
H2020 - 700478

RAdars for loNG distance maritime surveillancE and Search and Rescue opeRations

# EUROPEAN SEA BORDER SURVEILLANCE AND SHIP REPORTING SYSTEMS: CASE CISE

| | |
|---|---|
| **Deliverable Identifier:** | D2.2 |
| **Delivery Date:** | September 30th, 2016 |
| **Classification:** | Dissemination Level *(PUBLIC)* |
| **Editor(s):** | Mr. Sam Vuorinen (Laurea University of Applied Sciences) |
| **Document version**: | 1.0 - 2016 |

| | |
|---|---|
| **Contract Start Date:** | May 1st, 2016 |
| **Duration:** | 42 months |
| **Project coordinator:** | EXUS Software Ltd. (UK) |
| **Partners:** | EXUS (UK), DXT (FR), ICCS (GR), TUD (DE), LAU (FI), FNM (IT), TEL (GR), NATO (BE), HMOD (GR), DMA (FR) |

This work was performed within the RANGER Project, with the support of the European Commission and the Horizon 2020 Programme, under Grant Agreement No.700478

**Document Control Page**

| | | |
|---|---|---|
| **Title** | European Sea Border Surveillance and Ship reporting Systems: case CISE | |
| **Editors** | Mr. Sam Vuorinen | LAU |
| | | |
| | | |
| **Contributors** | Mr. Vincent Lassourd | DMA |
| | Mr. Giovanni Soldi | NATO |
| | | |
| **Peer Reviewers** | Mr. Nikos Chrisopoulos | HMOD |
| | Mr. Marco Evangelista | FNM |
| | | |
| **Security Assessment** | ☒ passed<br>☐ rejected<br>Comments: | |
| **Format** | Text - Ms Word | |
| **Language** | en-UK | |
| **Work-Package** | WP2 | |
| **Deliverable number** | D2.2 | |
| **Due Date of Delivery** | 30/09/2016 | |
| **Actual Date of Delivery** | 21/10/2016 | |
| **Dissemination Level** | Public | |
| **Rights** | RANGER Consortium | |
| **Audience** | ☒ public<br>☐ restricted<br>☐ internal | |
| **Date** | 30/09/2016 | |
| **Revision** | None | |
| **Version** | 1.0 | |
| **Edited by** | Mr. Sam Vuorinen, LAU | |
| **Status** | ☐ draft<br>☒ Consortium reviewed<br>☒ WP leader accepted<br>☒ Project coordinator accepted | |

**Revision History**

| Version | Date | Description and comments | Edited by |
|---|---|---|---|
| 0.1 | 29/06/2016 | Document draft created | LAU |
| 0.2 | 05/09/2016 | Draft version sent for review | LAU |
| 0.3 | 07/09/2016 | First Contributions | LAU, DMA, NATO |
| 0.4 | 15/09/2016 | Final Contributions | LAU, DMA, NATO |
| 0.5 | 16/09/2016 | Additional Contributions | LAU, DMA, NATO |
| 0.6 | 23/09/2016 | Final version sent for review | LAU |
| 0.7 | 29/092016 | Final version reviewed | LAU, HMOD, FNM, EXUS |
| 0.8 | 30/09/2016 | Final version uploaded in RedMine | LAU |
| 0.9 | 07/10/2016 | Additional changes made | LAU, EXUS |
| 1.0 | 15/10/2016 | Final changes made, document re-submitted. | LAU |

# Executive summary

This document focuses into the 'Common Information Sharing Environment for Maritime Surveillance in Europe' ('*CISE'/'EUCISE*') that is, according to official project documents, 'a voluntary collaborative process, across authorities and borders, to enhance and promote awareness over the European maritime domain, for the prosperity and security of the EU and its citizens'.

In a nutshell, CISE is an information sharing platform among the European Union ('*EU*') member states' maritime authorities to gather together maritime domain's surveillance data (*i.e. detection, recognition, identification*) from numerous national and independent surveillance systems in order to picturise and to maintain the best possible situational awareness, readiness and cost effectiveness from the European sea borders, sea territories and areas related (*e.g. Search and Rescue Regions*). It is worth noticing, that CISE is meant to be only a transmission tool between the different user communities, and is not storing the exchangeable data, but only exhanging it in the commonly agreed form for commonly agreed users. Each User Community remains responsible for gathering and storing its data by means of its own sectoral systems and security standards.

Based on the throughout desktop studies, the main question asked in this document is to define how the 'Radars for Long Distance Maritime Surveillance and Search and Rescue Operations' ('*RANGER*') –project would bring added value to CISE used. As for background the CISE state-of-the-art is defined in the first chapters of this document. Later this status is compared with the objectives and defined outcomes of the RANGER. Afterwards possible means for strengthening CISE are presented. Hence the system focused is both operational but intrinsically technical, and because these two aspects are not recommended to be separated in order to get the most understandable outcome of the deliverable, the point of view is also similarly two-layered.

Yet, CISE is still ongoing as a prototype, it is worth of notice that possible changes made can also affect this study. CISE is planned to be operative by 2020.

# Table of Content

# 1. Introduction – Purpose of the document

When announcing the first principal guidelines for the European Union Integrated Maritime Policy nearly a decade ago, the European Commission ('*EC*') underlined the union's immediate and indirect dependence of its surrounding waters (*i.e. oceans and seas*). Moreover, the Commission highlighted that as in many governance sectors, also EU's maritime domain has developed isolated way too long, leading partially to inefficiencies, incoherencies and disharmony of use.[1]

In its proposal for the European Union's Integrated Maritime Policy in 2007, the Commission saw that only when the clear recognition of all matters relating to Europe's oceans and seas are interlinked and sea-related policies are developing in conjunction, Europe is ready to face the challenges of globalisation and competitiveness, climate change, marine environment degradation, maritime safety and security, as well as energy security and sustainability. It was also emphasized that the three 'umbrella areas' that holds the major role to achieve the common goals at the area are the *maritime surveillance*, *maritime spatial planning* and a comprehensive and accessible *source of data and information* for all the relevant authorities and other parties.[2]

It was clear that the maritime surveillance had the highest importance in ensuring the safe use of the EU's waters and in securing its maritime borders. Several consultations and researches were launched in order to obtain the wanted clear awareness of how wide, scattered, layered and overlapping the maritime domain might be from the surveillance's point of view. Later it was clear that different sectoral authorities, all dealing with monitoring and surveillance of actions at sea, were gathering data and information for the best possible situational awareness for their *own* use. However, this situational picture was not commonly shared or did not include the information gathered by other sectoral users. This problem was not always due to the lack of personal willingness, but also because of the missing exchange platform or other resources. The Commission announced that developing the necessary means to allow such data and information exchange should enhance the different users' awareness picture and will increase the efficiency of Member States' ('*MS*') authorities and improve cost effectiveness.[3]

After several collaborative projects and surveillance system prototypes (*e.g. 'MARSUNO' and 'BlueMassMED'* [*see chapter 3*]) the idea of The Common Information Sharing Environment for Maritime Surveillance in Europe (*'CISE'/'EUCISE'*) was established. The CISE focused in this document, can be seen as the substantial step and an evolutionary product of the Commission's aforementioned proposals and the actions took. All three major areas mentioned in the guiding communication[4] are concretely in-built in CISE architecture in order to ensure the accurate decision-making and safe and secure the use of marine space.

According to the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union ('*Frontex*') the past year 2015 was marked by an unprecedented number of detections of illegal border-crossing into the EU - the migration crisis without equivalent in Europe since World War II. It should be noted that two out of three main illegal entering routes into the union main land was at the sea area: the maritime border between Turkey and Greece and the Central Mediterranean border. Solely the so called Eastern Mediterranean Route was reported 1642 percent (%) of annual increase. Third route remains at the green borders between Turkey and Greece.[5] The European Agenda on Security names terrorism, organised crime and cybercrime as the three core priorities which are highlighted for immediate action in the European Union. It is already detected that these' side effect, i.e. smuggling, irregular migration and drug trafficking goes along the Central and Eastern Mediterranean routes.[6]

Undoubtedly it is not only the mentioned growing number of illegal actions at sea that speaks on behalf of the better situational awareness, but also a fine but steady annual increase in vessel traffic volumes (*seaborne goods and passengers*) at the EU waters and visiting the union's ports that raises the demand for better readiness for surveillance and actions, like preventing illegal maritime border

crossings and search and rescue operations ('*SAR*') in general.[7] All these together justifies the need for modern and state-of-the-art surveillance and monitoring equipment.

Even though the driving factor to improve the means of union's sea domain surveillance together and between the MSs was the need for shared and real-time information picture and an environment to work and adjust that, new challenges occurs even today. These potential or already realised threats remind us, that the decisions made are still accurate but further improvement is needed in the field of maritime surveillance. As said[8], the current sea surveillance is no longer adequate to cope with these challenges, while Europe needs to have the capability to act in response to the numerous crises occurring within its maritime environment.

In this particular purpose, the European Commission's project 'Radars for Long Distance Maritime Surveillance and Search and Rescue Operations (*'RANGER'*) innovates by combining novel and ground-breaking radar technologies with innovative supporting technological solutions for early warning, in view of delivering a surveillance platform that will offer detection, recognition, and identification as well as tracking of suspicious vessels capabilities far beyond existing legacy radar systems, seamlessly fitting and contributing to the CISE framework through the provision of on-demand CISE compliant services.[9] In order to ensure that RANGER will exceed its objective, current state-of-the-art European sea border surveillance and ship reporting systems, in this paper CISE, must be assessed.[10]

This document will concentrate to report the possible means through which RANGER will strengthen CISE and this way also the security of the EU and its citizens. The document on hands will serve as a one benchmarking tool, together with other similar ones, for the RANGER project - both the objectives and the final results.[11]

## 1.1 Structure of the document

As required, the current state-of-the-art of European sea border surveillance and ship reporting systems, in this case CISE, must be assessed before any additional measures. This is fundamental in order to guarantee that RANGER has the best possible premises to reach its goals. This is also essential for mapping and comparing the added value RANGER might bring to CISE.

As it cannot be assumed that all the possible readers are highly aware of the ongoing CISE with the latest information about events and development done e.g. in the administrative level or on the field in the MS related, this desktop study offers the basic knowledge about CISE in a nutshell with the current situation updates, after defining the mandatory theoretical and methodological approach for the research itself in the *second chapter* (2nd). The formed up-to-date picture is important in order to enable and offer the fully understanding, or at least the most relevant background about the ongoing project to support any further actions and readers' mind-settings. This work is done mainly in the *third chapter* based on the policy analysis and official reports (3rd).

After defining the CISE state-of-the-art, this status is compared with the objectives and the wanted outcomes of the RANGER. As mentioned earlier, the system focused (*i.e. CISE*) is both operational but intrinsically technical, and because these two aspects are not rational to be separated in order to get the most understandable outcome of the deliverable, the point of view is also similarly two-layered. The criteria for benchmarking proposal for both the project's objectives (*improvement in vessel detection, recognition and identification*) and afterwards the final results is formed and derived e.g. from the users', infrastructure's and environment's operative and technical requirements as well from the administrative and legislative demands, mostly European Union's Maritime Security Strategy and Integrated Maritime Policy. This can be found in the *fourth chapter* (4th) and is done in collaboration with several professional entities and writers.

