to establish a ballpark figure. For instance, it could be argued that expenses on maritime surveillance would be of similar significance in the larger EU Member States, such as France, Germany, Greece, Italy, Spain and the United Kingdom, as it would in the smaller Member States. This has also been the view of the Cooperation Project WP3 participants. Hence, relating the maritime surveillance expenses from the MSEsG survey to coastal zone GDP (based on NUTS3) of the reporting Member States, can provide a reasonable measure by which a total cost for the EU can be gauged.

Cost of maritime surveillance probably higher than EUR 5.9 billion per year.

When applying the above method on 2010 figures, the maritime surveillance *operational* expenses amount to some 0.06% of coastal zone GDP, on average, across the 23 coastal Member States, while maritime surveillance *investment* cost amount to 0.05%. As such, total maritime surveillance operational expenses amount to EUR 3.3 billion, while total maritime surveillance investment expenses amount to EUR 2.6 billion. This gives a grand total of maritime surveillance cost of EUR 5.9 billion for the coastal Member States.

Given the data foundation on which the total cost of maritime surveillance in the EU was derived, there is good reason to believe that the figure has been underestimated. For instance, considering the relatively high percentage of coastal

GDP that Italy spends on maritime surveillance compared to the average of 0.06%, the average is unlikely to be applicable to the other major EU Member States.

Cost of maritime surveillance could be EUR 8.5-9.7 billion per year.

Assuming, in light of the above, that France, Germany, Greece, Italy, Spain and the United Kingdom on average spend double the EU coastal Member State average; that is, 0.12% instead of 0.06%; and the remaining coastal Member States spend half the EU coastal Member State average; that is 0.03%, the total maritime surveillance *operational* expenditures would amount to EUR 4.7 billion. Applying a similar approach to maritime surveillance *investment* expenditures would result in a total of EUR 3.8 billion. That is, a grand total of EUR 8.5 billion per year. While these averages are in line with the results from the MSEsG survey, i.e. when categorising the responses according to the larger and smaller EU Member States; it is likely that the estimates is still undervalued. Hence, assuming the higher spending (0.12% of GDP) for all Member States we reach a cost of EUR 9.7 billion – leading to a range of cost estimates between EUR 5.9 billion and EUR 9.7 billion.

In connection with the above, it should nonetheless be highlighted that the reported investment cost appears to be unbalanced compared with the operational cost; or the other way around. Indeed, maritime surveillance investment cost comprising more than 40% of total maritime surveillance is likely to be too high. As mentioned above, this could suggest that total operational cost is still underestimated.

Potential cost savings of CISE could be substantial

Considering the fact that *all* MSEsG respondents expect CISE to deliver cost savings, and that more than of them expects the savings to be either moderate or significant, it is worth mentioning that even a 1% cost saving effect from CISE on the total cost of operations and investments, could amount to a value of more than EUR 85 million annually. Even if CISE only brings a 1% cost saving effect on maritime operational expenditures, this could amount EUR 47 million per year. A more significant impact from CISE, say a cost saving effect of 5%, would correspond to a value of EUR 236 million in operational cost savings, or EUR 426 million when including savings to maritime surveillance investments.

Additional Member State information

Information about the cost saving potential can also be gauged through other points of entry. One interesting example is information provided by Finland. In connection with the establishment of the FIMAC (Finish Maritime Authorities Cooperation), which in essence can be described as a national CISE, cost savings have been estimated (both investment and maintenance of sharing assets). Such saving estimates are provided for the cooperative use of radio communication networks for GMDSS; radars, related servers and sensors; sea cables; surveillance cameras; and AIS shore stations, VHF radio communication networks. These provide a good basis upon which ballpark savings for CISE could be established; albeit with a number of assumptions.

6.2.2 Other economic outputs

As presented in the methodology for the baseline development, other economic outputs are the economic changes that may occur as improved sharing of maritime

surveillance information – hereunder through CISE – which will improve maritime functions via more adequate, more relevant; and more timely information.

Hence, the economic baseline provides, in accordance with the risk assessment, measures of social outputs that we aim to change through CISE, and it gives thus a measure of the potentials for improvement. As for the economic outputs, it is not always straightforward to find data to measure exactly what we want to improve.

Economic output indicators

With this and the bottom-up approach in mind, Table 6-1 introduces the economic output indicators that have been selected for the description of the economic baseline; and that also comprise the foundation for analysing changes and so the added value due to the implementation of different CISE policy options. The indicators have been selected on the basis of the risk assessment presented above, which will give a comprehensive overview of the situations and events that may negatively affect the EU maritime domain in the forthcoming 15 years. Regarding the economic domain, the risks affecting maritime interests are of particular relevance. These include smuggling – hereunder of counterfeit and pirated goods, piracy, and a number of other economic risk types.

Table 6-1 Economic output indicators

Name	Definition	Rationale
Entry of smuggled goods	Number of interceptions at EU sea borders and quantity of intercepted goods. Smuggled goods here include any products entering the EU illegally (avoiding customs).	Since smuggling seeks to avoid import duties and taxes, the EU and its Member States lose revenues that otherwise could have been levied - i.e. if the goods had been legally imported." The EU loses because customs duties (in contrast to VAT, which is a national tax) are Union own resources.
Entry of counterfeit and pirated goods	Number of interceptions at EU sea borders and quantity of intercepted counterfeit and pirated goods. Counterfeit goods here include any type of IPR infringing product entering the EU.	Improved information exchange may increase the EU customs' ability to both identify and intercept the import of counterfeit and pirated goods.
Ship accidents	Number of ships involved in accidents	Improved information exchange may improve the avoidance of ship collisions. In addition, in the effect of the occurrence of such an event, information exchange may facilitate co-ordination and efficiency of actions by relevant authorities.
Piracy	Number of pirate attacks – using the definition of the United Nations Convention on the Law of the Sea (UNCLOS). Alternative indicators: › Number of pirates transferred and remanded › Number of pirates transferred and convicted › Piracy disruptions by EUNAVFOR.	Piracy affects trade routes as well as fishing activities in certain fishing grounds. Improved information exchange reduces the risk of being susceptible to piracy, as it will help crews become more cautious and alert to suspicious activities at sea. Cooperation across sectors and borders is crucial to fight piracy. The following quote from a Europol report stresses the importance of a well-coordinated effort. "A hijacked ship may be owned by a Dutch shipping company, flagged in Panama, manned by Filipinos and finally liberated by German Special Forces. Good coordination is vital to improve the effectiveness of judicial and law enforcement response."

These economic risks have been identified and assessed by maritime experts. This has partly taken place through the risk assessment presented above and partly through the use cases described in Part 2. Note that the analysis of economic indicators in Part 2 in practice has been delimited by the analysis of the Cooperation Project.

Entry of smuggled goods

The largest concern regarding the entry of smuggled goods into the EU concerns cigarettes and alcohol coming through the Eastern European border. This is the area where the European Anti-Fraud Office (OLAF), which deals with smuggling of goods into the EU, is focusing most of its efforts. According to OLAF, smuggling cases are on the rise.[93]

The 2005 amendment to the EU Customs Code provided the legal basis for the development of a common framework for risk management of the supply chain. The risk management of the supply chain, as defined in the EU Common Risk Management Framework (CRMF), involves a broad range of risks including terrorist threats and activities of organised crime, prohibited and dangerous goods, product health and safety concerns, regulatory compliance and financial risks. Operationally, the framework is underpinned by the electronic EU Customs Risk Management System (CRMS). This is the channel for wide ranging communication between Member States and systematic risk information exchange. It is available to Member State risk analysis centres, to all external border control points in the EU and to the Commission. According to the risk information exchanged within the CRMS (2011 and 2012), the main threats in terms of the entry of smuggled goods involve substantial seizures of cigarettes, narcotics, drug precursors, dangerous counterfeit goods and small arms. After the detailed evaluation of the CRMF in the area of supply chain risk management, the Commission issued Communication[94]. This was followed by Council Conclusions (insert footnote with reference: 876173/13 Rev.3 of 18. June 2013), which calls the Commission to bring forward, within a 12-month period, a coherent strategy on risk management and supply chain security.

In terms of smuggled cigarettes, statistics indicate that EU law enforcement agencies seized 4.7 billion illicit cigarettes in 2009[95]. The major origins of cigarette smuggling comprise Moldova and Ukraine, and there is a trend of Belarus and Russia becoming the main origins.

The share of the illicit cigarette market in the EU appears to be growing, i.e. having increased from 8.3% in 2006 to 10.4% in 2011.[96] This coincides with a sharp increase in consumption in the Mediterranean region, which has increased from 8.9% in 2008 to 19.3% in 2011. High illicit cigarette and tobacco consumption is also found in Member States like Ireland, France, Germany and the UK, which are

[93] OLAF (2012) Annual Report
[94] COM (2012) 793 of 8 January 2013.
[95] SEC(2011)791 final
[96] OLAF (2012) Stepping up efforts to fight against cigarette smuggling – A comprehensive EU strategy

often the main destinations for cigarettes that enter via the Eastern border. Most of the Member States are nonetheless affected by smuggling, either as points of entry, transit, or destination countries. The European Commission estimates that illicit tobacco trade is depriving Member States and the EU of over EUR 10 billion revenue every year in terms of unpaid taxes and duties[97]

There are generally two types of smuggled goods, namely (i) genuine goods, which can either be known brands or other cigarettes that are produced legitimately in the country of origin (also known as "cheap whites"); and (ii) and counterfeit goods. The entry of counterfeit goods is described in the section below; yet, it can be hard to separate the two from each other in the statistics.

The smuggling situation has changed over the last decade. In the early 2000s, for example, smuggling mostly concerned brand products, while today the majority of cigarettes entering the Eastern European border – i.e. mainly via road and rail traffic – are either "cheap whites" produced legitimately at the country of origin or counterfeits.[98]

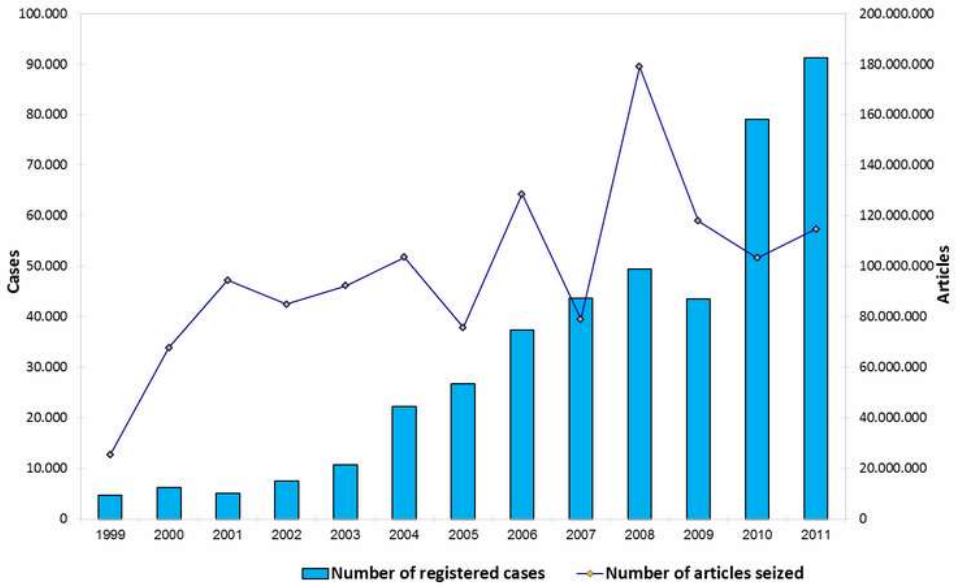
At this point, it has not been possible to find statistics on commercially smuggled alcohol.