In order to provide a better understanding of the current state of CISE, and potential strategies to achieve the stated objective, a SWOT analysis has been undertaken. SWOT analysis is only one of many possible planning tools, used to evaluate the Strengths, Weakness, Opportunities and Threats involved in a project, or any other situation requiring a decision. This study will present the CISE SWOT analysis in practical means in the end but also the basics of the theoretical and methodological approach o the mentioned second chapter. The CISE SWOT analysis is compared to RANGER's objectives defined earlier. Afterwards, the conclusions are presented and discussed in the *fifth chapter* (5th). These should reveal by which possible means the RANGER could strengthen CISE.

# 2. Methodological approach

Usually research methods can be divided in two categories, data collection and analysis methods. The methods used for data and material collecting are typically different interviews, surveys, observations and data compilation of various archives. After this, the methods used for analysing the gathered data are usually different kinds of frequency-, frame-, and discourse- or network analysis. However, they are often linked to each other.

This paper with its content is based on the desktop study as a data collection method. By this, researchers usually mean the same as the mentioned data compilation from different archives and documents etc. that are afterwards analysed with different techniques. The method is also known as 'desk research' or 'secondary research', as it relies on already existing research and publications contrary to 'primary research' or 'basic research' in which the data are collected and produced for the first time from, for example, the certain phenomena or other research subjects.

The primary data sources used in this deliverable are mainly official and public European Commission's and other institutions' documents, such as communication between different actors and entities, written acts and directives as well as professional and expert hearings. Secondary and complementary references used are technical documents, project reviews and papers etc.

The analysis method used after the data collection is the SWOT analysis with qualitative analysis that involves the summary, collation and synthesis of the outcome. In practice, once the research subject has been objectively evaluated and discussed through the information gathered, several sides and point of views occurs. Firstly, the SWOT analysis allows to continue simplifying these aspects by categorising them with the four-angled matrix (*Table 1*).

**Table 1: The SWOT matrix** (adapted from Pahl & Richter, 2007)

| | | |
|---|---|---|
| | **Helpful**<br>(to achieving the objective) | **Harmful**<br>(to achieving the objective) |
| **Internal**<br>(attributes of the organisation) | Strengths<br>*(S)* | Weaknesses<br>*(W)* |
| **External**<br>(attributes of the environment) | Opportunities<br>*(O)* | Threats<br>*(T)* |

According to Pahl and Richter[12], the SWOT analysis' four angles or criteria typically presented are:

- (*S*) Strengths; that are internal attributes of the actor which helps to achieve the objective(s).
- (*W*) Weaknesses; that are internal attributes of the actor which are harmful to achieve the objective(s).
- (*O*) Opportunities; that are external conditions which helps to achieve the objective(s).
- (*T*) Threats; that are external conditions which are harmful to achieve the objective(s).

In each category, there might be several strengths, weaknesses, opportunities and threats but is also possible that some of the four angles is missing or inadequate. Usually when all the discoverable attributes are recognised and categorised from the research object, later in this study CISE, they are used for future development or concrete error correction by asking and answering the following four questions:

- How can we use each (*S*) strength?
- How can we beat each (*W*) weakness?
- How can we exploit each (*O*) opportunity?
- How can we defend against each (*T*) threat?

The actual analysis in this document is done when these questions are asked in the light of the project objectives and the main question presented in the first chapter that is also the priority purpose of this study: 'how will RANGER strengthen CISE?' Sub questions to this in SWOT's focus might be the following four:

- How can RANGER use each (*S*) strength in CISE?
- How can RANGER beat each (*W*) weakness in CISE?
- How can RANGER exploit each (*O*) opportunity in CISE?
- How can RANGER defend against each (*T*) threat in CISE?

To gain the full benefits of SWOT, the analysis should firstly provide information that helps in decision making. Secondly, it should be remembered along the way, that the first two attributes are, as written, internal as well the last two are external. For example, what do we do better in RANGER than anyone else (*strengths*) and where should we take the advantage of RANGER (*opportunities*) etc. If the following questions are not asked and the SWOT analysis is only used for revealing and listing the four attributes, it is not very useful and rarely leads in any long-lasting solutions.

As mentioned earlier, SWOT analysis is only one of the many possible evaluation tools. However, it is chosen here because it already offers an easy-to-understand visual matrix and relevant supporting questions. In this study, the SWOT analysis concentrating solely to CISE is presented first which after it is compared to RANGER's defined objectives. However, they are in-written in the same matrix so that they can be easily compared. (*see chapter 5*). Afterwards, the conclusions are presented and discussed through the SWOT-based questions. These should reveal the areas and possible means by which the RANGER could strengthen CISE.

The second analysis method used together with SWOT is the qualitative analysis that is said to be an inductive reasoning where understanding of the object is done via the seen large phenomena and patterns – and vice versa, these patterns are tried to be understood through the smaller affecting particles found in them. In this certain case study, the larger patterns (*e.g. political, economic*) are tried to be revealed by scanning the official documents etc. which after answering the above mentioned SWOT questions the smaller objects might be revealed which complement and confirm the conclusions made. So, qualitative analysis should complete the SWOT analysis as it is even more objective when admitting that every perspective is worth of study, how things look from different angles before making any stronger conclusions.[13]

# 3. Description of CISE

A clear, simple and at the same time all-inclusive definition of CISE cannot be done only by few sentences. In this chapter the administrative milestones and background are presented in order to provide the reader a better understanding of the CISE present situation.

As the European Council had already in 2006 announced that when improving and strengthening the overall management of the border control and surveillance at the European Union's external borders, the "priority will be given to examining the creation of a European Surveillance System for the southern maritime borders".[14] After this the importance of the common, integrated and non-overlapping surveillance of the EU's maritime domain was truly recognised and approved in the European Union's Integrated Maritime Policy late 2007 (*see chapter 1*).

Right in the beginning of 2008, the Commission communicated with several important EU entities about the creation of a European Border Surveillance System ('*EUROSUR*'), which at the same time foresaw the first steps of forming a Common Information Sharing Environment for the EU maritime domain ('*CISE*').[15] This sequence was right as the maritime surveillance was seen as a major part of the overall European border surveillance according to the mentioned year 2006 Council announcement and since.

When planning the basis and general concept for EUROSUR the Commission underlined that it should support the Member States in reaching the full situational awareness of their external borders and should also increase the reaction capability of their law enforcement authorities. In order to meet the objectives the Commission established three main phases in EUROSUR. These were:

- "PHASE 1: Upgrading and extending national border surveillance systems and interlinking national infrastructures in a communication network.
- PHASE 2: Targeting research and development to improve the performance of surveillance tools and sensors (e.g. satellites, unmanned aerial vehicles / UAVs, etc.), and developing a common application of surveillance tools. A common pre-frontier intelligence picture could be developed to combine intelligence information with that obtained from surveillance tools.
- PHASE 3: All relevant data from national surveillance, new surveillance tools, European and international reporting systems and intelligence sources should be gathered, analysed and disseminated in a structured manner, to create a common information sharing environment between the relevant national authorities."[16]

It was also clearly said that the "phase 3 should focus on the maritime domain, as it concerns putting together the multitude of information sources that are monitoring activities on the open seas; the equivalent challenge of monitoring such a vast space does not arise in relation to land borders"[17].

The Commission also clarified in details that there should be two major steps to take under the phase three (*PHASE 3*), which were:

- "Step 1 (*originally '7' in Commission's worksheet*): Integrated network of reporting and surveillance systems for border control and internal security purposes covering the Mediterranean Sea, the southern Atlantic Ocean (Canary Islands) and the Black Sea.

- Step 2 (*originally '8' in Commission's worksheet*): Integrated network of reporting and surveillance systems for the whole EU maritime domain."[18]

Also two different targets were set: firstly, the plan for further steps towards the integration of all European maritime reporting and surveillance systems should be established and secondly, an outline for the system architecture for an integrated network of reporting and surveillance systems for the Mediterranean Sea, the southern Atlantic Ocean (Canary Islands) and the Black Sea should be formed. In 2008 the certain sea areas mentioned were the most problematic from illegal border crossings' point of view. That is why the first actions were targeted namely there. These areas were also in a need of better surveillance coordination as the event density was noted.

The above mentioned declarations and targets were the real starting point for CISE's predecessor projects and later on for CISE itself. The concrete development could begin.

In the spirit of the mentioned EUROSUR general concept's phase three (*PHASE 3*) about the creation of the common information sharing environment and in order to navigate firmly on the right course straight from the beginning, Commission established the guiding principles towards the integration of maritime surveillance a year after, in 2009. In this document, the common information sharing environment for the EU maritime domain was officially defined for the first time. CISE's different components were first explained in order to avoid misunderstandings among the EU-wide project participants:

- "Common: As the information is to be shared between the different user communities, data used for this information should be collected only once.
- Information must enable user-defined situational awareness. Coming from disparate user communities, information should be identifiable, accessible, understandable and usable. Processing such information with the appropriate security safeguards must be ensured.
- Sharing means that each community receives but also provides information on the basis of previously agreed standards and procedures.
- Environment refers to interconnected sectoral information systems that allows for users to build up their specific situational awareness pictures, which enable them to identify trends and detect anomalies and threats."[19]

Commission's demandings also were that CISE should ensure:

- Interoperability: Ways should be found to enable the information exchange between sectoral systems both operational and those currently being developed by the EU its agencies and the MS. This requires that existing and future system solutions are developed enabling information sharing and the protection of information shared on the basis of agreed access rights.
- Improving situational awareness: The information obtained in this environment should considerably improve the situational awareness within the EU and its MS.
- Efficiency: The sharing environment should contribute the unity of effort across maritime entities by avoiding duplications in the information collection and by this to reduce the financial costs for all actors involved.
- Subsidiarity: Member States are responsible for coordinating the collection and verification of information from all their national sources, preferably via a single national coordination mechanism. MS will also, where applicable, manage third party access rights, qualify the information and data security levels, and approve and control the selective dissemination and data security mechanisms.[20]

**CISE principles**

As a conclusion, the detailed principles for CISE were written including guiding issues and recommendations to be considered. The principles were as follows:[21]

**Table 2: Commission's principles for CISE** (adapted)

| GUIDING ISSUES | RECOMMENDATIONS |
|---|---|
| **Principle 1: An approach interlinking all user communities** | |
| **A flexible information sharing environment**: participants having access to as much information as possible and building up an individual situational picture that meets their operational requirements | **No data duplication:** traffic monitoring data should be disseminated only once and could then be made available to all recognised users |
| **Providing comprehensive information for better decision making:** all communities has to contribute, all existing databases should be linked | **Interoperability across EU user communities:** interoperability and connectivity of all relevant actors at national level |
| | **National coordination:** better governance of maritime surveillance should be achieved first at national level. Already identified information hubs should serve as interfaces for the common information sharing environment |
| | **International and regional cooperation:** even building up interfaces within the EU maritime interfaces, care should be given to the potential of sharing selected information with third countries |
| **Principle 2: Building a technical framework for interoperability and future integration** | |
| **Interoperability and interconnection of systems:** instead of putting all the information together into a single database, each user should make its data accessible to other users who need it | **Technical framework:** architecture should be designed as a cost effective interconnection of different information layers based on interoperability and common standards. Interoperable data models and standards on handling data have to be agreed and secure communication lines have to be established between relevant data users based on pre-defined access rights |
| **Use of a Community based system:** for certain information (e.g. departure and arrival information), it is easier and more cost-efficient to collect and disseminate the data in a centralised manner | **Interoperability and common standards:** the best technical solution for service synchronisation, data quality and standard methodologies for vocabulary and data exchange building-up on best practices is needed |
| **Use of sectoral systems for the sharing of classified information:** for certain categories of information (e.g. intelligence related), a sectoral approach is needed to safeguard the security interests of the concerned user communities or recipients | **EU Agencies:** relevant EU Agencies play an important supportive and coordinative role within their user community. They could also serve as hubs for the information exchange if needed. |

| | |
|---|---|
| **Regional approaches:** MS should consider developing capacity for a joint situational awareness of legal and illegal activities at sea which would contribute to an improved regional reaction capability | |

| **Principle 3: Information exchange between civilian and military authorities** | |
|---|---|
| **Military gathered information and capabilities:** the support of MS' military forces to civilian-led maritime safety and internal security missions is important and vice versa. Defence capabilities (e.g. operation of unmanned platforms, the detection and analysis of underwater sounds) are valuable for civilian use also | **Enhanced coordination:** a close coordination between the EC, MS and those who the European defence community may indicate for this purpose should be established. Translating this enhanced coordination into policy orientations will be done in full respect of each user community's legal framework. |
| | **Better use of surveillance tools across communities:** authorised civilian and military users should be enabled to task and to receive data from European surveillance tools for the purpose of maritime surveillance |
| | **Space generated data:** the use of space assets can support operations carried out by civilian and military authorities |

| **Principle 4: Obstacle-removing from specific legal provisions** | |
|---|---|
| **Processing of personal data:** the different above mentioned activities needs personal data processing. Laws and regulations regarding to this are observed in the framework of the CISE | **Data protection:** any mechanism aiming at the cross-border exchange of data from various existing databases is made subject to defining at least the nature of the data involved, the capability of the data providers, the purposes (and the methods) of the exchange and the potential recipients of the data, as well as incorporating the necessary safeguards with regard to the confidentiality and security of data and the protection of personal data, where this may be relevant |
| **Confidentiality requirements:** a significant amount of maritime reporting and surveillance data is qualified and/or has to be treated as confidential. The processing and transferring of this type of data needs to be ensured that recipients are equally bound by confidentiality and professional secrecy obligations | **Processing of personal data:** the processing of personal data for military, State security and criminal law enforcement currently remains outside of the general legal framework for data protection. However, data protection may be addressed on an ad hoc basis in specific legal instruments in these fields, both at Community and Member State level but additional safeguards will be required in case it would be envisaged to share personal data between authorities falling within the scope of the existing legal framework for data protection and authorities falling outside that scope |
| **Civil/military data sharing:** with regard to a possible information and data exchange between different authorities, it has to be examined how the integrity of classified information, confidential business data, information related to criminal investigations and the protection of personal data can be guaranteed | |

As seen above, a large groundwork was made at the Commission level before any concrete work within CISE was started. These principles led the way for the future work while planning CISE's frames and functionalities.

**CISE Six Step Roadmap**

Later this same approach was confirmed in the CISE roadmap which' draft Commission presented in October 2010. This six step (*table 4*) draft roadmap to establish the CISE was further detailed in 2011 when the results of the CISE pilot projects were taken into account (*see lower)*. However, it was already admitted in 2010 that one single technical solution will highly unlikely fit each and every exchange of information within the CISE.[22]

**Table 3: The mutually agreed six steps of CISE roadmap** (adapted)

| |
|---|
| 1. Identifying all user communities |
| 2. Mapping of data sets and gap analysis for data exchange |
| 3. (Defining) Common data classification levels |
| 4. Developing the supporting framework for the CISE |
| 5. Defining access rights |
| 6. Providing a coherent legal framework |

The roadmap and its steps are further analysed in the RANGER project deliverable number D3.5. 'Report on CISE's Roadmap, Policies and Practices in Maritime Surveillance'.

CISE did not start immediately as an own project or developing concept when the principles and roadmap steps were first established. As it was mentioned already in the Commission's document regarding the three main phases in creation of EUROSUR, the first step to take in phase three was to focus to create better and integrated network of reporting and surveillance systems covering the Mediterranean Sea, the southern Atlantic Ocean (Canary Islands) and the Black Sea as it was the most problematic area at that time. The creation of this network and its lessons learned would bring added value to CISE beforehand as there was an urgent need for better surveillance in these areas. Solely in 2008 when the EUROSUR document was written, more than 760 persons[23] were illegally crossing the border from Africa to the Canary Islands (EU) each month. Numbers were even more alarming through the Mediterranean Sea, almost 8300 persons[24] each month.

In order to answer the need for more effective and integrated sea surveillance and to learn from the field, Commission called several project proposals right from the year 2008.[25] Some of the projects were collecting the vital experience from other sea areas than Mediterranean as well. For example, the BlueMassMED[26] started in 2008 was the first European maritime surveillance pilot project, whose target was to catalyse and promote cooperation in maritime information sharing between 37 different state partners from six Member States bordering the Mediterranean Sea and the Atlantic approaches. Also other EU Commission's project, MARSUNO[27] started 2009, was a step towards achieving the aims to render existing monitoring and tracking systems more interoperable between coastal Member States to the Northern European Sea basins and the COOPP-project[28] started in 2011 aimed to support further cross-border and cross-sector operational cooperation between public authorities (including EU Agencies) in the execution of the defined maritime functionalities, with a focus on information sharing across sea basins.

All the mentioned first European maritime surveillance related projects were in relation with the future developments of CISE. As we can compare the CISE's principles and the main objectives

in these projects, their outcomes and weak areas spotted supported the process of creating a Common Information Sharing Environment (CISE). They also showed the way for more collaborative The European test bed for the maritime Common Information Sharing Environment in the 2020 perspective ('*EUCISE2020*') - project to come (*see chapter 3.1*)

CISE architecture should be descriped as a 'cost effective decentralised interconnection of different information layers that increases efficiency of maritime surveillance systems by filling existing information gaps across Europe while avoiding data duplication'[29]

**Table 4: EU Milestones for CISE Development from DEC2006 onwards**

| | |
|---|---|
| 2006 | The European Council Meeting in December 2006 agrees the improvement of the management of the European Union's external borders, where the priority was given to examining the creation of a European Surveillance System for the southern maritime borders. |
| 2007 | European Union's Integrated Maritime Policy |
| 2008 | Examining the creation of a European Border Surveillance System (EUROSUR), where maritime surveillance was emphasised. / BlueMassMED-project |
| 2009 | Guiding principles for a common information sharing environment for the EU maritime domain (*CISE*) / BlueMassMED and MARSUNO -projects |
| 2010 | CISE Draft Roadmap,<br>BlueMassMED and MARSUNO -projects |
| 2011 | BlueMassMED, MARSUNO and COOPP -projects |
| 2012 | BlueMassMED and COOPP -projects |
| 2013 | COOPP -project |
| 2014 | European Union Maritime Security Strategy (*EUMSS*) & Action Plan / COOPP and EUCISE2020 –projects |
| 2015 | EUCISE2020 -project |
| 2016 | EUCISE2020 -project |
| 2017 | EUCISE2020 –project (*ends*) |

## 3.1 The current situation of CISE at the EU level

This chapter presents the main actions taken and ongoing at the EU level in order to support the successful cooperation between all relevant actors and entities in the preparatory work and to enable the best possible ground for operative CISE by 2020 as well as to detect all possible barriers that might still exist. As there is much done at the EU level, equally important and related ground work is ongoing in the Member States. These actions are described in more detail in the RANGER project deliverable number D3.5. 'Report on CISE's Roadmap, Policies and Practices in Maritime Surveillance'. As some of these actions might contain restricted information, the deliverable is not public.

**EU CISE 2020**

Currently CISE environment architecture and relevant exchange solutions are under progress and tested with selected expert partners. To help that to proceed, The European test bed for the maritime Common Information Sharing Environment in the 2020 perspective ('*EUCISE2020*') – project started in the 1st of December 2014. The EUCISE2020 is a Commission funded project lasting up to the second half of 2017. The main aim is to offer a test environment for CISE functions on a large scale, in particular between civilian and military authorities. The project takes as reference from different factors in the field of EU maritime surveillance, legal framework, as well as from studies, pilots and projects accomplished in the last three years. In particular the project is based on:

- CISE Roadmap based on the official EU documentary
- The results of pilot projects BluemassMed, MARSUNO and COOPP mentioned
- Several advisors at the area
- The European studies on maritime surveillance already carried out
- The results of security research projects in progress
- The need of innovation expressed by the maritime stakeholders arising from their operational experience in managing maritime surveillance processes and systems at European, international and national levels.[30]

The activities of EUCISE2020 are implemented and managed by a consortium of 37 partners from 15 different European countries including maritime authorities, universities, research institutes and other different organisations. The project attains the widest possible experimental environment of innovative and collaborative processes between European maritime institutions The objective is to create a political, organisational and legal environment to enable information sharing across the seven relevant sectors/user communities (*transport, environmental protection, fisheries control, border control, general law enforcement, customs and defence*) based on existing and also on future surveillance systems/networks to achieve a fully operational CISE by 2020.[31]

However, it has already been admitted that one single technical solution will highly unlikely fit each and every exchange of information within the CISE. Related to this and the above mentioned EUCISE2020's leading role for the design, implementation and testing the common environment with maritime surveillance entities, the main idea still remains that all existing national systems and IT solutions at the surveillance field from all relevant sectors can become interoperable in the context of future Maritime CISE. That is why CISE is meant to be only a transmission tool between these different user communities' systems and solutions not storing the exchangeable data, but only exhanging it in the commonly agreed form for commonly agreed users. Each User Community

remains responsible for gathering and storing its data by means of its own sectoral systems and security standards. But when offering the relevant data to common use through the CISE environment and vice versa when receiving any data inside the CISE network, it must be gonethrough commonly afreed trustworthy security standards while receiving its present classification level.[32]

At the EU downs to national MS level the priority areas focused at this point in order to enable the further cross-border and cross-sectoral cooperation as well the smooth as possible integration of already existing surveillance systems and IT solutions to CISE are (*identified also by the MARSUNO, BlueMassMed and Cooperation project mentioned above*):

- "Real-time sharing of positions of patrol vessels and aircrafts and functional specifications to ensure the fastest possible response to mass rescue operations and/or other events at sea,
- Collaborative tools for cross-border crisis management,
- Data consolidation and exchange of information on suspicious vessels navigating in EU waters, and
- National registries of recreational boats: computerised processing of information requests between Member States"[33]

**Additional CISE Actions Ongoing**

In parallel and addition to the launched EUCISE2020 to lead the implementation work, the Commission has also took many other further actions.