Entry of counterfeit and pirated goods

Every year, the European Commission publishes a report describing the customs detentions of articles suspected of infringing intellectual property rights (IPR), such as trademarks, copyrights and patents. The statistics in the report are compiled on the basis of data transmitted by the EU Member States and can give an insight into IPR infringements and enable further analysis of how entry of counterfeit goods affect the EU market. The following figure depicts the evolution in number of registered counterfeit cases and seized articles.

[97] http://europa.eu/rapid/press-release_IP-13-512_en.htm
[98] SEC(2011)791 final

Figure 6-1 Number of registered counterfeit cases and seized articles



Source: TAXUD > Counterfeit and piracy > Facts and figures

The figure shows an upward trend in both the number of cases and the number of seized articles. The equivalent value of genuine products comparable to the articles seized in 2011, i.e. the domestic retail value, has moreover been estimated to be around EUR 1.2 billion.[99] Moreover, statistics published in July 2012 show an upward trend in the number of shipments suspected of violating intellectual property rights[100].

More than 92% of all counterfeit imports take place through commercial traffic, but not all shipments are seaborne. With the growth and still expanding e-commerce market, much import of counterfeit products now occurs in smaller packages and through air, express and postal traffic. As such, the majority of registered counterfeit import cases also pertain to air and postal transport, but the majority of articles seized (some 65%) are seaborne. Countries of counterfeit entry also differ significantly between Member States. As such, the top 10 Member States account for about 90% in terms of both counterfeit cases and seized articles.[101]

In terms of seized counterfeit product types, the top three categories are medicines, packaging materials, and cigarettes. Together, these categories accounted for nearly 63% in 2011.

[99] TAXUD (2012) Report on EU customs enforcement of intellectual property rights: Results at the border - 2011

[100] TAXUD > Counterfeit and piracy > Facts and figures

[101] TAXUD (2012) Report on EU customs enforcement of intellectual property rights: Results at the border - 2011

Ship accidents

Maritime accidents include a number of incidents at sea and can be distinguished in sinking, collisions, groundings, fires and others. An indication as to the current situation comes from EMSA reports[102]. In the period between 2007 and 2010, the number of vessels involved in accident dropped from 762 to 644. Collisions was the most numerous category followed by groundings, with sinking being the smallest category. According to the EMSA report, there seems to be a link between accident numbers and economic activity. There is a variation among the type of vessels involved in accidents with cargo vessels being the most numerous category in 2010 followed by passenger vessels.

Maritime accidents can have important impacts in economic, environmental as well as health terms; however, not all maritime accidents have the same impact. Reported lives lost were generally less in 2010 than 2008 (even though slightly higher than 2009) the majority in cargo and fishing vessels.

As far the geographical distribution of the maritime accidents, the EMSA report finds a distinction between the Atlantic & North Sea, the Baltic and the Mediterranean & Black Seas, with the former registering more than four times more incidents than the other two. Geography, prevalent weather conditions as well as traffic density are presented as reasons that can explain this picture. During the period under consideration, maritime accidents have been progressively reducing in the Atlantic & North Sea, the Baltic, while for the Mediterranean & Black Seas they remain more or less stable.

Piracy

Piracy is almost exclusively a problem in the Horn of Africa and other hot spots regions across the world such as South East Asia and the Indian subcontinent, Malacca Strait and Indonesia archipelago, North West Africa and Niger Delta, and Central America and the Caribbean. Despite happening 8,000 miles away from Europe, piracy in the Gulf of Aden and the Somali coast has a considerable impact on Europe and Europe's international trade. Statistics show that 15% of the world's oil production and 20% of the world's trade pass through the Gulf of Aden. Moreover, 80% of all maritime traffic through the Gulf are destined for Europe[103].

Piracy also carries a significant human cost. For example, in 2011 some 4,500 people were subjected to violent crimes by Somali pirates seeking financial gain.[104] Of these, 1,206 were held hostage for an average of eight months. Public reports show that 57% of hostages were mistreated: 174 hostages experienced extreme abuse, 371 were used as human shields, 144 were both subject to abuse and used as human shields, and 35 hostages died.

Figure 6-2 shows that, over a very long time horizon, piracy has been on the rise both in the Gulf region and in other sea basins. However,

---

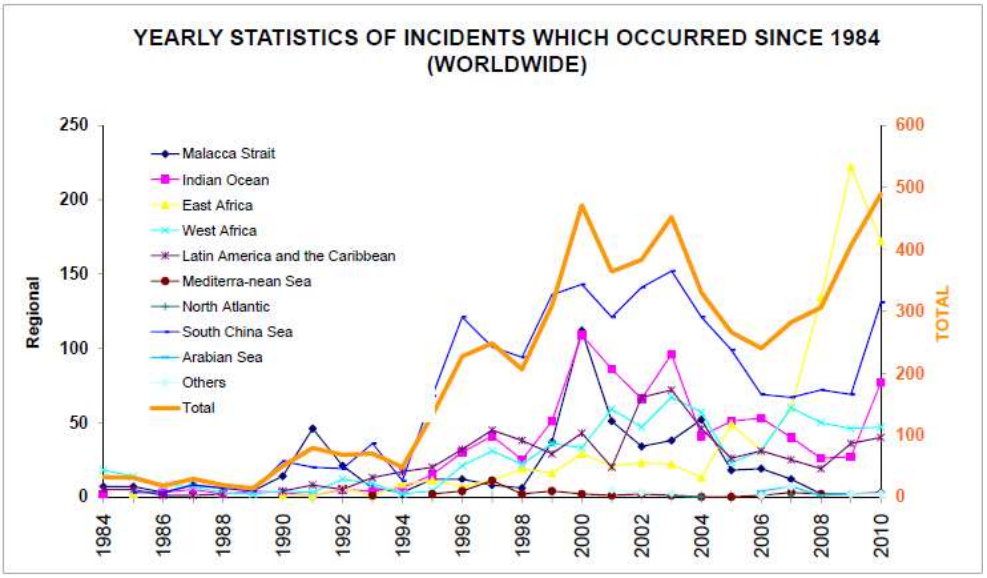
[102] EMSA (2011), Maritime Accident Review 2010

[103] Europol (2010, December 16) Joint efforts against maritime piracy, press release https://www.europol.europa.eu/content/press/joint-efforts-against-maritime-piracy-643?device=desktop, last accessed 12 July, 2013

[104] http://oceansbeyondpiracy.org/sites/default/files/hcop_2011_2_pgr.pdf

Table 6-2 below shows that due to EUNAFVOR's efforts, there was a sharp reduction in piracy off the coast of Somalia in 2012.

Figure 6-2 Yearly statistics of piracy and armed robbery



Source: IMO (2011) Report on acts of piracy and armed robbery against ships

Table 6-2 Recent piracy trend in areas under the command of EUNAVFOR

	2008	2009	2010	2011	2012	2013
SUSPICIOUS EVENTS	8	59	99	166	73	8
TOTAL ATTACKS	24	163	174	176	36	1
PIRATED	14	46	47	25	5	0
DISRUPTIONS	0	14	65	28	16	0

Source: EUNAVFOR (http://eunavfor.eu/key-facts-and-figures/)

While the efforts and results of EUNAVFOR are remarkable, they do not come without a cost. This is illustrated in the below table. CISE may nonetheless have the potential of reducing the current surveillance cost.

Table 6-3 Total cost of piracy off the coast of Somalia

Cost Factor	Total Cost, 2011
Ransoms	$160 million
Insurance	$635 million
Security Equipment and Guards	$1.064 - $1.16 billion
Re-Routing	$486 million - $681 billion
Increased Speed	$2.71 billion
Labor	$195 million
Prosecutions and Imprisonment	$16.4 million
Military Operations	$1.27 billion
Counter Piracy Organizations	$21.3 million
Total Economic Cost of Somali Piracy, 2011	**$6.6 billion to $6.9 billion**

Source: Oceans Beyond Piracy.

Other economic outputs

The risk assessment do also discusses a number of other economic outputs that could be subject to influence by CISE, but that are difficult to quantify. These include local wars in the vicinity of chokepoints; non-EU claims disputing EU's TTW/EEZ borders; disputes between regional powers affecting trade, and damage to underwater pipelines and communication cables.

6.2.3 Economic impacts

We do not estimate the total level/value of the economic impacts of activities in the maritime domain. This is neither feasible nor necessary – although in some cases – there may be concrete data for some sea basins. Instead, it is necessary to select and define the economic impact indicators that may change in value as CISE induces changes to the economic (and social and environmental) indicators. Hence, the assessment of economic impacts has been done in an incremental manner.

The economic impact indicators presented in Table 6-4 are addressed when relevant in connection with the analysis of bottom-up use cases/situations – i.e. depending on the selection of use cases/situations. Values have been put on the impacts with the use of the economic unit values (see also Part 2).

Table 6-4 distinguishes between intended and unintended economic impacts. In practice, we focus on the intended impacts as they are closely linked with the maritime domain and the economic outputs. The added value of CISE might appear in a number of other types of economic benefits. These are mainly analysed in a qualitatively manner.

Table 6-4 Economic impact indicators

Name	Definition	Rationale
Intended impact indicators		
Income from taxes/duties	Duty revenues from imported goods.	Since smuggling by definition seeks to avoid customs, EU Member States lose revenues that otherwise could have been levied - i.e. if the goods had been legally imported.
Income to businesses and from sales tax	Income to local businesses can, for example, be affected by the sales of counterfeit goods – which in turn affect income from sales taxes.	The import of counterfeit and pirated products, can lead to forgone sales by companies running a legal business – and thus sales tax incomes. The sale of counterfeit and pirated goods may also, due their sub-standard quality, lead to significant losses of brand value, and possibly market shares.
Trade	Income to the shipping industry as well as income to importers and exporters.	For example, piracy will affect trade routes and thus lead to i.e. longer shipping routes and reduced trade due to diverted shipping.
Unintended impact indicators		
Insurance prices	Insurance fees paid by shipping companies	Safer shipping, i.e. through areas prone to shipping, may lead to lower insurance fees to shipping companies.

7 Baseline: social

7.1 Social risks

Risks affecting territory and citizens

The risk assessment presented above gives a comprehensive overview of the situations and events that may negatively affect the EU maritime domain in the forthcoming 15 years. Regarding the social domain, the risks affecting territory and citizens are of particular relevance. These include terrorism (using the sea as either a base or a conduit for attacks ashore); irregular immigration, including human trafficking that endangers the internal stability of EU countries; and drugs and arms trafficking.

The social risks have been identified and assessed by maritime experts. This has partly taken place through the risk assessment presented above and partly through the use cases/situations described in Part 2.

Social risks on the EU agenda

In continuation of this, Part 2 explains how the social outputs and impacts of CISE are mainly assessed using a bottom-up approach – i.e. through use cases/situations. In addition, we check whether the social risks or issues analysed are in line with the EU agenda. While many of the social agenda goals are quite general in the sense that they pursue sustainable economic and job growth or poverty reduction and elimination of social exclusion, DG HOME has specific issues of high maritime relevance on the agenda – e.g. immigration, human trafficking and terrorism. Furthermore, DG SANCO has the protection and improvement of public health on the agenda.

7.2 Social indicators

7.2.1 Social outputs

As presented in the methodology for the baseline development, social outputs are the social changes that may occur as improved sharing of maritime surveillance information – hereunder through CISE – will improve maritime functions via more, more adequate, more relevant; and more timely information.

In accordance with the risk assessment, the social baseline provides measures of social outputs that we aim to change through CISE, and it gives thus a measure of the potential for improvement. However – as for the economic outputs – it is not always straightforward to find data that can help measure exactly what we want to improve. For example, as described in more detail below, regarding irregular immigration we would like to assess whether CISE can help rescue more immigrants at an earlier stage in order to reduce health or fatal impacts and/or to reduce the number of immigrants that succeed in entering a Member State. However, often data are only available for the number of irregular immigrants that have been refused entry into a Member State.

With this and the bottom-up approach in mind, Table 7-1 introduces the social output indicators selected for the description of the social baseline; which also constitute the basis for analysing changes and with them the added value due to the implementation of different CISE policy options.

Table 7-1 Social output indicators

Name	Definition	Rationale
Irregular immigration /human trafficking	Number of irregular immigrants, including those subject to human trafficking, refused entry at the external sea borders of the EU.	It is difficult to distinguish irregular immigration from human trafficking. The act of transporting immigrants by sea is of high health/mortality risk. Immigrants may take up irregular labour and adversely affect local labour markets in the EU.
Drug trafficking	Number of drug interceptions at sea or sea borders.	Drugs consumed in the EU are mainly produced outside the EU and mainly shipped to the EU by sea. Drug abuse has adverse health and crime impacts.
Arms trafficking	Number of small arms and light weapons (SALW) smuggled into the EU by sea.	Illegal arms have crime impacts and endanger the internal stability of EU Member States.

Irregular immigration/human trafficking

We would like to assess whether CISE can help rescue irregular immigrants at an earlier stage and/or to reduce the number of immigrants that succeed in entering a Member State. However, we have mostly data on the number of interceptions and hence refusals of immigrants.

Eurostat produces annual data on third-country nationals refused entry at EU's external borders, including sub-data on refusals at the sea borders. The most recent data are shown in Table 7-2. In the period for which data are available, this measure of irregular immigration has been relatively stable, although with a dip in 2009-10, possibly as a result of the economic crisis generating fewer job opportunities for immigrants. Italy has overtaken the place of the UK in terms of the number of third-country nationals refused at the sea border, while Estonia remains on the third place. Interestingly, those refused entry into Estonia are primarily crew members of ships docking at ports wishing to leave the ship without a valid visa.

The national figures are also qualitatively described by the National Contact Points (NCPs) of the European Migration Network (EMN) in their *Annual Reports on Migration and International Protection Statistics*, which are ultimately compiled in an annual EU synthesis report. The latest report is the *Annual Report on Migration and International Protection Statistics 2009*. Note that these figures are not directly comparable with those directly provided by coast guards (see e.g. Figure 7-1).

Table 7-2 Number of third country nationals refused entry at the EU (external) sea borders

	2008	*2009*	*2010*	*2011*	*2012*
Total refusals	**11620**	**7610**	**6770**	**10515**	**9360**
Austria	*:*	*:*	*:*	*:*	*:*
Belgium	105	60	85	35	40
Bulgaria	170	80	60	140	165
Cyprus	20	55	85	15	10
Czech Republic	*:*	*:*	*:*	*:*	*:*
Denmark	:	5	:	0	0
Estonia	1880	595	1260	1625	1220
Finland	25	0	15	20	45
France	755	580	600	970	885
Germany	40	55	150	25	15
Greece	210	385	165	225	220
Hungary	*:*	*:*	*:*	*:*	*:*
Iceland	0	0	:	:	:
Ireland	430	225	240	130	100
Italy	1445	1190	1270	4345	3210
Latvia	30	15	25	40	190
Liechtenstein	*:*	*:*	*:*	*:*	*:*
Lithuania	65	50	40	35	35
Luxembourg	*:*	*:*	*:*	*:*	*:*
Malta	5	15	0	0	5
Netherlands	95	60	65	75	85
Norway	:	15	5	15	:
Poland	40	45	50	85	75
Portugal	35	5	15	5	15
Romania	200	105	105	80	85
Slovakia	:	:	:	:	:
Slovenia	15	5	0	5	5
Spain	2785	1165	230	250	510
Sweden	5	0	0	0	5
Switzerland	*:*	*:*	*:*	*:*	*:*
United Kingdom	3265	2900	2305	2395	2440

Source: Eurostat's website under Statistics > Population and social conditions > Population > International Migration and Asylum > Enforcement of Immigration Legislation (migr_eirfs).

Note: Landlocked Member States in *italics*.

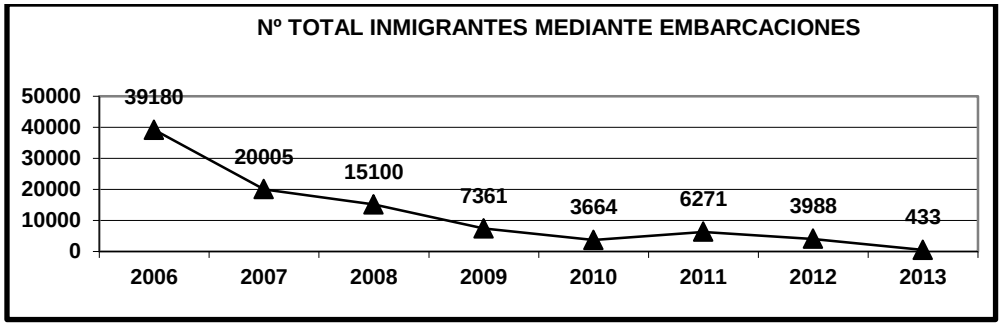
Frontex Risk Analysis Network

The Frontex Risk Analysis Network (FRAN) produces quarterly risk analysis reports containing data on illegal immigration collected by the network. These risk

analyses provide an important situational picture of illegal immigration at the EU level. Although Eurostat constitutes one of the data sources of FRAN[105], the FRAN data go beyond Eurostat data by providing information in more detail. The FRAN for example operates with alternative data such as "detected illegal entries between Border Crossing Points".

Figure 7-1 shows that the total number of rescued migrants has declined sharply since 2006 – although 2006 was a rather extreme year. Note that this measurement of irregular immigration gives much higher numbers than the ones in Table 7-2 above – i.e. the number of rescued immigrants is higher that the number of refused immigrants. A general declining trend is evident in all the cases; however the numbers are quite sensitive to political and economic events (even though with a latency effect).

Figure 7-1 Total of rescued migrants since 2006 at the Spanish coast (Canary Islands are included)



Source: Spanish Guardia Civil.

Drug trafficking

While there are no Eurostat data on drug trafficking, a European-wide assessment of drugs trade is made by the European Monitoring Centre for Drugs and Drug Addictions (EMCDDA). The data used here refer to the seizure of drugs or arrest of drug smugglers by European law enforcement authorities in EU waters or sea borders.

A wide variety of drug types enters the EU or is produced in continental Europe. Hence, to make the analysis manageable, the drug types focused on in the present study are cannabis, heroin and cocaine. The rationale for using these drugs as indicators is the fact that they predominantly enter Europe by sea.

Cocaine is the second most commonly used illicit drug in Europe. The main countries of origin for cocaine are Colombia, Peru and Bolivia. Spain and Portugal are the principal EU entry points of the drug. However, an increasing amount also enters the EU via the Western Balkans and South-East Europe.[106]

[105] http://www.Frontex.europa.eu/intelligence/strategic-analysis
[106] Europol, annual report 2011.

Table 7-3 Quantities of cocaine seized 1995-2010

Table SZR-10. Quantities (kg) of cocaine seized 1995 to 2010

Part (i) 1995 to 2010

Country		Crack included	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Belgium		Yes until 1999	576	839	3321	2088	1762	1652	:	3946	644	3522	9228	3946	2470	3852	4605	6844
Bulgaria	(1)	No	:	:	:	:	:	2	9	45	3107	1	142	144	5	10	235	30
Czech Republic		No	:	:	:	:	:	:	:	6	3	3	10	5	38	8	13	14
Denmark		Yes	110	32	58	44	24	36	26	14	104	32	57	76	88	56	72	54
Germany		No	1846	1373	1721	1133	1979	913	1288	2136	1009	969	1079	1717	1878	1069	1707	3031
Estonia		No	:	0	0	3	0	0	0.14	2	31	5	43	1	13	4	5	218
Ireland		Yes	22	642	11	333	86	18	5	32	108	167	243	195	1752	167	118	95
Greece		No	9	156	17	283	46	156	297	239	201	1152	43	57	255	67	626	221
Spain		Yes until 2003	6897	13742	18418	11687	18110	6165	33681	17617	49279	33135	48429	49650	37784	27981	25349	25242
France		No	865	1742	844	1051	3687	1311	2096	3651	4172	4484	5186	10166	6579	8215	5212	4125
Italy		Yes until 2001	2663	2387	1650	2163	2973	2368	1813	4042	3539	3589	4380	4638	3929	4132	4073	3836
Cyprus		No	3	0.004	0.02	0.02	5	58	0.1	2	10	1	1	7	2	18	2	2
Latvia		No	0.01	0.01	0.02	0.06	2	0.03	1	0.4	0.8	0.7	0.7	1	12	5	0	206
Lithuania		No	:	2	3	10	0.3	2	0.1	0.7	0.2	13	1	3	1	41	6	404
Luxembourg		Yes until 2000	0.5	13	9	6	0.3	0.4	8	2	11	4	1	4	3	6	1	3
Hungary	(2)	Yes	:	:	:	:	:	11	6	55	23	94	8	7	15	23	20	14
Malta		No	:	:	:	:	:	:	3	5	4	0.15	3	4	15	21	16	4
Netherlands	(8)	Yes	4851	9222	11495	8998	10361	6472	8389	7968	17560	12000	14600	10600	10500	:	:	10000
Austria		No	55	73	87	99	63	20	108	37	58	76	245	62	78	78	53	241
Poland		No	:	:	:	:	:	81	51	399	801	28	17	22	161	29	117	111
Portugal	(3)	Yes until 2000	2116	812	3163	625	823	3075	5574	3140	3017	7423	18083	34477	7363	4878	2697	3244
Romania	(4)	No	:	:	:	:	:	13	3	3	13	25	110	11	47	3	1283	3
Slovenia	(5)	No	:	:	:	:	:	1	1	55	2	107	2	5	42	91	3	2
Slovakia		No	:	:	10	10	3	0.2	0.4	0.07	0.9	2	0.4	1	0	379	7	0.4
Finland		No	0.07	0.07	0	2	2	39	7	0.4	1	1	1	7	4	3	3	4
Sweden	(6)	Yes	4	18	34	19	420	50	39	41	42	29	34	1358	39	66	75	35
United Kingdom	(7)	No	672	1219	2350	2962	2960	3948	2841	3566	7773	4661	3848	3280	3471	2916	2643	2387
Croatia		No	:	:	:	:	:	:	1	3	351	18	9	6	105	29	7	15
Turkey		No	:	:	:	:	:	:	2	8	3	126	81	78	116	94	89	302
Norway		No	4	24	5	93	60	12	23	36	31	41	178	41	95	76	61	94
Total			20693	32296	43196	31609	43367	26403	56272	47052	91895	71709	106063	120567	76858	54316	49100	

Notes:
A fuller historical series, back to 1985 for reporting countries, is available in the Supplementary tables section of this Statistical bulletin
Numbers are rounded to the nearest kg except for quantities less than 1 kg where more precise information is provided when available.
(1) 0.947 kg of coca leaves were also seized in 2006 and 0.336 kg in 2007; 0.596 kg Coca tea, 0.060 kg Coca leaves, 20000 kg Coca paste in 2008 and 3.638 kg coca leaves in 2009.
(2) 0.112 kg of coca leaves were also seized in 2007.
(3) In 1997 and 1998, coca leaves were also seized. Cocaine liquid was also seized in 1999. Since 2007 quatity of coca leaves seized is included in the total quatity of cocaine seized (17.9 kg in 2007 and 0.28 kg in 2008).
(4) 11.26 kg of coca leaves and 0.8 l of liquid cocaine were also seized in 2009.
(5) 1.1 ml of liquid cocaine was also seized in 2008 and 2.4 ml in 2009.
(6) Cocaine and crack are reported together (however, there are usually very few, if any, seizures of crack).
(7) Since 2007 data for Scotland are not available, see Table SZR-00 part (II)
(8) In 2010 because of possible incompleteness and unknown unreliabilities figures were truncated by the WODC. Four police regions did not report about seizures. Figures include seizures by Customs and Military Police. Figures are a 'reasonable estimation'. Also 397 cocaine balls were seized.