First of all, as the future CISE will be new-fangled and different not only visually but technically as well as operationally and undoubtedly rise several questions among the User Community despite the meticulous preparation work, the Commission started to develop a nonbinding Maritime CISE handbook in close co-ordination with Member States. The handbook should be published by the end of 2016.

The CISE handbook will offer i.a.:

- Best-practice recommendations and useful information on how to apply Maritime CISE.
  - Recommendations are amongst other things intended to promote a "care to share to be aware" -culture across and between different sectors among national authorities involved in maritime surveillance.
- Guidance on the recommended handling of personal or commercially sensitive information by the relevant authorities.
  - Best practices on information sharing and technical and operational guidelines

The handbook takes into account the results of various preparatory actions and pilot projects mentioned with the EUCISE2020 above as well the EUCISE2020 itself, other related projects funded under the Integrated Maritime Policy Programme (IMP), FP7- and Horizon2020 – programmes[34] among others.[35]

When ready, such a handbook may be formally adopted by the Commission in the form of a Recommendation. By this action, the handbook may also, amongst the above mentioned more detailed outcomes:

- Generally encourage Member States' maritime surveillance authorities to exchange information across borders and across user communities if some doubts still remains. This may increase cooperation among authorities on a voluntary basis, not forced by the EU.
- Provide a standard form for a Memorandum of Understanding (MoU) among the Member States' maritime surveillance authorities regarding the conditions for information sharing and the use of the data shared.
- Address administrative practice in a coordinated manner by providing guidelines to help Member States and other CISE stakeholders to interpret and apply specific provisions of EU legislation.
    - This can also stimulate changes in situations when national legislation is more stringent in comparison with the legislation on EU level.[36]

Secondly, the Commission supports all relevant measures to develop, maintain, and disseminate standards allowing maritime surveillance systems to be interoperable. Ongoing projects and pilots should not be stopped but further develop according to general standards that will facilitate maritime information exchange between surveillance authorities and the development of IT solutions, which is major challenge for co-operation between MS, industry development and competitiveness.[37]

In order to provide the mentioned general standards, one of the main goals in the Cooperation ('*COOPP*') project was to developed a concept for a flexible 'computer common language' that can be used to ensure the interoperability of surveillance information systems.[38] The common language, so called CISE Data Model version 1.0, was therefore originally defined in COOPP-project and has now been renewed and established as a common data model in the EUCISE2020.[39]

- This common data model is built to serve as a translation tool between maritime surveillance information systems, in particular between civilian and military systems.
- A technical reference architecture for public services will be defined by end 2017, in line with the European Interoperability Reference Architecture developed by the programme on "Interoperability Solutions for European public administrations" (ISA programme), within the framework of the Digital agenda for Europe. Specifications to support virtual collaboration from existing IT systems will also be needed.[40]

Thirdly, the Commission supports with centralised EU funding the modernisation of MS' national IT systems for maritime surveillance to enhance information exchange and by this and generally encourages MS to further enhance information sharing between authorities involved in maritime surveillance.[41]

Fourthly, as the EUCISE2020 is ongoing scanning its future form and dimensions, the Commission has recommended Member States involving the competent national data protection authorities as early stage as possible to ensure that the operational means and objectives comply with national data protection requirements. Prior impact assessments could be one way of support for national initiatives in order to ensure that the most effective and cost efficient measures are put in place.[42]

Fifthly, The Commission has started the review of existing sectorial European legislation in order to address and remove all legal limitations to information exchange while ensuring compliance with relevant data protection requirements. Although the Commission believes that most of these have been addressed, they may still exist at national level. These may persist due to the organisational structures of Member State authorities.[43]

Sixthly, the Commission has launched an analysis process on the governance options of the Maritime CISE i.e. where and how it should be managed. Further reflection is required in particular the need for service level agreements between national authorities.[44]

And finally seventhly, The Commission will formally conduct the assessment of the proof of value (POV) i.e. to weight the all relevant details, facts and the work done, in the fourth quartile of 2017. After this it will also launch a review process to assess the implementation of a Maritime CISE and the need for further action by 2018.[45]

Currently the Commission holds the overall supervision role bringing the CISE forward properly according to the EU acts and standards. As seen above, several parallel actions are taken place and ongoing in order to assure the fruitful cooperation between the relevant parties and MS taking into account all possible scenarios of administering and situating the future CISE platform and its technical cells – keeping in mind the ensuring of the best possible footing for operative CISE by 2020.

## 3.2 Policy Analysis and Official Reports – Summary of Findings

In this chapter the already scanned official communications, reports, documents etc. are shortly analysed and summarised keeping in mind, how RANGER will benefit CISE. The reference documents are the most commonly used and re-referred when it comes to the factual argumentation regarding the CISE, maritime surveillance development or the EU maritime affairs around that topic. The writers would like to remind that the amount of the official or at least legally-binding as well as voluntary based documents is constantly rising inside the EU. That is why the cropping in this chapter is due to the writing moment, September 2016.

The structure of this chapter might need a bit clarification beforehand. First the CISE objectives are once again shortly repeated. After this the EU policy measures supporting these objectives are presented and finally the reference documents (*used in maritime information exchange development as well in CISE and therefore also in this study*) as well the other CISE supporting actions are crosschecked towards these policy measures. This should reveal, what type of the below-mentioned policy measures are mainly used considering future CISE. Later this leads to the RANGER added value.

As it is already pointed out, there are challenges regarding the lack of sharing maritime surveillance information among relevant entities in the EU. However, problem solving has been started and the common will is to make a change. The drivers behind this, in a nutshell were:

- "Administrative cultures and traditions are dominated by sectorial thinking
- Many technical solutions are user community specific and not always suited for immediate integration with the systems of other functions or countries
- Legal limitations constrain restrain the ability of Member States to provide the legal conditions to enable information sharing across sectors and with other countries.

– Increased demands on surveillance and increased budgetary constraints."[46]

Not surprisingly the specific objectives of CISE are also directly linked to the above mentioned drivers. Hence, it is a direct objective to

– "Reduce the legal limitations and promote legal certainty, and
– Reduce the technical limitations via the establishment of an appropriate IT environment, and
– Reduce the cultural limitations via the establishment of a new culture in purpose-oriented information sharing."[47]

These specific objectives are generally addressed in the EU formal policy i.e. in-written to the guiding principles and steps to be taken at the union level. In the next table the public EU policy measures and major decisions are divided according to the mentioned specific objectives, which they mostly likely will support. Although, it should be remembered that one objective might have other linking as well but the most obvious are presented here.

**Table 5: CISE objectives vs. policy measures[48]**

| Objectives | Supportive policy measures |
|---|---|
| Reduce the legal limitations and promote legal certainty | - Remove legal limitations by allowing the transfer of maritime surveillance information to certain enumerated functions<br>- Safeguard the protection of personal data, confidentiality, IP rights and the use of data when data is being shared through the CISE environment<br>- Establish the principle of responsibility to share as a legal obligation |
| Reduce technical limitations via the establishment of an appropriate IT environment | - Define a common information exchange model<br>- Provide for common data classification levels and access rights<br>- Provide for a catalogue of datasets and information services<br>- Define a messaging protocol and potentially the service discovery specifications and correlation and fusion rules<br>- Provide framework for semantic and technical interoperability agreements<br>- Provide financial support to establishment of IT environment |
| Reduce the cultural limitations via the establishment of a new culture in purpose-oriented information sharing | - Define CISE principles based on responsibility to share and need to know principles<br>- Support the entering into agreements between maritime surveillance authorities regarding terms and conditions of information sharing<br>- Provide financial support to facilitate cooperation and joint operations |

Keeping table five (*table 5*) division in mind, one can form at least three options to set weight for taken policy measures. These are shortly described below:

- Option 1: No EU actions
- Option 2: Measures based on voluntary
- Option 3: Legally binding measures

**Option 1: No EU actions**

As we already now and is mentioned above, there is a common willingness to share the maritime situational picture and increase the awareness around the topic. If selected, this option would leave the current approach unchanged i.e. no policy change in this issue that is also why it is not selected here for further consideration. In the fields of law, acts etc. where actions are not made regarding to CISE, they are probably not needed in the first phase or at all. Contrary, No EU Actions can be still used as a baseline scenario and reference point for other measures.

**Option 2: Measures based on voluntary**

In CISE, the willingness is there to be, as mentioned when excluding the first option. Voluntary based measures are partly in everyone's interest as totally compulsory measures might be seen too arrogant and as a political intervention to one's sovereignty what comes to keeping or releasing its own sensor data and surveillance information that is, basically, prioritised to own needs and to protect own territories. As the European countries still realize the obvious connections when living

in the union in its original meaning, they are still trusting in the voluntary work. There is also the win-win, i.e. share-and-get –situation that is needed, excpecially in those MS lacking of adequate sensor equipment or suffering the possible faced phenomena first (*e.g. illegal immigration*). The most problematic or challenging are the connections and measures towards the third countries (*i.e. outside of the union*) e.g. in exchanging and securing the data.

The success of the voluntary measures in reaching the goals depends on the willingness and facilitation, but also national resources of the different actors to participate. Voluntary measures, unlike legislation, may still provide more responsiveness and flexibility as they can be established and altered more fluently and quickly than legislation. On the other hand, there is a limit to what can be achieved by voluntary cooperation as there is limitations and protected areas in existing legal limitations to overcome, assuring coherent implementation, but also as to the degree of uptake on information sharing.[49]

**Option 3: Legally binding and legal measures**

This policy option promotes the legal or legally binding measures when addressing the CISE objectives. This option might be seen the best what comes to the equality among MS and possible connections to the third countries as well as similarly regulated methods when interpreting the law. However, the major drawback of this policy option lies in the same area, the lack of sufficient and timely coordination regarding the adoption of the multiple sectorial legislative acts and delegated acts and the administrative complexity associated with the process. This complexity can be simplified by grouping the sectorial legislative amendments depending on their legal basis and further distinguishing depending on the type of the legislative act amended (*i.e. a regulation amending regulations adopted on the same legal basis, directive amending directives adopted under the same legal basis*)[50].

**Summary of Findings**

The next table below crosschecks the findings of the most common reference and guiding documents as well as other measures taken, together called as supportive actions, towards the above-opened policy measures. The table also gives the each supportive action a reference number 1 to 3 (*1-3*) that equals the policy options opened above.

Most of the reference numbers (*e.g. COM (2007) 575*) are left away in order to focus and see the content properly, without the institution of bureau affections.

It is undeniable that some of the actions and documents might fit under the different objective as well as the shown present one, e.g. legislation might as well lead the way to cultural changes as well it is at same time shaping the legislative ground for actions. This is also why they are categorised according to their prior intention to affect at the legislative field. Also the certain pilot projects are categorised by their aims to support the common situational awareness in real time while the project is ongoing and afterwards via this enable the cultural changes in this matter.