Source:
Reitox national focal points. See Table SZR-00 part (I) and Table SZR-00 part (II)

Source: MCDDA statistical bulletin.

According to Europol, large amounts of heroin arrive in the EU by sea. Smugglers use different routes to avoid interception.

"Much of this heroin exits Afghanistan, a major producer, via the borders with Pakistan and Iran, which offer the shortest and most direct routes to Europe. There are clear signs that, in recent years, Africa has become a major hub for heroin trafficking to Europe, no doubt in order to avoid the more extensively monitored and checked frontiers along traditional trafficking routes. From Iran, heroin is smuggled across the border into Turkey reaching Europe by travelling along the

Balkan routes. While there is a growing diversification of trafficking patterns into Europe, it remains to be the case that the Balkan route is the favoured transport channel."[107] It is estimated that about 100 tons of heroin is transported annually through the Balkans, of which 85 tons eventually make it to the most lucrative consumer market: Western Europe.

Table 7-4 Quantities of heroin seized 1995-2010

Table SZR-8. Quantities (kg) of heroin seized 1995 to 2010

Part (i) 1995 to 2010

Country		1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Belgium		149	133	65	76	74	185	:	48	51	142	270	154	548	63	275	386
Bulgaria	(1)	:	:	:	:	:	206	1545	1060	831	832	437	726	1300	1227	1183	330
Czech Republic		:	:	:	:	:	:	:	34	9	36	36	28	20	46	31	31
Denmark		37	61	38	55	96	32	25	63	16	38	27	29	48	44	22	39
Germany		933	898	722	686	796	796	836	520	626	775	787	879	1074	503	758	474
Estonia		:	:	0	1	1	0.4	1	4	0.1	0.2	0.4	4	6	0.1	4	0.004
Ireland		6	11	8	38	17	24	30	17	27	27	33	130	147	207	79	30
Greece		173	190	146	185	97	660	330	324	247	315	331	312	259	448	595	521
Spain		546	537	479	418	1159	484	631	275	242	271	174	472	227	548	300	233
France		499	617	415	344	203	444	351	476	545	558	749	1052	1036	1118	970	1088
Italy		954	1270	477	715	1310	1012	2058	2593	2592	2557	1374	1329	1897	1313	1155	944
Cyprus	(2)	:	:	:	:	2	5	2	0.3	2	3	0.9	1	1	3	0	0.1
Latvia		0.9	0	0.1	0.1	0.8	0.8	0.5	6	0.6	0.5	0.04	0.2	2	2	2	1
Lithuania		:	:	:	:	0.9	1	3	3	0.8	3	2	5	6	14	4	10
Luxembourg		13	3	3	4	2	3	1	3	4	6	4	9	9	8	5	5
Hungary		:	:	:	:	:	670	154	160	256	90	238	131	80	29	125	98
Malta		:	:	:	:	:	:	3	1	6	0.8	15	2	:	8	8	5
Netherlands	(7)	351	516	999	784	770	896	739	1122	417	1200	900	1000	520	:	:	548
Austria		47	81	102	118	78	230	288	60	43	235	282	34	117	104	190	96
Poland		:	:	:	:	:	217	389	299	7	255	41	155	124	79	86	25
Portugal	(3)	66	47	57	97	76	568	316	96	72	99	182	144	62	68	128	47
Romania		:	:	:	:	:	53	33	20	321	65	285	33	130	385	85	108
Slovenia	(4)	:	:	:	:	:	393	89	69	89	144	134	182	60	137	42	36
Slovakia		:	11	90	14	6	99	16	15	7	2	4	2	2	13	14	1
Finland		16	6	2	2	3	6	8	3	2	0.2	52	0.2	0.4	0.2	2	0.4
Sweden		31	26	12	71	64	30	32	59	13	34	19	103	30	55	31	58
United Kingdom	(5)	1395	1070	2235	1348	2346	3387	3929	2732	2732	2170	1907	1031	1059	1552	1516	732
Croatia		:	:	:	:	:	:	20	37	86	114	27	82	74	153	59	98
Turkey	(6)	:	:	:	:	:	:	3710	2657	4705	8847	8173	10312	13228	15447	16059	12690
Norway		49	74	56	38	46	52	68	59	52	129	36	93	8	55	130	102
Total		5266	5551	5906	4994	7148	10454	15606	12815	13999	18950	16522	18434	22075	23627	23859	

Notes:
A fuller historical series, back to 1985 for reporting countries, is available in the Supplementary tables section of this Statistical bulletin
Numbers are rounded to the nearest kg except for quantities less than 1 kg where more precise information is provided when available.
(1) 5658 doses of heroin were also seized in 2005, 112 in 2006, and 101 in 2007.
(2) 1.9 ml of heroin were also seized in 2007, 76 ml in 2008 and 2 ml in 2009 .
(3) There were also 5 doses of liquid heroin seized in 2001.
(4) 225.5 ml of liquid heroin was also seized in 2008 and 19.6 ml in 2009.
(5) Since 2007 data for Scotland are not available, see Table SZR-00 part (ii)
(6) 331.4 kg liquid heroine were also seized in 2009.
(7) In 2010 because of possible incompleteness and unknown unreliabilities figures were truncated by the WODC. Four police regions did not report about seizures. Figures include seizures by Customs and Military Police. Figures are a 'reasonable estimation'. Also 253 heroin balls were seized.

Source:
Reitox national focal points. See Table SZR-00 part (i) and Table SZR-00 part (ii)

Source: MCDDA statistical bulletin.

Morocco is Europe's main supplier of Cannabis. Cannabis resin from Morocco is smuggled into Europe primarily through the Iberian Peninsula, with Belgium and the Netherlands having a role in secondary distribution and storage. Recent reports

[107] https://www.europol.europa.eu/sites/default/files/publications/europolreview2011.pdf

suggest that Moroccan cannabis resin is being transited through Estonia, Lithuania and Finland en route to Russia.[108]

Table 7-5 Quantities of cannabis resin seized 1995-2010

Table SZR-2. Quantities (kg) of cannabis resin seized, 1995 to 2010

Country		1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Belgium		32582	49899	8980	818	3132	176	:	6635	5655	39921	6394	8055	58545	1529	18660	3153
Bulgaria		:	:	:	0.7	0	514	423	83	385	0.4	0.01	31	6	0.06	45	0.1
Czech Republic		:	:	:	:	:	:	:	11	65	23	5	0.5	0.4	0.7	13	9
Denmark		:	:	:	:	:	:	1763	2635	3829	1758	1406	1035	:	2914	1220	2318
Germany		:	:	7328	6110	4885	8525	6863	5003	8303	5473	3638	5606	3678	7632	2220	2144
Estonia		:	:	:	:	:	:	0.2	1	59	84	49	205	155	49	19	15
Ireland		:	1933	1248	2157	2511	380	567	3333	5350	3227	4855	6972	1235	5229	1538	748
Greece		230	833	6417	31	56	57	271	201	90	25	10209	73	5	62	47	20
Spain		:	247745	315328	428236	431165	474504	514181	564809	777546	794437	669704	459267	653631	682672	444581	384315
France	(1)	39203	35576	51664	52176	64097	48711	58196	:	78348	103705	83471	67892	34183	71076	56073	52795
Italy		:	:	:	15406	46831	20942	17605	28755	25181	15932	23199	19728	20034	34616	20311	20141
Cyprus		33	30	15	1	7	10	1	1	1	53	5	1	0.3	41	90	10
Latvia		2	2	1	3	:	:	0.2	0.4	50	0.2	2	0.4	0.3	7	1	24
Lithuania		:	:	:	:	:	:	0.3	0.6	263	2	68	106	1	35	10	271
Luxembourg		:	14	0.9	2	1	1	4	0.7	5	0.4	5	5	0.5	8	0.7	13
Hungary		:	:	:	:	:	19	0.9	3	2	3	13	3	12	3	16	9
Malta		:	:	:	:	:	4	4	10	34	33	20	45	:	23	23	43
Netherlands	(6)	:	:	:	:	:	29590	10972	32717	:	16000	5500	4600	9950	:	:	3500
Austria		:	:	:	:	109	244	138	135	239	427	151	252	164	166	192	69
Poland		:	:	:	:	:	:	13	118	47	41	19	35	33	115	17	85
Portugal	(2)	7333	5324	9621	5575	10636	30467	6473	7022	31556	28994	28258	8458	42772	61204	22966	34774
Romania		:	:	:	:	:	:	:	:	39	44	15	10	6	33	37	62
Slovenia	(3)	:	:	:	:	:	:	0.4	0.1	:	8	0.7	4	0.7	0.4	0.7	0.2
Slovakia	(4)	12	0.4	:	:	0.5	2	0.6	2	0.1	0.96	0.3	0.5	0.7	0.05	1	0.2
Finland		:	:	:	:	492	197	567	484	423	467	431	283	360	47	440	250
Sweden		495	216	626	391	1117	1182	700	820	883	820	1266	692	1379	1020	1424	702
United Kingdom	(5)	44607	66934	118854	88522	53045	48366	58999	44160	65379	64167	51017	23535	16788	31799	12563	27866
Croatia		:	:	:	:	:	:	5	2	2	6	53	12	4	5	113	3
Turkey		:	:	:	:	:	:	268	1212	816	1811	2381	2656	6302	7916	9511	29156
Norway		:	:	:	:	:	:	828	1097	2222	2093	1352	1460	668	1234	2405	822
Total		124495	408504	520082	599426	618085	663891	678844	699251	1006772	1079556	893485	611023	849916	909435	594537	

Notes:
Numbers are rounded to the nearest kg except for quantities less than 1 kg where more precise information is provided when available.
(1) In 2002 and 2003, seizures of cannabis products cannot be broken down by product; 57115 kg of cannabis were seized in 2002 and 82515 kg in 2003.
(2) The value for 1995 includes cannabis seeds. Since 2007 quantity of cannabis pollen seized is include in the total quantity of cannabis resin seized (1851.34 kg in 2007 and 58.29 kg in 2008).
(3) In 2003, seizures of cannabis resin and herbal cannabis cannot be broken down by product; 220.16 kg of herb and resin were seized in 2003.
(4) In 1997 and 1998 less than 0.1 kg were seized.
(5) Since 2007 data for Scotland are not available, see Table SZR-00 part (II)
(6) In 2010 because of possible incompleteness and unknown unreliabilities figures were truncated by the WODC. Four police regions did not report about seizures. Figures include seizures by Customs and Military Police. Figures are a 'reasonable estimation'.
Source:
Reitox national focal points. See Table SZR-00 part (I) and Table SZR-00 part (II)

Source: MCDDA statistical bulletin.

For instance, in Denmark, most of the drugs consumed arrive from outside Europe via maritime routes. "Morocco is the primary producing country of cannabis which reaches the Danish market, and Spain, Portugal and the Netherlands are the main transit countries. The vast majority of heroin is reported to originate in South-West Asia, and it reaches the national market via the traditional routes, through Iran and

[108] EMCDDA, annual report 2012

Turkey. Cocaine seized in Denmark is produced in South America and distributed via the Netherlands and Spain."[109]

Arms trafficking

In its general assembly in December 2005, the United Nations adopted the definition of SALW as any man-portable lethal weapon that expels or launches, is designed to expel or launch, or may be readily converted to expel or launch a shot, bullet or projectile by the action of an explosive.

Broadly speaking, "small arms" are weapons designed for individual use. They include, inter alia, revolvers and self-loading pistols, rifles and carbines, sub-machine guns, assault rifles and light machine guns. "Light weapons" are, broadly speaking, weapons designed for use by two or three persons serving as a crew, although some may be carried and used by a single person. They include, inter alia, heavy machine guns, hand-held under-barrel and mounted grenade launchers, portable anti-aircraft guns, portable anti-tank guns, recoilless rifles, portable launchers of anti-tank missile and rocket systems, portable launchers of anti-aircraft of anti-aircraft missile systems, and mortars of a calibre of less than 100 millimetres.[110]

Trafficking in firearms has been on the political agenda of the EU for the past decade. The following quote from Cecile Malmström, EU Commissioner for Home Affairs, in a November 2012 conference on arms trafficking, shows that illegal trafficking of weapons is considered the source of several social problems in the EU.

> *"Firearms still cause widespread death and bodily harm in the EU; they spread (more than ever before, it seems to me)* ***fear****, and* ***undermine citizens' feeling of security,*** *as they are highly visible symbols of the power of criminal groups, and they generate large* ***profits*** *for criminal groups, increasing their economic power and ability to commit other crimes."*

The Organisation for Security and Cooperation in Europe (OSCE) and the United Nations Office on Drugs and Crime (UNODC) gather data. According to the UNODC, more than 5,000 murders were committed with firearms in 2011 in the EU.[111]

Other social outputs

The risk assessment do also discusses a number of other social outputs that could be subject to influence by CISE, but that are difficult to quantify. These include terrorism at sea or using the sea as conduit, number of terrorist attacks and use of vessels with explosives or Weapons of Mass Destruction (WMD) against port facilities – since there is limited protection of major EU ports from an attack by sea; and tsunamis and storm surges that are accidental and natural risks.

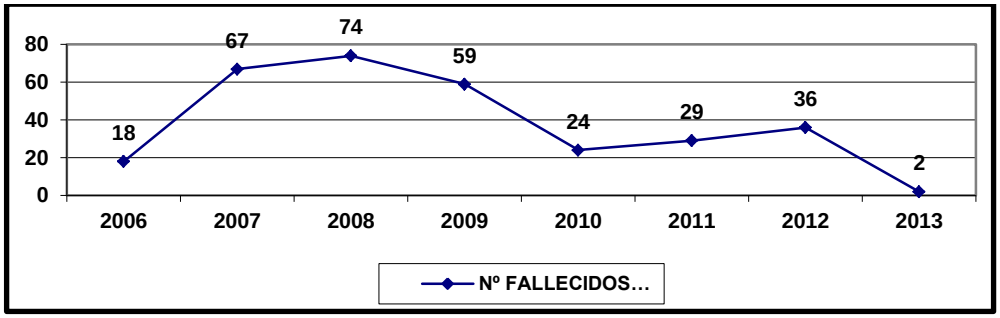
---

[109] http://www.emcdda.europa.eu/publications/country-overviews/dk#dro
[110] http://www.un.org/events/smallarms2006/faq.html
[111] http://www.unodc.org/documents/data-and-analysis/statistics/Homicide/Globa_study_on_homicide_2011_web.pdf

7.2.2 Social impacts

As for the economic impacts, we do not estimate the total level/value of the social impacts of activities in the maritime domain – such as the total health cost due to maritime events. This is neither feasible nor necessary – although in some cases there may be concrete data on some sea basins, e.g. regarding number of deaths connected with irregular immigration. Figure 7-2 shows, for example, such figures for the Spanish waters.

Figure 7-2 Total of dead bodies recovered by Spanish authorities since 2006



Source: Spanish Guardia Civil.

Note: In 2012, 22 dead bodies were found in Spanish territorial water, but the real figure is 36 because the Spanish Civil Guards (Guardia Civil) recovered 14 corpses from Moroccan territorial waters that were taken to Spain (it is compulsory to include the number in the Spanish official statistics).

Instead, it is necessary to select and define the social impact indicators that may change in value as CISE induces changes to the social (and economic and environmental) indicators. Hence, the assessment of social impacts has been done in an incremental manner – e.g. if CISE improves the performance of drug interceptions, the number of drugs entering the EU will be reduced leading to savings in health costs.

In line with the overall methodology, Table 7-6 furthermore distinguishes between intended and unintended social impacts. However, in practice we focus on the intended impacts as they are closely linked to the maritime domain and the social outputs.

Finally, depending on the use cases/situations being analysed to assess the added value of CISE, a number of other social benefits may occur. These are, however, mostly be analysed in a qualitative manner.

Table 7-6 Social impact indicators

Name	Definition	Rationale
Intended impact indicators		
Deaths	Lost human lives due to maritime events – valued via the Value of Statistical Life (VSL).	A number of the social outputs of maritime activities lead to adverse mortality impacts.
Health	Health cost due to maritime events – valued via the unit health cost/ implications of a given social output (possibly also economic or environmental outputs).	A number of the social outputs e.g. drug abuse (possibly also economic or environmental outputs) of maritime activities lead to adverse health impacts.
Crime	Crime prevention/solving cost due to maritime events – valued via the unit cost of a given social output (possibly also economic or environmental outputs).	Illegal arms have crime impacts and endanger the internal stability of EU Member States.
Unintended impact indicators		
Jobs	Lost local job opportunities, and so income, for EU nationals as a result of jobs taken by irregular immigrants – valued via a (low income) salary level.	An indirect impact of irregular immigrants entering the EU territory.

8 Baseline: environmental

8.1 Environmental risks

Risks affecting marine environment

As in the case of the social risks, the risk assessment identified the key risks and threats on the marine environment for the forthcoming years. Specifically, the assessment highlighted the following risks:

- Environmental degradation
- IUU fishing
- Illegal discharge of oily bilge and ballast water
- Risks to biodiversity
- Damage to underwater pipelines and communications cables
- Collisions, groundings, wrecks, cargo fires or explosions
- Risks to biodiversity
- Poor safety measures in offshore oil and gas platforms, and wind, wave and tidal energy farm.

The risks and threats to the marine environment were assessed against specific criteria to identify those that have a particularly high magnitude and that can be addressed largely through the implementation of CISE. This analysis was based on a consultation with experts and on information from the risk assessment, the use cases and the literature.

Environmental risks on the EU agenda

The environmental impacts to be assessed are strongly linked to the broader environmental objectives which are set by the EU environmental agenda. The assessment will inform about the contribution of the implementation of CISE to these objectives, such as protection of biodiversity, reduction of the impacts from nutrients and other pollutants etc. This contribution is not described in a great detail

but provide in the form of a general overview of causes and effects. The association of the selected risks and threats and the EU environmental agenda is illustrated in the table below.

Table 8-1 EU environmental agenda

EU environmental agenda	Pressures on fish stocks from IUU fishing	Accidental oil spills	Illegal operational oil spills	Chemical pollution
Europe 2020	X			
7th Environmental Action Plan	X	X	X	X
EU Maritime Strategy Directive	X	X	X	X
Thematic strategy for the Marine Environment	X	X	X	X
EU Biodiversity strategy to 2020[112]	X			
Common Fisheries Policy	X			

CISE and environmental objectives link

Several environmental objectives included in existing EU level environmental policies relate directly to the objectives of CISE and the different policy options for its implementation. This implies that the implementation of CISE will also contribute to achieving aims that have been set by the EU environmental agenda. Following are brief descriptions of relevant EU level initiatives that relate to similar objectives under CISE:

Europe 2020, which is the EU's strategy for smart, sustainable, and inclusive growth for the coming decade includes objectives on resource efficiency. Under Europe 2020, the flagship initiative for a resource-efficient Europe provides a long-term framework for actions in many policy areas, notably through supporting policy agendas for sustainable fisheries. CISE will in this context contribute via less use of assets, fewer search and rescue flights and so less fuel use.

The recently proposed 7th Environmental Action Plan also contains several linked objectives with CISE. These include the restoration of biodiversity, a substantial reduction of natural resource use and a better implementation of EU environment law.

The implementation of CISE would contribute to achieving many of the objectives under the EU Maritime Strategy Directive and the Thematic Strategy for the Marine Environment as CISE would help improve maritime functions via more

[112] Including full implementation of the Birds and Habitats Directive.

adequate, relevant, reliable, and timely information. The Common Fisheries Policy relates directly to achieving goals towards sustainable fisheries.

The EU Biodiversity strategy to 2020 aims to halt the loss of biodiversity and ecosystem services in the EU by 2020. These objectives relate to achieving sustainable fisheries, and preserving ecosystem services. Implementation of CISE would also contribute to fulfilling these objectives by providing the required information needs.

8.2 Environmental indicators

8.2.1 Environmental outputs

As highlighted in the description of the methodology for the construction of the baseline scenario and in accordance to the section on the social baseline, the environmental outputs represent the improvements on the environmental maritime domain that are expected to be achieved through the implementation of CISE.

Output indicators

The provision of measurable environmental outputs deriving from the implementation of CISE is a key element of the impact assessment. Similar to the social outputs, the different policy options for the implementation of CISE can act as a vehicle for the implementation of policy targets in the domain of the marine environment and also contribute to the prevention or mitigation of adverse environmental impacts deriving from harmful occurrences such as sea pollution and overfishing. The measurement of such effects has been based on selected indicators, which are monitored in the context of the EU legislation and international agreements. The fact that the selected indicators exist ensures the availability of accessible data that are necessary for the assessment of the environmental impacts. The table below shows the selected indicators and describes the rationale for their selection.

Table 8-2 Environmental output indicators

Name	Definition	Rationale
Pressures on fish stocks from IUU fishing	Number of sightings, inspections and presumed infringements detected during Joint Deployment Plans	The indicator can be applied for the monitoring of the illegal fishing activities which takes place in the sea. CISE is expected to have an effect both in terms of deterrence and better detection. Specifically it is expected that the absolute number of infringements (relative to the size of the EU fishing fleet) will drop, and at the same time the infringement ratio will increase because of improved abilities to conduct targeted inspections.
Accidental oil spills	Annual number of accidents (with > 7 tonnes of oil spilt) and volume of oil spilt in EU- 25 for accidental oil spills where > 7 tonnes of oil was spilt	Oil spills in marine areas have a significant impact on marine ecosystems. The indicator points to the effectiveness of the measures on oil-spillage prevention. CISE can lead to a more effective use of the intervention means (e.g. oil spill clean-up ships) and can enhance the planning of the required action across the various actors including EMSA.
Illegal operational oil spills	Annual number of detections and verifications of possible oil spills	The effectiveness of the mechanisms that have been set up in coastal States to track illegal discharges and to support response to accidental pollution can have a significant impact in preventing and mitigating such pollution.
Chemical pollution	Nutrients- Exceedance of the critical loads for eutrophication in Europe (as average accumulated exceedances) in 2004	The indicator provides an indication of the level of the success of the measures to reduce nutrient pollution of the marine environment. CISE can contribute to this continuous need of data to address numerous technical aspects related to the monitoring and control of chemical pollution.
	Toxic metals - Aggregated assessment of hazardous substances in biota measured in the North East Atlantic, Baltic Sea, and Mediterranean Sea (level of concentration of Cadmium, Mercury and Lead)	The monitoring of substances in the sea is carried out by several bodies and CISE can help in achieving an enhanced monitoring of these substances and in identifying emerging levels
	Persistent organic pollutant (POP) - Aggregated assessment of hazardous substances in biota measured in the North East Atlantic, Baltic Sea, and Mediterranean Sea (HCB, lindane, PCBs and DDT)	Same as above

A short description of the magnitude the current and future risks and threats is provided below.