**Table 6: CISE objectives vs. policy measures vs. reference documents**

| Objectives | Supportive policy measures | | Supportive action (guiding document etc.) |
|---|---|---|---|
| Reduce the legal limitations and promote legal certainty | - Remove legal limitations by allowing the transfer of maritime surveillance information to certain enumerated functions<br>- Safeguard the protection of personal data, confidentiality, IP rights and the use of data when data is being shared through the CISE environment<br>- Establish the principle of responsibility to share as a legal obligation | 3 | An Integrated Maritime Policy for the European Union |
| | | 3 | The European Agenda on Security |
| | | 3 | European Union Maritime Security Strategy (*EUMSS*) & its action plan[51] |
| | | 3 | Examining the creation of a European Border Surveillance System (*EUROSUR*) |
| | | 3 | Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain |
| Reduce technical limitations via the establishment of an appropriate IT environment | - Define a common information exchange model<br>- Provide for common data classification levels and access rights<br>- Provide for a catalogue of datasets and information services<br>- Define a messaging protocol and potentially the service discovery specifications and correlation and fusion rules<br>- Provide framework for semantic and technical interoperability agreements<br>- Provide financial support to establishment of IT environment | 3 | Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain |
| | | 3 | Better situational awareness by enhanced cooperation across maritime surveillance authorities: next steps within the Common Information Sharing Environment for the EU maritime domain |
| | | 3 | Development of the key IT components (of CISE) |
| | | 2 | Interoperability improvements in Member States to enhance information sharing for maritime surveillance |
| | | 2 | The European test bed for the maritime Common Information Sharing Environment in the 2020 perspective **(**EUCISE2020) |
| | | 2 | CISE Architecture Visions Document |
| | | 2 | EUCISE2020: Deliverable D4.3 EUCISE2020 Data Model |
| | | 2 | EUCISE2020: CISE Handbook |
| Reduce the cultural limitations via the establishment of a new culture in purpose-oriented information sharing | - Define CISE principles based on responsibility to share and need to know principles<br>- Support the entering into agreements between maritime surveillance authorities regarding terms and conditions of information sharing<br>- Provide financial support to facilitate cooperation and joint operations | 2 | Test Project on Cooperation in Execution of Various Maritime Functionalities at Sub-Regional or Sea-Basin Level in The Field of Integrated Maritime Surveillance (COOPP) |
| | | 2 | COOPP Final Report (*with its outcomes as a recommendation*) |
| | | 2 | Pilot project on integration of maritime surveillance in the Northern European Sea basins (MARSUNO) |
| | | 2 | MARSUNO Final Report (*with its outcomes as a recommendation*) |
| | | 2 | Pilot project on integration of maritime surveillance in the Mediterranean Sea and its Atlantic approaches" (*BlueMassMED*) |
| | | 2 | BlueMassMED Final Report (*with its outcomes as a recommendation*) |
| | | 1 | The development of the CISE for the surveillance of the EU maritime domain and the related Impact Assessment |
| | | 3 | Frontex Annual Risk Analysis |

The table shows that a broad set of policy and other measures, having the potential to address the specific objectives, has been drafted. According to the short policy analysis related to the references and CISE's active measures taken, the result seems to be as follows in order to aim the specific objectives:

There can be found totally at least eleven (*11*) correlations to voluntary based actions (*option 2*) , nine (*9*) to legal or legally binding actions (*option 3*) and one (*1*) to external actions that actively are related neither one (*option 1*). As in some policy analyses, the same attribute might get several correlation numbers, in this study only the most obvious one remains. This is partly because too many variations might reject the final outcome to have its concrete form. This however does not mean, that the measures presented would be able to tackle all the various objectives in a satisfactory manner alone as it is only the reference given.

Reduce the legal limitations and promote legal certainty

- Total measures in this objective was five (*5*)
- Five out of nine (*5/9*) of all the legal or legally binding actions correlates with this objective

Not surprisingly seem the legal or legally binding actions would be most suitable for this objective since the effectiveness of the second option, voluntary based actions, would be relatively low and no long-lasting outcomes might occur as there would be large legal complexity armada and administrative complexity associated with the implementation of this option. As the legal background work has been done, some of the actions might benefits the voluntary work as well that might have in these situation more possibilities.

Reduce technical limitations via the establishment of an appropriate IT environment

- Total measures in this objective was eight (*8*)
- Three out of nine (3/9) of all the legal or legally binding actions correlates with this objective
- Five out of eleven (5/11) of all the voluntary based actions correlates with this objective

The second specific objective of reducing technical limitations may be more effectively implemented through voluntary work. By voluntary work it is meant that everyone can e.g. participate in the suitable projects that are called and conducted to promote the common issue and vice versa benefits the further implementation of the cooperation and the results. As the project partners, for instance, are answered the Commission project calls and selected into the consortium, they undoubtedly have some effort to give and via this benefit the whole union that implements the taken actions in concrete.

Although the effectiveness of this policy option would be somewhat lower, if no legal or legally binding actions will occur here. This is essential and outmost important to notice that the strength for voluntary based projects and their outcomes, as well as the possibility to implement the results in coherent way comes from the general and/or specific EU law principles (subsidiarity and proportionality).

Reduce the cultural limitations via the establishment of a new culture in purpose-oriented information sharing

- Total measures in this objective was eight (*8*)

- One out of nine (1/9) of all the legal or legally binding actions correlates with this objective
- Six out of eleven (6/11) of all the voluntary based actions correlates with this objective
- One out of one (1/1) of all the non EU actions correlates with this objective

For the same reasons as mentioned in the previous objective, the option based on a voluntary cooperation will suit this option as well. The strength in this option is two-sided: it is easy to implement by voluntary basis and it is flexible. It should still take into account the adaptability and coherence with specific EU law and institutions that forms and adjust the drivers behind the actions i.e. the catalyst to seek answers and participate. That is why most of the CISE pilot projects occurs here as the cultural change in information exchange starts within.

As said, each of the policy options has its strengths and weaknesses. To some degree, these differ depending on the specific objective sought to be achieved through the policy option.

This short analysis based on the table study indicates that the policy option two (*2*) regarding to voluntary actions would be most suitable in achieving most of the objectives without denying that it would not work properly without implementing and/or parallel developing the policy option three (*3*) regarding the legal background. A combination of the two options would therefore be the preferred option for implementing CISE.

This is also a strong indicator for RANGER when considering the attributes and factors, how it would benefit CISE and the bigger picture around it. In the next chapter and finally in the SWOT analyses this is concluded.

# 4. Defining Criteria for Benchmarking

Before entering into the field of benchmarking it should be kept in mind that although the use of 'comparative data', as benchmarking basically is, has been used for years between one or more industries and companies at the same market area, benchmarking as defined today was developed in the early 1980s at the Xerox Corporation in response to increased competition and a rapidly declining market.

Shortly put, benchmarking is an ongoing, systematic process for measuring and comparing the work processes or products of one organisation to those of another, by bringing an external focus to internal activities, functions, or operations. The main aim or goal in benchmarking is to provide the company key personnel, in charge of processes, with an external standard and viewpoint for measuring the quality and cost of current internal activities, and to help identify where opportunities for improvement may be. When taking steps and deciding to benchmark, a company or industry usually has already detected a place for improvement in its processes or might just need the new perspective for the present situation. All the same, it is a wise movement.

Benchmarking usually is, or it should be integrated into the fundamental operations throughout the organisation that analyses the data collected longitudinally. Benchmarking attempts to answer usually the following questions:

- How well are we doing compared to others?
- How good do we want to be?
- Who is doing it the best?
- How do they do it?
- How can we adapt, what they do, into our institution?
- How can we be better than the current best?[52]

As a contrary to the above written questions let's bring in mind the SWOT analysis questions regarding to RANGER once more (*from page 10*):

- How can RANGER use each (*S*) strength in CISE?
- How can RANGER beat each (*W*) weakness in CISE?
- How can RANGER exploit each (*O*) opportunity in CISE?
- How can RANGER defend against each (*T*) threat in CISE?

As seen above, there is several similarities between the idea and willingness to improve (*benchmarking*) and how to do it (*SWOT*).

## 4.1 European Union Maritime Security Strategy and Integrated Maritime Policy

The following subchapters are presenting first the indicators that results the need for better surveillance capability (*e.g. equipment and systems*) at the European maritime domain. When these indicator are presented in more detail, as they were first referred also at the in chapter one, the operative and technical requirements to challenge the indicators are then drafted. Indicators are taking into account the general remarking and recommendations as well as principles from the (*topic mentioned*) background documents.

**Economic indicators**

1. **Output**: Ship accidents (*number of ships involved in accidents*): improved information exchange may improve the avoidance of ship collisions or grounding etc. In addition, in the effect of the occurrence of such an event, as early warning as possible together with the fluent information exchange may facilitate co-ordination and efficiency of actions by relevant authorities.

1.1 **Impact**: 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.

2. **Output:** 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*): 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 value added taxes* [*VAT*], *which is a national tax*) are Union own resources.

   **Output:** 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.

2.1 **Impact:** 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.

3. **Output**: Piracy (*number of pirate attacks*): 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.

3.1 **Impact:** 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.

3.2 **Impact:** 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.

**Social indicators**

1. **Output**: 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.

1.1 **Impact**: Deaths (lost human lives due to maritime events – valued via the Value of Statistical Life): a number of the social outputs of maritime activities lead to adverse mortality impacts.

1.2 **Impact:** 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.

2. **Output**: 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.

2.1 **Impact:** Health (health cost due to maritime events – valued via the unit health cost/implications of a given social output): a number of the social outputs e.g. drug abuse (possibly also economic or environmental outputs) of maritime activities lead to adverse health impacts.

3. **Output**: Arms trafficking *(number of small arms and light weapons smuggled into the EU by sea*): illegal arms have crime impacts and endanger the internal stability of EU Member States.

3.1 **Impact:** Crime (*crime prevention/solving cost due to maritime events – valued via the unit cost of a given social output*): illegal arms have crime impacts and endanger the internal stability of EU Member States.

**Environmental indicators**

1. **Output**: Pressures on fish stocks from Illegal, Unreported, and Unregulated (*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.

1.1 **Impact:** 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*).

2. **Output**: Accidental oil spills (*annual number of accidents, with > 7 tonnes of oil 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.

   **Output**: 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.

2.1 **Impact:** 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*), but also negative health impacts (*e.g. by eating sea fauna*).

3. **Output**: 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.

   - 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).

   - Persistent organic pollutant (POP) – Aggregated assessment of hazardous substances in biota measured in the North East Atlantic, Baltic Sea, and Mediterranean Sea.

3.1 **Impact:** Chemical pollution (*degradation of on the marine environment and ecosystem services from chemical pollution*).

**Table 7: Combination of indicators**

| | **Indicators** | | |
|---|---|---|---|
| | **Economic** | **Social** | **Environmental** |
| **Output** | - Ship accidents<br>- Entry of smuggled goods<br>- Entry of counterfeit and pirated goods<br>- Piracy | - Irregular immigration/human trafficking<br>- Drug trafficking<br>- Arms trafficking | - Pressures on fish stocks from Illegal, Unreported, and Unregulated (*IUU*) fishing<br>- Accidental oil spills<br>- Illegal operational oil spills<br>- Chemical pollution |
| | 4 | 3 | 4 |
| **Impact** | - Income from taxes/duties<br>- Income to businesses and from sales tax<br>- Trade<br>- Insurance prices | - Deaths (*lost human lives*)<br>- Jobs<br>- Health (*health costs*)<br>- Crime | - IUU fishing<br>- Oil pollution<br>- Chemical pollution |
| | 4 | 4 | 3 |
| **Total** | **8** | **7** | **7** |

As seen above, the economic indicator is slightly above the other two when weighting the total results (*output vs. input*). However, when considering only the outputs, economic and environmental aspects are equal as in impacts the economic and social aspects.

From some directions the impacts might be seen stronger dimensions compared to the outputs as they are the result the EU must live and deal with. From this viewpoint the economic reasons are equal drivers with social ones when considering CISE and related surveillance system improvements. The exact 'ranking' between these two cannot be said according to this short study but if mirrored against 'the duty to care', respecting each and every life equally, social indicator might be counted the most driving one.

## 4.2 Operative and Technical Requirements for Vessel Detection, Recognition and Identification

In this chapter the operative as well as the technical requirements for vessel detection, recognition and identification are presented. As mentioned already earlier, the criteria for this benchmarking is only a proposal in order to have the best possible outcome of the project's main objective: improvement in vessel detection, recognition and identification. Despite its proposal nature, the following requirements represent the potential end users', infrastructures and environment's operative and technical demandings for the objectives listed. Some of the mentioned requirements can be count also two-layered i.e. they are important factors from bot technical and operational viewpoints.

As for background, the terminological definition of 'detection', 'recognition' and 'identification' must be done.

- By 'detection' the first signals and/or marks of the object (*e.g. vessel)* is meant. This usually happens when the object enters the outer edge/line of our surveillance area and that captured information reaches the surveillance system displays and the operator on duty. Cameras and/or radars are used.
- When using 'recognition', the object is first a) permanently tracked, that means that the object becomes a target. This word *does not* contain any hostile meaning, but is only a term for object that is tracked and confirmed not to be a 'ghost echo' i.e. false positive/false alarm. Tracking means that the object e.g. the radar echo is strong enough for the manoeuvring parameters to be calculated i.e. course and speed. Secondly b) when recognised, the 'rough' type of the target can be named, whether it is a merchant vessel, warship, leisure boat etc. This type can be categorised with the help of mobilised units at the field but also with the visually operating equipment e.g. cameras.
- The 'identification' means that the visual sight confirmation of the target is adequate and precise enough so that the target can be named. Usually naming is done by the vessels own name of with its IMO-number that is a unique reference for ships and for registered ship owners and management companies.

**Operative Requirements**

As the CISE should offer its' end users more data and information to be used in ones' daily basis and work supporting the relevant actions at the sea, coastline and in some cases also in the harbours, it should be reliable enough. Despite that CISE is not, however, replacing any of the current operative surveillance systems in the MS, but only producing some added value, this requirement is not vital. Even though, the information filtered, layered and classified with certain classification level must be always trustworthy as it steers, in the end, directly or indirectly the operative work and the use of resources in the field. The reliability is one of the basic requirements that holds its value also from the technical point of view so it can be counted as two-layered (*see table 8*).

Second important factor is the system availability by witch the 24/7/365 i.e. "twenty-four-seven" operational system is meant, i.e. the system must operate constantly. This is counted as well as a two-layered requirement due to the following challenge to beat that has strong influence in enable the 24/7/365 operativiness: As the end users require constantly operating system, the usability must be internationally and nationally duplicated. Two different actions should be considered: 1) the administrative operativiness' duplication in prior to others, i.e. the main place of use at the EU-level (*administrator actions*) must be duplicated and 2) national linking points/use points should be

duplicated as well. Additionally this also means that the alternative places of use should be periodically tested. The duplication is one of the basic requirements in order to exploit the system most efficient way. Reasons for the secondary use of points' activation might be e.g. blackouts (*i.e. temporarily lack of power*), maintenance, technical or/and human failures or any kind of sabotage. Still, once again, as the CISE is not replacing any of the national systems, these requirements might be counted more technical than operational. However, the have influence between.

The system must be able to merge i.e. system has to consolidate targets detected by all radars (coastal and Over-the-horizon radar) with data provide AIS, VMS or any source.

Also the system must be highly adjustable. The adjustability plays a great role first when detecting and then recognising the object as the weather conditions at sea are manifold but also changing rabidly. Adjustments like sea and rain clutter, ready settings for certain sea states as well as settings for interference and noise removals etc. must be in-built. Also different marks, lines etc. should be able to add on the screens so that territorial waters, avoidable areas etc. could be surveyed efficiently. In some radars the wider the setting selection the difficult the radar is to use. Due to that, the setting selection must be easy to use i.e. user friendly so that also the quick adjustments are possible when rapid reaction are needed – usually in cases of illegal activities at sea. The target cannot be lost. As for CISE and from RANGER's point of view, these (*adjustable, settings*) are one of the most wanted added value for the present plans.

Also referring to the setting selection, but keeping it separate, still pictures from the connected cameras should be able to print as well as videos saved from the screens (camera or radar etc.). This is vital on order to prove and justify the responsibility in criminal matters.

In table eight below (*table 8*) the above written requirements are summarised. As the all mentioned details have impact on both technical and operational work, specific difference is unable to do. However, when marked with '+ ', the impact might be lower than if marked with '++'. The '++' means that the impact is more vital on that specific area, either technical or operational.

**Table 8: Operative requirements for vessel detection, recognition and identification**

| Requirement | Technical | Operational |
|---|---|---|
| System reliability | ++ | + |
| System availability 24/7/365 | ++ | + |
| EU-level usability duplication | ++ | + |
| National level usability duplication | ++ | + |
| Merging ability | ++ | + |
| Adjustability | + | ++ |
| Easy-to-use | + | ++ |
| **Total** | **++ = 5 / + = 2** | **++ = 2 / + = 5** |

**Technical Details / Requirements**

In order to enable the above mentioned requirements at least at their minimum, the specific technical details should be considered as listed below. If the technical requirement has a direct link into the operative actions, it is marked aside. Again, when marked with '+ ', the impact might be lower than if marked with '++'.

**Table 9: Technical requirements for vessel detection, recognition and identification**

| Requirement | Technical | Operational |
|---|---|---|
| Detection target size (*the minimal height above the sea level of a detectable target from certain distance*): ASL <= 2m, and higher, up to 150Nm, ASL <= 5m, and higher, up to 200 Nm. | ++ | + |
| Detection rate (*the detection ratio of actual targets*): 99% - measured comparing with AIS and using cooperative boats during pilots. | + | ++ |
| False positives (*the ratio of false positives [false alarms]*): false positive detection of unusual behaviours should not exceed 1%. | + | ++ |
| Spatial accuracy (*the accuracy of the target localisation*): Range accuracy of 100m, Azimuthal accuracy of 0.2°. | + | ++ |
| Range resolution (*the minimal distance between targets almost the same speed, in order the radar to be able to distinguish them*): < 3Km (*depends on the bandwidth used*). | + | ++ |
| Covered area width (*the width of the zone covered by the radar*): up to 180°. | + | ++ |
| Transmitted power (*the power produced by the radar transmitter*): for the Full Scale solution and for a 50 kHz bandwidth, 2 kW Power Output for continuous wave. | ++ | + |
| Environmental footprint (*compliance with environmental directives*): installable in protected zones such as Natura 2000 areas. | ++ | + |
| Update rate (*detection/ tracking updates*): 30/60 sec. | ++ | + |
| Ionospheric clutter mitigation (*reduction of ionospheric noise/echoes*): more than 60 dB attenuation. | ++ | + |
| **Total** | **++ = 5 / + = 5** | **++ = 5 / + = 5** |

As a conclusion, and as seen above in tables eight and nine (*tables 8-9*), strict line between the technical and operational requirements is hard to set as the technical details usually has a huge impact to the operative work.

However, the mentioned requirements leads the way for benchmarking. As there are many options (*i.e. radars and other equipment*) on the markets that can meet the requirements at least partly, the relevant questions regarding to RANGER are:

- How well is RANGER meeting these requirements?
- Is there others who are doing it better/closer to these req.?
- How do they do it?
- How can we adapt, what they do, into our system?

# 5. Conclusion - SWOT Analysis on Means for Strengthening CISE

In this chapter we are closing the end of this study. On the previous pages the CISE is generally presented through its development history and the current state-of-the-art as well as the actions ongoing. Then, policy analysis was made from the above mentioned in order to see which way the future development might be the most efficient to do on policy level and finally, benchmarking criteria was drafted by locating the economic, social and environmental indicators at the area. This was completed with the operational and technical requirements. On the next pages all the mentioned notes from previous pages are compared to possible RANGER added value get. This is done with the SWOT analysis. As we are already aware of, to gain the full benefits of SWOT, the analysis should firstly provide information that helps in decision making. Secondly, it should be remembered that the first two attributes are internal as well the last two external. Next we are answering the RANGER-SWOT questions with the information gained.

**How can RANGER use each (*S*) strength in CISE?**

When realising as planned, the CISE will provide a new, multi-layered environment for information exchange that the end users can exploit as a supportive and detailing data source for their own situational picture and awareness. The final CISE is as strong with its information gathering dimension as there is different users providing their National Exchange Platform's (*NEP*) data to be used for common good. Additionally, the more technically better surveillance equipment CISE end users have the more reachable and 'early-warning' the whole EU maritime domain is. Hence, if already existing and different entities and institutions on different layers and fields linked on the maritime functions and domain could use RANGER as a priority or data ensuring secondary system, the more adequate the whole situational picture from each corner of the EU would be. As the common Data Model has already been published based on the pilot projects, best practices and several expert hearings throughout the CISE consortium etc., these functionalities should be taken closely into account when further developing RANGER.

To use the mentioned network strengths in CISE, the design of RANGER platform should ensure the full compatibility with CISE framework and sources while operational. RANGER will comply with the framework by customising a set of services that can be adapted to or consist a CISE information layer. Additionally, when combined with the RANGER's three main services: RANGER Early-Warning System (*EWS*), 2) the Over-The-Horizon (*OTH*) and 3) the Permanent Echo - Multiple Input Multiple Output (*PE-MIMO*) radar tracks, RANGER ensures CISE to provide and deliver continuous information about the tracking of ships at long range, from over-the-horizon to the shore and the opposite. Also the highly adjustable settings are one of the most wanted added value RANGER has to offer.

The CISE strengths could be fully exploited when, in addition to the above mentioned, the development of a CISE translation gateway layer, which will serve as a connecting link between the RANGER architecture's resources (*RANGER platform and RANGER sensors*), is done. The work generally follows a proprietary protocol and format, and the framework which implements the CISE concepts. In this, the proof of concept to design a successful CISE translation gateway already exists from the previous ICEWATER FP7 project.