Pressures on fish stocks from IUU fishing

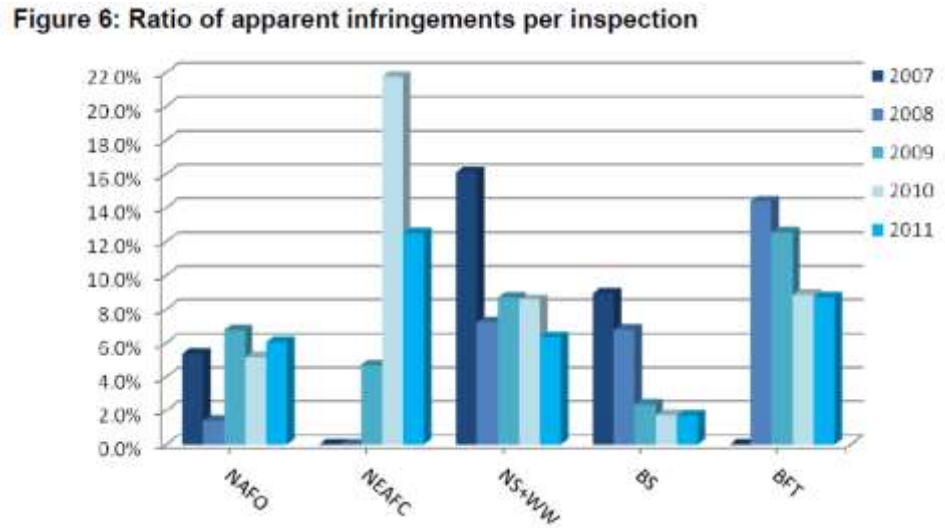
It is estimated that catches from IUU fishing represent approximately 49% of the total catches in the EU waters. This rate varies between different species and Seas. For example IUU fishing is accountable for 20%-30% of the total cod catches in the Northeast Atlantic and 40% of Bluefin tuna catches in East Atlantic and in the Mediterranean. The main impacts of IUU fishing are the fact that it undermines all efforts at national and regional levels to conserve and manage fish stocks. If IUU fishers target vulnerable stocks (which is a likely situation because of the potential better yield compared to abundant fish stocks) that are subject to strict management, this will also decrease efforts from authorities and other fishers to rebuild those stocks to healthy levels.

In January 2010 the EU implemented a certification system according to which all imported and unprocessed products are required to be certified by the flag states of the fishing vessels[113]. Further all processed products which are imported are required to have a statement by the company in the exporting country which carries out the processing. In addition, a European black list has been developed that includes IUU vessels and flag states that are considered to not address the problem adequately.

The EU certification system is considered as promising, however, the following issues have been identified:

- Difficulties in some countries to comply with the EU requirements
- Increased bureaucracy for exporting countries
- Imposition of pressures on the EU prices due to the restriction on imports.

Figure 8-1 Ration of apparent infringements



Source: Annual Report of the EFCA for 2011 (Figure 6).

According to the European Fisheries Control Agency's annual report for 2011 "Many infringements detected during 2011 were related to reporting issues. It should be highlighted that the ratio of infringements at sea and ashore has been decreasing in recent years."

[113] Commission Regulation (EU) No 395/2010 of 7 May 2010 amending Commission Regulation (EC) No 1010/2009 as regards administrative arrangements on catch certificates, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:115:0001:0024:EN:PDF

If the number of infringements is chosen as the most suitable indicator, the best baseline data available to our knowledge is produced by the EFCA in its annual reports. The data presented below is from 2011.

Table 8-3 Number of sightings, inspections and presumed infringements detected during JDP.

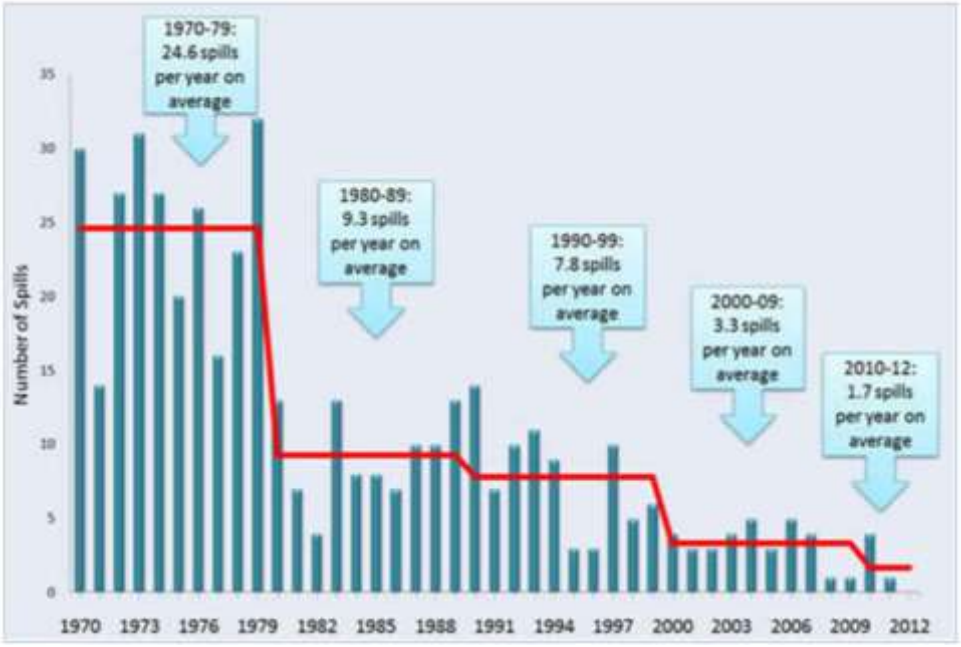
JDP North Sea & Western Waters	**Pelagic JDP Western Waters**	**JDP Baltic Sea**	**JDP Bluefin tuna**	**JDP NAFO & NEAFC**	
5268 sightings (2322 sea; 2946 air) 3978 inspections (1337 sea; 2631 ashore; 10 transport) 255 vessels with at least 1 infringement found (93 ashore; 159 sea; 3 by air surveillance) 295 presumed infringements reported (189; 106 ashore)	572 sightings (83 sea + 142 air + 347 ashore) 349 Inspections (64 sea + 285 ashore) 12 infringements (2 sea + 10 ashore)	847 sightings (710 sea + 137 air) 4720 inspections (4135 ashore + 585 sea) 80 infringement (44 ashore +36 sea)	1032 sightings 677 inspections 59 presumed infringements	83 sightings 33 sea & port Inspections 2 presumed infringements	943 sightings 112 inspections 14 presumed infringements

Due to the strong drivers and difficulties to tackle IUU fishing, it is expected that the threat will continue in the future. CISE is expected to improve maritime surveillance performance both regarding the detection and verification of suspicious fishing vessels and regarding the ability to respond to such suspected events.

Accidental oil spills

Shipping can have severe effects on the marine environment and it can affect severely ecosystem services. Oil affects marine ecosystems in several ways. Due to its consistency, oil can lead to smothering of animals, the destruction of plants. Oil spills that follow accidents account for a significant percentage of the total oil spilled worldwide. Specifically for accidental oil spills from tankers, 44% of the spills occur due to groundings, 27% due to fire explosions and 14% due to collisions. Spills of more than 20,000 tonnes account for approximately 10-15% of the total amount of oil spilled in the oceans worldwide. This share corresponds to approximately 1 billion tonnes. Below is a figure showing the decrease in the accidental large oil spills (worldwide).

Figure 8-2 Number of large spills (> 700 tonnes) from 1970 to 2012[114]



No matter the importance of the spills, between 1990 and 2005 approximately 106 accidental spills were recorded. The trend is the same worldwide as in European seas where the number of accidental oil spills continues to decrease. This achievement is mainly attributed to the phase-out of single-hull tankers that will be completed in 2015.

Nevertheless, the number of spills is still significant. Despite the decline of accidental oil spills in EU waters that has been achieved by the adoption of measures such as the phasing-out of single-hull ships, the risk of accidental oil spills remains significant, since the increasing energy demand is expected to increase the transport of oil by the sea.

Illegal operational oil spills

Shipping is responsible for a significant chemical pollution which occurs mainly in ports and across the waterways. In these areas, ships often illegally discharge oil and other polluting substances. It has been estimated that approximately 3000 illegal operational spills take place in EU waters every year.

There is a decreasing trend in illegal operational spills at least in areas where surveillance mechanisms have been implemented (e.g. in the Baltic and North Seas). For example, in 1999, 488 cases of illegal operational spills were recorded in the Baltic Sea whereas in 2008 the number of discharges had dropped to 210. Nevertheless, the significance of this illegal activity is expected to remain important also due to the increasing trend of maritime transport in the EU waters.

[114] The International Tanker Owners Pollution Federation Limited, Major oil spills (updated in 2012) , available at: http://www.itopf.com/information-services/data-and-statistics/statistics/

Chemical pollution

The marine environment can be affected by the following three main categories of chemicals: nutrients, persistent organic pollutants (POPs) and toxic metals. The risks and threats of oil pollution are described above. Nutrient pollution is a leading factor of eutrophication caused in marine waters. The eutrophication issue is created when phytoplankton and other plant forms grow excessively and cause disturbances in the marine ecosystem. Nutrient pollution has been increasing significantly mainly in the Baltic Sea and in the North East Atlantic Sea. Still, a decreasing trend is seen in the Baltic Sea and in the Mediterranean Sea, however, as mentioned above eutrophication remains a significant issue in those areas. As such, further measures need to be taken to reduce the relevant impacts and risks. POPs include pesticides such as DDT, herbicides, PCBs (a component found in many coolants, flame-retardants, adhesives), and BPA (a compound found in plastics – primarily in plastic bottles). POPs tend to accumulate in food chains through the fatty tissues and throughout the food chain, thus marine mammals around the world carry high burdens of POPs. Toxic metals are chemical elements that are typically hard, shiny, malleable, fusible, and ductile, with good electrical and thermal conductivity. Metals are toxic if they change the structure and function of proteins and enzymes.

Although practices have improved, the risk of eutrophication s continues to occur and actions to ensure better implementation of the rules are needed. In particular, the possible increase in biofuel cultivation is by some feared to lead to additional pollution. Aquaculture is also a polluter that is expected to increase in the future. The low costs of POPs for manufacturers lead many countries to continue to allow their use. Taking into account the travel ability and the persistence of POPs in the environment, pollution is expected to continue in the future.

8.2.2 Environmental impacts

Below is a description of the expected effects of improved information sharing for each environmental output.

Pressures on fish stocks from IUU fishing

The tackling of IUU fishing largely relies on the effective exchange of data that takes place during fisheries inspections. Cross-border information sharing on the position of fishing vessels enables a more effective planning, risk mapping, and increases the efficiency of the inspections[115].

The Regulation 1224/2009 allowed the exchange of information on Vessel Monitoring Systems (VMS) between different sectors and facilitated the exchange of data between different Member States[116]. Further, the Community Fisheries Control Agency (CFCA) is currently developing the network Fishnet to enhance the information sharing related to (JDP) inspections.

[115] MARSUNO (2011), Thematic report, Fisheries control
[116] MARSUNO (2011), Thematic report, Fisheries control

Nevertheless information concerning fishing licenses and special fishing permits is complex and inefficient[117]. The process is expected to gradually improve through the introduction of web services. Further, the information often lacks of details on the specific character of the risks. Such details vary between different countries due to differences on the national legislations and restrictions imposed by the intelligence. In some countries difficulties on data sharing are imposed if different authorities are responsible for fisheries inspections as there might legislative and structural limitations. Cross-sectorial data exchange is also expected to improve due to relevant requirements imposed by the Regulation 1224/2009.

Through an enhanced data exchange at inter- and intra-sectorial and well as cross-national levels, CISE is expected to improve the process of detecting IUU vessels, intelligence gathering and the cross check process. Further, CISE might also improve the overall monitoring of the illegal import chains and help develop more effective surveillance systems.

Accidental oil spills

The CleanSeaNet service was developed by the European Maritime Safety Agency (EMSA) in 2007 to monitor oil spills and to detect vessels suspected of illegal spills (see next section)[118]. The service provides information on possible oil spills, pollution alerts and information on the relevant maritime authorities, within 30 minutes. The service is operated centrally through the CleanSeaNet Data Centre that receives, manages, distributes and visualises the information. The service together with the Vessel traffic monitoring in EU waters (SafeSeaNet) can also provide emergency support in the case of accidental spills. As regards SafeSeaNet that was initiated in 2004, this initiative has a significant role in the prevention of accidental oil spills as it supports the identification of high-risk vessels in the early stages and contributes to the application of precautionary actions and risk mitigation. The initiative also allows access to standardised data and provides accurate data on the position of ships. Both of these aspects are particularly important to the prevention of and response to accidents.

For the responses to ship-sourced pollution, EMSA has established a Network of Stand-by Oil Spill Response Vessels and Equipment to ensure a continuous availability of pollution-response vessels in the case of an accident. The network operates in all European Seas and currently includes 17 vessels with an average capacity of 3,674 m^3 for recovered oil. These vessels can be mobilised simultaneously in the case of an accident.

Specifically for accidental spills, CISE can lead to a more effective use of the intervention means (e.g. oil spill clean-up ships) and can enhance the planning of the required action across the various actors including EMSA. This improvement can be achieved through the improved availability of information and the establishment of common operating procedures that are put forward through CISE. Further, CISE may allow the development of new (or the improvement of the

[117] MARSUNO (2011), Thematic report, Fisheries control

[118] EMSA (2013), CleanSeaNet, available at: https://csndc.emsa.europa.eu/homepublic

existing) common services across sectors and borders for a more effective and efficient response to accidents.

Illegal operational oil spills

The operational oil spills can be tracked through a combination of satellite and aerial observations that detect and confirm such illegal operations respectively.

As in the case of accidental spills, CISE can potentially create a better knowledge of the actual situation and to coordinate action by several countries concerned. An enhanced coordination through CISE can facilitate the verification process of the possible spills detected by CleanSeaNet. Some experience of the first generation of CleanSeaNet is available by EMSA.

Chemical pollution

Currently chemical pollution in the EU seas is monitored through numerous initiatives. At a global scale, the United Nations Environment Programme (UNEP) leads the Global International Waters Assessment (GIWA) that was developed to allow the production of an integrated assessment of international waters. The International Convention for the Prevention of Pollution from Ships (MARPOL) was established to tackle the pollution caused by accidental and operational activities of vessels. MARPOL covers pollution from various sources including chemicals, oil, waste and garbage. The Stockholm Convention was signed by 152 countries in 2001 to reduce the release of POPs to the environment. The Rotterdam Convention establishes a common responsibility and promotes joint efforts through legally binding requirements to control the trade of hazardous substances. Similarly the Basel Convention sets international requirements on the management and international transport of hazardous and other wastes.

The Regional Conventions also promote cooperation across EU and non-EU countries for the monitoring and reduction of chemical pollution in the respective regions. For example the Arctic Monitoring and Assessment Programme (AMAP) has the aim to provide information and scientific advice on the status of the arctic regions and to promote cooperative actions to prevent and remedy chemical pollution.

The EU participates actively in those international and regional initiatives and has adopted legislation on various areas which relates to the monitoring and control of chemical pollution. Most notably, the Marine Strategy Framework Directive (MSFD) puts forward the assessment of the state of the marine environment and the Water Framework Directive (WFD) establishes three types of monitoring (surveillance, operational and investigative).

Data exchange is important for the effective assessment and monitoring of chemical pollution in the sea. The evaluation of the state of the marine environment that is based on robust data, acts as a basis for the definition of the prevention and remediation measures. This process is iterative as in the light of new data, the existing measures might need to be adapted or new actions might be required.

In this context, CISE can contribute to this continuous need of data to address numerous technical aspects related to the monitoring and control of chemical pollution. The improvement and availability of information and the enhanced cross-sectorial and cross-national levels that are promoted through CISE will

potentially improve the understanding of issues that are related to chemical pollution. CISE might also reduce the duplication of efforts that currently occurs due to the monitoring requirements of the WFD, the MSFD and the regional conventions (noting that efforts are already on-going at EU level). These include the CG function of environmental rules, EMODNET, etc.

As in the case of the social impacts, the assessment of the environmental impacts has been based on the definition of environmental impact indicators. The linkages between the improved information sharing and the environmental impact indicators have been assessed based on the use cases (bottom-up approach) and on information from the literature. Depending on the availability of data, the impacts have been also expressed in monetary values.

Overall, the environmental outputs also represent the intended environmental impacts. The table below describes the environmental impact indicators that have been applied for the assessment of the environmental impacts. Specifically for the impacts from oil pollution, these are considered to be of the same nature regardless of the source of pollution (from accidents or from illegal operations). No unintended environmental impacts have been identified.

An effort was made to define the environmental impact indicators, based on the classification of the ecosystem services of the Economics of Ecosystems and Biodiversity (TEEB). According to TEEB, the ecosystem services are categorised in four different categories: provisioning, regulating, habitat or supporting and cultural services. However, this approach was abandoned since, currently, the knowledge of the benefits provided by ecosystem services is limited.

Table 8-4 Environmental impact indicators

Name	Definition	Rationale
Intended impact indicators		
IUU fishing	Depletion of fish stocks from excessive catches from IUU fishing and degradation of marine biodiversity.	IUU fishing is linked directly to the provision of fisheries and is also associated to economic and social impacts (e.g. number of jobs and turnover of the fisheries sector)
Oil pollution	Degradation of on the marine environment and ecosystem services from oil pollution	Other than the direct impacts on the marine environment, oil pollution can also have severe economic and social impacts (e.g. impacts on the tourism sector and on the recreational services)
Chemical pollution	Degradation of on the marine environment and ecosystem services from chemical pollution	Same as above

Appendix A Literature

Ahtiainen et al (2012), The value of reducing eutrophication in European marine areas — A Bayesian meta-analysis, Ecological Economics, Volume 83, November 2012, Pages 1–10

BASCAP (2011) Estimating the global economic and social impacts of counterfeiting and piracy, http://www.iccwbo.org/advocacy-codes-and-rules/bascap/

Bensassi, S. and Martinez-Zarzoso, I. (2010) How costly is modern maritime piracy for the international community? MPRA Paper No. 27134

Commuri, S. (2009) The impact of Counterfeiting on Genuine-Item Consumers' Brand Relationships, Journal of Marketing, Vol. 73, 86-98

Deloitte (2012), Study on the current surveillance IT landscape and the resulting options for the Common Information Sharing Environment for Surveillance in the Maritime Domain (CISE)

EC (1990), Commission Communication on the protection of individuals in relation to the processing of personal data in the community and information security, *COM/90/314final*

EC (1992), Regulation 2913/92 establishing the Community Customs Code

EC (1995), 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 (Data Protection Directive, *OJ L 281, 23.11.1995*

EC (1998), Council Directive 98/41/EC of 18 June 1998 on the registration of persons sailing on board passenger ships operating to or from ports of the Member States of the Community, *OJ L 188, 2.7.1998*

EC (2000a), Directive 2000/59/EC of the European Parliament and of the Council of 27 November 2000 on port reception facilities for ship-generated waste and cargo residues - Commission declaration, *OJ L 332, 28.12.2000*

EC (2000b), Directive 2000/60/EC of the European Parliament and of the Council of 23 October 2000 establishing a framework for Community action in the field of water policy, *OJ L 327, 22.12.2000*

EC (2001a), Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 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*

EC (2001b), Commission Decision of 29 November 2001 amending its internal Rules of Procedure (notified under document number *C(2001) 3031*) (2001/844/EC, ECSC, Euratom)

EC (2002a), 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*

EC (2002b), Regulation (EC) No 2099/2002 of the European Parliament and of the Council of 5 November 2002 establishing a Committee on Safe Seas and the Prevention of Pollution from Ships (COSS) and amending the Regulations on maritime safety and the prevention of pollution from ships, *OJ L 324, 29.11.2002*

EC (2003), Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC, *OJ L 41, 14.2.2003*

EC (2004a), Regulation (EC) No 789/2004 of the European Parliament and of the Council of 21 April 2004 on the transfer of cargo and passenger ships between registers within the Community and repealing Council Regulation (EEC) No 613/91 (Text with EEA relevance), *OJ L 138, 30.4.2004*

EC (2004b), 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 European Union, *OJ L 349, 25.11.2004*

EC (2004c), Council Joint action 2004/551/CFSP on establishment of the European Defense Agency

EC (2005a), Commission staff working document - Annex to the: Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters - Impact assessment {COM(2005) 475 final}, SEC/2005/1241

EC (2005b), Council Regulation (EC) No 768/2005 of 26 April 2005 establishing a Community Fisheries Control Agency and amending Regulation (EEC) No 2847/93 establishing a control system applicable to the common fisheries policy, *OJ L 128, 21.5.2005*

EC (2005c), Directive 2005/35/EC of the European Parliament and of the Council of 7 September 2005 on ship-source pollution and on the introduction of penalties for infringements, *OJ L 255, 30.9.2005*

EC (2006a), Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, *OJ L 386, 29.12.2006*

EC (2006b), 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*

EC (2006c), Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union

EC (2007), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – An Integrated Maritime Policy for the European Union, *COM(2007) 575 final*

EC (2008a), Directive 2008/106/EC of the European Parliament and of the Council of 19 November 2008 on the minimum level of training of seafarers (recast) (Text with EEA relevance), *OJ L 323, 3.12.2008*

EC (2008b), Directive 2008/56/EC of the European Parliament and of the Council of 17 June 2008 establishing a framework for community action in the field of marine environmental policy (Marine Strategy Framework Directive) (Text with EEA relevance), *OJ L 164, 25.6.2008*

EC (2008c), Directive 2008/105/EC of the European Parliament and of the Council of 16 December 2008 on environmental quality standards in the field of water policy, amending and subsequently repealing Council Directives 82/176/EEC, 83/513/EEC, 84/156/EEC, 84/491/EEC, 86/280/EEC and amending Directive 2000/60/EC of the European Parliament and of the Council, *OJ L 348, 24.12.2008*

EC (2009a), Communication from the Commission to the European Parliament, the Council, 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, *COM(2009) 538 final*

EC (2009b), Commission Staff Working Document: EU led actions relevant for the integration of maritime surveillance activities. Accompanying document to the Communication from the Commission to the European Parliament, the Council, 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 final*

EC (2009c), Impact Assessment Guidelines, *SEC(2009) 92*

EC (2009d), Directive 2009/15/EC of the European Parliament and of the Council of 23 April 2009 on common rules and standards for ship inspection and survey organisations and for the relevant activities of maritime administrations (Text with EEA relevance), *OJ L 131, 28.5.2009*

EC (2009e), Directive 2009/16/EC of the European Parliament and of the Council of 23 April 2009 on port State control (Text with EEA relevance), *OJ L 131, 28.5.2009*

EC (2009f), 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, *OJ L 343, 22.12.2009*