**How can RANGER beat each (*W*) weakness in CISE?**

As counted also in strengths, the complexity and multitudinous of actors, systems and regulations of each Member State can partly be seen as a weakness as well. The lack of similarity between the communities, in addition to which the areas of responsibility of public authorities might even vary from state to state makes the implementation of CISE and consequently RANGER more challenging. When the national authorities responsible for different aspects of surveillance (*e.g border controls, security, fisheries control, customs, environment, defence, etc.*) collect data separately and often do not share them, some data might be collected more than once. By some estimates, only 30% of the useful data is shared across the sectors and Member States. This unwanted situation is maintained by the still remaining legal barriers to cross-sectorial information sharing at the EU level as well at the national level due to the organisational structures of each Member States' authorities.

Partly due to above written, both the possibility for CISE as well as RANGER project delay rises. As mentioned in the context of the ongoing additional EU Commission led actions The Commission has carried out the review of existing sectorial European legislation in order to address and remove all legal limitations to information exchange while ensuring compliance with relevant data protection requirements. As the Commission also stated and believes that even though the most of the legal barriers have been addressed, they may still exist at national level due to the organisational structures of Member State authorities. It was also in the Commission main principles for CISE that the data duplication must be avoided, disseminated only once and "then be made available to all recognised users". It was also promoted that the "interoperability and connectivity of all relevant actors at national level" should be taken into account.

The above mentioned can lead to a situation, where the RANGER is available and used by some authorities in the certain MS, but not the data nor the relevant information is passed to all necessary parties i.e. the situational awareness of some authorities has increased while new equipment is in use but otherwise the situation remains the same as it was earlier. In the worst case scenario this jeopardise safety and security and might lead in casualties. It should also be remembered that if no adequate sensor technique is adapted in the early phase while it is available, the economic, social and environmental impacts might realise partially or completely (*see detailed more from subchapter 4.1.*) as, for instance, every avoided sea disaster, big or small, lefts the authority reserve to be used elsewhere on the daily actions and duties. In a long run, this improved efficiency saves money.

Also, as the 'black market' and the incessant tax avoidance costs European Union and its Member States hundreds of millions every year both in lost taxes but also, and once again, the resources tied in the prevention duties and processes, it is undoubtable that if saving both or another from the mentioned, economical improvement could be done at the other areas in urgent need for money or suitable official resources. Not only the monetary impact is the risk but also the risk for businesses and market overall as normal priced products cannot compete the much cheaper ones.

Additionally, even though it is not the most alarming problems at the European maritime basins at the moment, there has been signs and indicators about the mentioned piracy actions at the Mediterranean Sea in the 2000s. It is also a fact that the phenomena occurs at the African coastline (*e.g. Somalian sea*) and is ranked one of the most interfering problems for the merchant shipping worldwide i.e. the phenomena makes it difficult to hire personnel on board on the routes the phenomena occurs, insurance costs for cargo companies are rising, prevention methods and trainings onboard are needed as well as authority response is at demand – rightly demanded from the tax payers. All this together are in favor for long reaching surveillance but more importantly calls the cooperation between EU and the third countries in surveillance but also in information exchange matters.

As the irregular immigration/human trafficking, also drug trafficking cost the EU a huge amount of money as the union loses taxes if the drugs are misused prescription medicines. The bigger

problem still remains is the healthcare and rehabilitation for drug users or ex-drug users as well the criminal dimension with the dealing of drugs.

The mentioned has the impact also into the economic zone while the taxes, pension and insurance payments etc. of illegal labour are not taken care of, it is seen here more as a moral impact and misdemeanor in the light of the human rights as well. Saving lives by supporting independent living and education at the place of origin should be the priority but if saving lives at the trafficking routes at the sea, the 'another life' after that must be guaranteed forth of living as well. Correlation to the economic impacts might be seen as well from the healthcare that is arranged in many countries also for the persons with no documents / relevant post address i.e. place to live.

When having also the indirect influence to the legal arm and weaponry industry, the bigger problem stays with the effect of the internal safety and security and the unsafe environment as well.

CISE with the help of RANGER 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 CISE could also facilitate exchange of data between port authorities and all administration in charge of surveys to identify polluters. These data could concern for example the disembarkation of waste to calculate de difference between two ports of call. 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.

CISE in collaboration with RANGER could also contribute the continuous need of data to address numerous technical aspects related to the monitoring and control of chemical pollution. Also, 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.

As seen above, as the union still might suffer from some duplications and non-coordination between authorities it might realise to the union's weakness not to take the CISE in use and/or strengthen it with RANGER. This might allow the economic, social and/or environmental indicators to be even harder to detect. As a state-of-the-art on its field, RANGER could promote the dialogue between the national authorities while introducing the system and its benefits in the MS. It should be strongly advised that in order to get the full benefits out of the system (*as referred in the 'strengths' earlier*) several or better if all national authorities related are involved.

This will also contribute the RANGER's visibility and further marketing when the potential surveillance benefits are widely recognized and further developed via the help of the user comments on the general functionality, further processing the best aspects and localise the potential development areas. The system will also be the widely tested the more entities involved from several different task areas.

**How can RANGER exploit each (*O*) opportunity in CISE?**

As the focus in strengths and weaknesses has been internal, we are now moving to the external ones in opportunities and in threats.

When the EU maritime related authorities eventually will have the system with interoperability that allows information sharing and increases the situational awareness, there is a huge opportunity to involve relevant third countries whose presence and collaboration could bring added value for all the network e.g. from early warning's viewpoint etc. If the RANGER is linked, the ready product demonstrated should get the wanted attention even better as it is the state-of-the-art of its own field and widely in use in Europe. The opportunity lies also in extending partners' knowledge in the CISE framework to develop new, even better CISE in the future with compliant services.

From the CISE's point of view, merging RANGER as outer product with its full abilities and functions into the CISE, there is a huge opportunity for general and critical resource savings. CISE will e.g. enable the maritime authorities to save costs regarding information gathering and the use of assets. This will lead e.g. to a reduction in data duplication resulting from cross-sectorial information sources as well as rationalisation in the deployment of assets such as ships and aircraft. Better coordination will happen also between sectoral activities related to maritime transport, the protection of commercial vessels, defence tasks provided by navies, control of illegal immigration and customs control, prevention of illegal fisheries and pollution and preservation of the maritime environment. All these aspects, for instance, has the direct or indirect influence in the external, neighboring, third countries e.g. in port-to-port traffic.

The advantage of avoiding resource wasting due to duplication of existing systems and the capability to provide cooperating neighbouring countries an open platform to share data, information and services, must be deployed.

When no major changes in one's current systems are needed as the CISE, even accompanied with RANGER's full benefits, can be adapted and linked from outside, enables this a significant growth in safety and security and the surveillance in general by facilitating the coexistence of multiple activities, while reducing environmental, social and economic impacts simultaneously.

As with the help of RANGER, there would be growth in authorities' operation capability, since enhancements in radar coverage and the information sharing with other member states of the obtained valuable information could help to improve the conduct of their operations. This also means that end users might e.g. detect activities beyond their specific surveillance zones, e.g. Search and Rescue Regions, from neighbouring third countries' range of responsibility. In these matters the CISE benefits the whole geographical area as an external opportunity.

The outside of CISE opportunity can be seen also from policy planning viewpoint. When started as a voluntary project, RANGER implementation should proceed also on voluntary basis supported by the EU-level legislation as seen to be the most efficient according to the policy analysis. Even though the full benefits would be gained if the system was ordered to be used, that would not help the cultural change between the entities similarly as it might when the full potential of RANGER+CISE -combination is noticed by themselves.

**How can RANGER defend against each (*T*) threat in CISE?**

However, even the multitudinous network behind the enabling its functionality CISE, the system is partially based/tied on participatory and cooperative of many such countries and administrations that could not share useful data. This is counted as an external threat as these entities are staying the 'outer circle' of CISE and only exploiting the data without providing any. As it is not strictly required the situational picture, indicators and phenomena cannot be reliably detect from these countries as it makes the whole data more or less inadequate.

The weaknesses due to the duplication and/or the tendency not to share information between the member states (as noted above) might make EU more vulnerable to the threats like cross-border terrorism, illegal immigration on small non-cooperating vessels, drug trafficking and arms trafficking. Also risk to biodiversity due to the illegal and non-controlled fisheries might rise as well as environmental degradation due to human pollution by discharging in the sea toxic substances. These might be detected on time if all countries with sea line and port-to-port traffic would participate both receiving and producing data.

Even though the benefits are quite clear the deployment of CISE accompanied with RANGER outcomes might be hampered by legal barriers on data classification, provoking later costs or time-loss when further exploiting RANGER. These 'administrative' threats are affecting the project and system inside the EU but outside the project scope that could be directly intervened.

Also from a business point of view, too non-realistic user requirements that cannot be adapted into the business case, fragmentation of ownership, non-realistic assumptions, verification of performance only in laboratory environment, lack of estimation of maintenance costs might jeopardise the strengths and opportunities.

**Table 10: Key findings regarding RANGER**

| Recommendation | Requirement for RANGER |
|---|---|
| **Interoperability, situational awareness and reaction capacity** | |
| As the CISE is both operational and simultaneously intrinsically technical, and because these two aspects are not recommended to be separated, strict line between the technical and operational requirements cannot be set as the technical details usually has an impact to the operative work and vice versa.<br>– However, as surveillance systems are, after all, tools, the operative requirements should be the priority.<br>– For the same reason the product must be authentically field-tested and evaluated as well as the user's opinions carefully listened *before* implementations. | – Technical and operative requirements (see *tables 8 and 9*) are considered and taken into account while assembling the product.<br>– RANGER concept is to be tested within the EUCISE2020 –project demonstrations (*i.e. played scenarios*) in order to see the interoperability with CISE. |
| The final CISE is as strong with its information gathering dimension as there is different users providing their data to be commonly used. Additionally, the more technically better surveillance equipment CISE end users have the more reachable and 'early-warning' the whole EU maritime domain is. As the maritime domain is scattered and its surveillance challenging, RANGER will undoubtedly technically help to improve this area of surveillance.<br>– Not to be based only to these suppositions, and as already mentioned, the product must be authentically field-tested and evaluated as well as the user's opinions carefully listened *before* implementations. | – RANGER concept is also to be tested on those areas were the sea surveillance is lacking of from<br>- resources viewpoint<br>- technical equipment viewpoint<br>- challenging landscape (*i.e. scattered archipelago*) viewpoint |
| If some MS are staying the 'outer circle' of CISE, while RANGER in use and adopted, and only exploiting the data without providing any, the situational picture, indicators and phenomena cannot be reliably detected from these countries and areas under their responsibility as it makes the whole CISE data more or less inadequate.<br>– Sufficient requirement level of incoming data from each CISE adapted country should be ensured. | – RANGER incoming data requirements are parallely decided in order to ensure comprehensive situational awareness. |
| **Costs and efficiency** | |
| If CISE is to be implemented as an essential part of the EU wide surveillance, also the 'CISE-exit' -situation should be carefully planned if a MS will no longer find the system or its derivatives relevant for its purposes or needs to be actively resigning. | – The mentioned 'CISE-exit' must be technically possible but more importantly its influences to the system's interoperability must be weighted in a first place.<br>– RANGER should not be in-built in CISE environment, but more or less |

| | |
|---|---|
| Some calculations show that the introduction of the CISE will generate up to 423 million euros in cost/effectiveness benefits for European authorities annually in its operative years. | additional/advanced service if wanted in the MS.<br>– If taken in use in the EU and wider, fast maintenance chain must be properly guaranteed if the efficiency and cost lowing will be held on the sustainable level. |
| **Fundamental and human rights, implementation** | |
| Among economic, social and environmental indicators, the social one with its impacts to EU's inner and outer safety and security might be counted the most driving one for supporting CISE-style technic.<br>– Partially voluntary based implementation (*excluding legislative implementation*) will produce the best benefits from RANGER as seen in the policy analysis. | – Social indicators should be taken into account while implementing the RANCER concept. |

The aforementioned requirements and findings will be included, analyzed and classified according to their priority level in RANGER deliverable D2.5 "RANGER System Requirements" (*first version*).