EC (2009g), Directive 2009/18/EC of the European Parliament and of the Council of 23 April 2009 establishing the fundamental principles governing the investigation of accidents in the maritime transport sector and amending Council Directive 1999/35/EC and Directive 2002/59/EC of the European Parliament and of the Council (Text with EEA relevance), *OJ L 131, 28.5.2009*

EC (2009h), Directive 2009/21/EC of the European Parliament and of the Council of 23 April 2009 on compliance with flag State requirements (Text with EEA relevance), *OJ L 131, 28.5.2009*

EC (2009i), Regulation (EC) No 401/2009 of the European Parliament and of the Council of 23 April 2009 on the European Environment Agency and the European Environment Information and Observation Network (Codified version), *OJ L 126, 21.5.2009*

EC (2009j), Council Decision of 6 April 2009 establishing the European Police Office (Europol), *OJ L 121, 15.5.2009*

EC (2009k), Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information, *OJ L 325, 11.12.2009*

EC (2010a), Communication from the Commission to the Council and 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 final*

EC(2010b) Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC Text with EEA relevance, *OJ L 283, 29.10.2010*

EC (2010c), Regulation (EU) No 911/2010 of the European Parliament and of the Council of 22 September 2010 on the European Earth monitoring programme (GMES) and its initial operations (2011 to 2013) Text with EEA relevance, *OJ L 276, 20.10.2010*

EC (2010d), Commission Regulation (EU) No 395/2010 of 7 May 2010 amending Commission Regulation (EC) No 1010/2009 as regards administrative arrangements on catch certificates, *OJ L 115, 8.5.2010*

EC (2011a), Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Establishing the European Border Surveillance System (EUROSUR), *COM 2011 873 final, 2011/0427(COD)*

EC (2011b), Commission Staff Working Paper, Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR), *SEC(2011) 1536 final*

EC (2012a), Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, *COM/2012/010 final - 2012/0010 (COD)*

EC (2012b), Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), *COM/2012/011 final - 2012/0011 (COD)*

EC (2013a), DG MARE, CISE – Information from Cooperation Project WP3 to COWI Impact Assessment Study: Guideline.

EC, DG MARE, Integrated Maritime Policy (IMP), http://ec.europa.eu/maritimeaffairs/policy/

EC, DG MARE, European Atlas of the Seas, http://ec.europa.eu/maritimeaffairs/atlas/seabasins/index_en.htm

EC, TAXUD (2012a), Report on EU customs enforcement of intellectual property rights, Results at the EU border – 2011, http://ec.europa.eu/taxation_customs/resources/documents/customs/customs_controls/counterfeit_piracy/statistics/2012_ipr_statistics_en.pdf

EC, TAXUD (2012b), Electronic Customs Multi-Annual Strategic Plan: 2012 Revision, Taxud.a.3 ARES (2012) 1677638, http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/e-customs_initiative/masp_strategic_plan_en.pdf

EFCA (2012, 2013), Annual Reports, for 2011 and 2012, http://www.efca.net/efca2/index.php?page=annual-reports

EFTEC (2008), Costs of Illegal, Unreported and Unregulated (IUU) Fishing in EU Fisheries, http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Protecting_ocean_life/eftec_Costs_IUU_Fishing.pdf

EMCDDA (2012), Annual Report - 2012, http://www.emcdda.europa.eu/publications/annual-report/2012

EMSA (2011), Maritime Accident Review 2010, http://www.emsa.europa.eu/implementation-tasks/accident-investigation.html

EMSA (2012), Blue Belt Service Pilot Project Evaluation report, 4 May 2012, *www.emsa.europa.eu/operations/safeseanet/download/1788/.../23.html*

EMSA (2013), CleanSeaNet, available at: https://csndc.emsa.europa.eu/homepublic

EU (2007), Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007 - PROTOCOLS - A. Protocols to be annexed to the Treaty on European Union, to the Treaty on the Functioning of the European Union and, where applicable, to the Treaty establishing the European Atomic Energy Community - Protocol on services of general interest, OJ C 306, 17.12.

EUROPOL Information Management, Products and Services, File no. 2510-271, http://www.mvr.gov.mk/Uploads/Europol%20Products%20and%20Services-Booklet.pdf

Europol (2010), Joint efforts against maritime piracy, press release https://www.europol.europa.eu/content/press/joint-efforts-against-maritime-piracy-643?device=desktop,

Europol (2011), Annual Report, https://www.europol.europa.eu/latest_publications/27

EUROSTAT (2013), database, http://epp.eurostat.ec.europa.eu/portal/page/portal/statistics/search_database

Executive Office of the President, Office of National Drug Control Policy (2004), The Economic Costs of Drug Abuse in the United States, https://www.ncjrs.gov/ondcppubs/publications/pdf/economic_costs.pdf

FEI (2012), BluemassMed Final Report, Cross-Border and Cross-Sectoral Maritime Information Sharing for a better knowledge and control of activities at sea http://bluemassmed.net/images/bmm

Garnier, B and F. Oliveri (2012), CISE Roadmap Step 2, GAP Analysis, JRC Scientific and Policy Report.

International Maritime Bureau reporting centre, http://www.icc-ccs.org/piracy-reporting-centre

LAMANS (2011) Study on information systems supporting fisheries control in the European Union, CFCA/2010/B/02.

MARSUNO (2011), Final report, http://www.marsuno.eu/PageFiles/598/Final%20Report%20111222,tryck.pdf

MARSUNO (2011), Thematic report, Fisheries control, http://www.marsuno.eu/PageFiles/598/FC1_tryck.pdf

MRAG and The Global Extent of Illegal Fishing and Fisheries Ecosystems Restoration Research, Fisheries Centre, University of British Columbia (2008), The Global Extent of Illegal Fishing, http://www.mrag.co.uk/Documents/ExtentGlobalIllegalFishing.pdf

OECD (2007) The economic impact of counterfeiting and piracy, http://www.oecd.org/industry/ind/38707619.pdf

OECD (2009) Magnitude of counterfeiting and piracy of tangible products: An update, http://www.oecd.org/industry/ind/44088872.pdf

OECD (2011), Valuing mortality risk reductions in regulatory analysis of environmental , health, and transport policies: policy implications, OECD, Paris. http://www.oecd.org/env/tools-evaluation/48279549.pdf

SKEMA Consolidation Study (2011), Methods for assessing safety and security performance, www.eskema.eu/

The International Tanker Owners Pollution Federation Limited, Major oil spills (updated in 2012), available at: http://www.itopf.com/information-services/data-and-statistics/statistics/

United Nations Office on Drugs and Crime (UNODC) (2011),Global study on homiside, http://www.unodc.org/documents/data-and-analysis/statistics/Homicide/Globa_study_on_homicide_2011_web.pdf

United Nations Office on Drugs and Crime (UNODC) (2013), World Drug Report 2012, http://www.unodc.org/unodc/en/data-and-analysis/WDR-2012.html

US Department of Transport (2008) Economic impact in the Gulf of Aden on Global Trade

Appendix B Abbreviations and definitions

Abbreviation	Full name
ABB	Activity Based Budgeting
AIS	Automatic Information System
BluemassMed	Blue Maritime Surveillance System Med, Pilot project on integration of maritime surveillance co-financed by the European Commission (COM(2010) 584 final)
CBA	Cost Benefit Analysis
CEF	Connecting Europe Facility
CFSP	Common Foreign and Security Policy
CHEN	Chiefs of European Navies
CISE	Common Information Sharing Environment for the EU maritime domain (COM(2010) 584 final)
CooP	Cooperation Project
COR	Committee of the Regions
CSDP	EU Common Security and Defence Policy
ICMPD	Centre for Migration Policy Development
DG	Directorate General
DG CNECT	Directorate-General for Communication Networks, Content and Technology (CNECT)
DG DIGIT	Directorate-General for Informatics (DIGIT)
DG ECHO	Directorate-General for Humanitarian Aid (ECHO)
DG HOME	Directorate-General for Home Affairs (HOME)
DG JUST	Directorate-General for Justice (JUST)
DG MOVE	Directorate-General for Mobility and Transports (MOVE)
DG TAXUD	Directorate-General for Taxation and Customs Union (TAXUD)
DG SJ	Legal Service (SJ)
EC	European Commission
ECJ	European Court of Justice
EDA	European Defence Agency
EDICOM	Inter-administration telematics networks for statistics relating to the trading of goods between Member States
EEAS	European External Action Service (EEAS)
EESC	Economic and Social committee

Abbreviation	Full name
EEZ	Exclusive Economic Zone
EMSA	European Maritime Safety Agency
EP	European Parliament
EU	European Union
EUMS	European Union Member State
EUR	Euro
EUROPOL	European Law Enforcement Agency
EUROSUR	European border surveillance system
FAO	Food and Agriculture Organisation (United Nations)
FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
GMES	Global Monitoring for Environment and Security
HR	High Representative of the Union for Foreign Affairs and Security Policy.
IMB	International Maritime Bureau
IMO	International Maritime Organisation
IMP	Integrated Maritime Policy
IP	Intellectual Property
IPM	Interactive Policy-Making
ISO	International Standards Organisation
IT	Information technology
IUU	Illegal, Unreported or Unregulated (Fishing)
JRC	Joint Research Centre
JTI	Joint Technology Initiative
JU	Joint Undertaking
LEA	Law Enforcement Agency
LRIT	Long-Range Identification and Tracking
MARSUNO	Maritime Surveillance in the Northern European Sea Basins, Pilot project on integration of maritime surveillance co-financed by the European Commission
MDA	Maritime Domain Awareness
MEUR	Million Euro
MoU	Memorandum of Understanding

Abbreviation	Full name
MSA	Maritime Situational Awareness
MSEsG	Member State Expert sub-Group
MSSIS	Maritime Safety and Security Information System
N/A	Not Available
NATO	North Atlantic Treaty Organisation
NGO	Non-Governmental Organisation
OLAF	European Anti-Fraud Office
PT MARSUR	Project Team Maritime Surveillance - EDA project on 'maritime surveillance network' (COM(2010) 584 final)
RMP	Recognised Maritime Picture
SafeSeaNet	Safe Sea Network; A European Platform for Maritime Data Exchange between Member States' maritime transport authorities.
SAR	Search and Rescue
SatAIS	Satellite-based AIS
SEIS	Shared Environmental Information System
SG	Secretariat-General
SOLAS	International Convention for the Safety of Life at Sea
TAG	Technical Advisory Group - Composed of representatives of all relevant maritime surveillance user communities
TEU	Treaty of the European Union
TFEU	Treaty of the Functioning of the European Union
ToR	Terms of Reference
TTW	Territorial Waters
UC	User case
UNCLOS	United Nations Convention on the Law of the Sea
USD	United States dollar
VAT	Value added tax
VDS	Vessel Detection System
VMS	Satellite-based Vessel Monitoring System used in the Fisheries sector (COM(2010) 584 final)
VSL	Value of Statistical Life
WMD	Weapons of Mass Destruction
WP	Work Package

Abbreviation	Full name
WPT	Wise Pen Team

Appendix C Risk assessment

Appendix C contains a copy of the Wise Pens International (WPI) report "Risk Assessment Study as an integral part of the Impact Assessment in support of a CISE for the EU maritime domain".

Appendix D Legal analysis

The legal analysis presented in appendix D is a copy of the updated "Draft interim report – legal mapping use groups based on legal barriers, need to know and responsibility to share (WSP 1.1) and defining legal general and specific legal barriers and EU right to act (WSP 1.2)". The report was accepted on 16 July 2013.

Regarding section 4 on policy options, please note that based on discussion with DG MARE the policy options have been updated and the section should therefore only be read as a legacy whereas Chapter 6 above is the most recent section on policy options.