**Table 11: Comparative SWOT matrix CISE vs. RANGER**

| | **Helpful** for achieving the objective | **Harmful** for achieving the objective |
|---|---|---|
| **Internal** (attributes) | **Strengths**<br><br>**In CISE**<br>- Already different existing entities and institution on different layers and fields, which contributes and promote the sharing of data to improve the co-operative maritime surveillance system. For instance: SafeSeaNet, CECIS, MARSUR, EUROSUR.<br>- Successful conclusions of different pilot projects from which to take inspiration and which contributed to advancement of the state-of-the-art of CISE, such as MARSUNO, BlueMassMed and Cooperation.<br>- A decentralised information structure where primary nodes (*National Exchange Platforms, NEP*) offers the capacity to provide a maritime information and to offer added-value services to the community of member states and EU entities.<br>- Layered framework<br>- The defining of formats and sharing protocols, a common vocabulary and a library of data in way of sharing data to be aware of events that occur and reduce their scope (EUCISE2020 Data Model)<br>- The technical and operational requirements closely adapted (*see more from chapter 4*)<br><br>**In RANGER**<br>- Design of RANGER platform to ensure full compatibility with CISE. RANGER will comply with this framework by customising a set of services that can adapt to or consist a CISE information layer.<br>- Ensure the ability of CISE to provide continuous information about the tracking of ships at long range, from over-the-horizon to the shore and the opposite.<br>- Development of a CISE translation gateway layer, which will serve as a connecting link between the RANGER architecture's resources (*RANGER platform and RANGER sensors*), which in general follow a proprietary protocol and format, and the framework which implements the CISE concepts.<br>- Proof of concept already available from the previous ICEWATER FP7 project to design a successful CISE translation gateway.<br>- Creation and consolidation of new RADAR technologies such as the OTH radar and PE-MIMO radar.<br>- Augment the current CISE state with three services: 1) the RANGER EWS, 2) the OTH radar tracks and 3) the PE-MIMO radar tracks.<br>- Commercial exploitation of the project outcomes ensured by a project consortium with strong industrial presence.<br>- Highly adjustable settings to meet the user demands | **Weaknesses**<br><br>**In CISE**<br>- Complexity deriving in part from the lack of similarity between the communities and the public authorities of each Member State, in addition to which the areas of responsibility of public authorities vary from state to state.<br>- National authorities responsible for different aspects of surveillance (*border controls, security, fisheries control, customs, environment, defence, etc.*) collect data separately and often do not share them. Consequently, some data are collected more than once. Only 30% of the useful data is shared across sectors and member states nowadays.<br>- Possible remaining legal barriers to cross-sectorial information sharing at EU level and at national level due to the organisational structures of Member states authorities.<br>- Partly due to above written, the project delay rises<br>- If no adequate sensor technique is adapted in the early phase, illegal border crossings/undetectioned of the vessels might have impact on<br>  - Income from taxes/duties (illegal workers)<br>  - Income to businesses and from sales tax (piracy, counterfeit goods etc.)<br>  - Trade<br>  - Insurance prices<br><br>**In RANGER**<br>Plan for the entire duration of the project might be too ambitious. |

| | **Helpful** for achieving the objective | **Harmful** for achieving the objective |
|---|---|---|
| | **Opportunities** | **Threats** |
| **External** (attributes) | **In CISE**<br>- Interoperability that will allow information sharing which will eventually increase situational awareness.<br>- CISE will enable the maritime authorities to save costs regarding information gathering and the use of assets. This will lead to a reduction in data duplication resulting from cross-sectorial information sources as well as rationalisation in the deployment of assets such as ships and aircraft.<br>- Avoid the waste of resources due to duplication of existing systems in use and the capability to provide cooperating neighbouring countries with an open platform to share data, information and services.<br>- Enable growth by facilitating the coexistence of multiple activities, while reducing environmental impacts.<br>- Improve the efficiency and cost-effectiveness of maritime surveillance by enabling appropriate, lawful, secure and efficient data sharing across sectors and borders throughout the EU.<br>- Better coordination between sectoral activities related to maritime transport, the protection of commercial vessels, defence tasks provided by navies, control of illegal immigration and customs control, prevention of illegal fisheries and pollution and preservation of the maritime environment.<br>- Sharing marine knowledge to facilitate innovation, investment and sound policy-making.<br><br>**In RANGER**<br>- Establish new scientific and technical knowledge and/or explore the feasibility of a new or improved technology, product, process, service, information sharing network or solution for the maritime surveillance<br>- Growth in the authorities' operation capability, since enhancements in radar coverage and the information sharing with other member states of the obtained valuable information could help to improve the conduct of their operations.<br>- Opportunity to extend partners knowledge in the CISE framework to develop in future new CISE compliant services.<br>- Policy planning viewpoint: When started as a voluntary project, RANGER implementation should proceed also on voluntary basis supported by the EU-level legislation as seen to be the most efficient according to the policy analysis. | **In CISE**<br>- The system is based on participatory and cooperative of many countries and a lot of administrations that could not share useful data.<br>- The weaknesses due to the duplication and the tendency not to share information between the member states make EU vulnerable to the following threats:<br>  - Cross-border terrorism.<br>  - Illegal immigration on small non-cooperating vessels.<br>  - Drug trafficking.<br>  - Arms trafficking.<br>  - Risks to biodiversity due to the illegal and non-controlled fisheries.<br>  - Environmental degradation due to human pollution by discharging in the sea toxic substances.<br><br>**In RANGER**<br>- Deployment of RANGER outcomes might be hampered by legal barriers on data classification, provoking later costs or time-loss when further exploiting RANGER.<br>- The system is based on participatory and cooperative of many countries and a lot of administrations that could not share useful data.<br>- From a business point of view: non-realistic user requirements that cannot be translated into the business case, fragmentation of ownership, non-realistic assumptions, verification of performance only in lab environment, lack of estimation of maintenance costs. |

## Annex A - List of Tables

## Annex B - List of Acronyms

| Acronym | Meaning |
|---|---|
| AIS | Automatic Identification System |
| ASL | Above Sea Level |
| BlueMassMED | Pilot project on integration of maritime surveillance in the Mediterranean Sea and its Atlantic approaches |
| CECIS | Common Emergency Communication and Information System |
| CISE/EUCISE | Common Information Sharing Environment for Maritime Surveillance in Europe |
| COOPP | Test Project on Cooperation in Execution of Various Maritime Functionalities at Sub-Regional or Sea-Basin Level in The Field of Integrated Maritime Surveillance |
| dB | Decibel |
| DMA | French Ministry of Ecology, Energy, Sustainable Development and Spatial Planning |
| e.g. | Exemplī grātiā, "for the sake of an example", "for example" [Latin] |
| EC | European Commission |
| EMSA | European Maritime Safety Agency |
| etc. | Et cetera, "and other things" or "and so on" [Latin] |
| EU | European Union |
| EUCISE2020 | The European test bed for the maritime Common Information Sharing Environment in the 2020 perspective |
| EUROSUR | European Border Surveillance System |
| EWS | Early Warning System |
| FRONTEX | European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union |
| i.a. | Inter alia "among other things" [Latin] |
| i.e. | Id est, "it is", "that is" [Latin] |
| ICEWATER | ICT Solutions for Efficient Water Resources Management -project |
| IMO | International Maritime Organisation |
| IMP | Integrated Maritime Policy Programme |
| IPR | Intellectual Property rights |
| ISA | Interoperability Solutions for European public administrations (programme) |
| IUU | Illegal, Unreported, and Unregulated fishing |
| kHz | Kilohertz |
| kW | Kilowatt |

| | |
|---|---|
| MARSUNO | Maritime Surveillance in the Northern Sea Basins |
| MARSUR | Maritime Surveillance: Technical solution that allows dialog between European maritime information systems -project |
| MoU | Memorandum of Understanding |
| MS | Member State |
| NATO | Nato Science and Technology Organisation |
| NEP | National Exchange Platforms |
| Nm | Nautical Mile (*equals 1,852 kilometers*) |
| OTH | Over-The-Horizon (*radar*) |
| PE-MIMO | Permanent Echo - Multiple Input Multiple Output (*radar*) |
| POP | Persistent organic pollutant |
| POV | Proof of value |
| RANGER | Radars for Long Distance Maritime Surveillance and Search and Rescue Operations |
| SafeSeaNet | Vessel traffic monitoring and information system in EU |
| SAR | Search and Rescue |
| SWOT | Strengths, Weaknesses, Opportunities and Threats |
| VAT | Value Added Tax |
| VMS | Vessel Monitoring System (*a near real-time, usually satellite-based, positional tracking system for fishing vessels*) |

## Annex C - References & Relevant Readings

[1] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2007) 575 final, "*An Integrated Maritime Policy for the European Union*", pp. 2-5
[2] Same, p. 2, 5
[3] COM(2007) 575 final, p. 5 & European Commission, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2009) 538 final, "*Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain*", p. 2
[4] COM(2007) 575 final
[5] FRONTEX, Risk Analysis Unit, "*Annual Risk Analysis 2016"*, March 2016, Frontex reference number: 2499/2016, pp. 14-19.
[6] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2015) 185 final, "The European Agenda on Security", p. 13
[7] EUROSTAT, http://ec.europa.eu/eurostat/statistics-explained/index.php/Maritime_ports_freight_and_passenger_statistics#Further_Eurostat_information, referred 16th of August 2016.
[8] European Commission, Directorate General for Migration and Home Affairs, "*Grant Agreement number 700748 'RANGER'"*, Annex 1 (part B), pp. 3-4
[9] Same, p. 4
[10] Same, part A, pp. 16-18
[11] Same
[12] Pahl N., Richter A., "*SWOT Analysis. Idea, Methodology And A Practical Approach*", GRIN Verlag, Munich, 2007 / Piercy N., Giles W., "*Making the SWOT Analysis Work*", Marketing Intelligence & Planning, Vol. 7 Iss: 5/6, pp. 5 – 7, Cardiff Business School and Strategic Marketing Development Unit, Marlow, 1989
[13] Taylor S.J., Bogdan R., DeVault M., "*Introduction to qualitative research methods: A guidebook and resource"*. John Wiley & Sons, 2015, pp. 7-11 & Strauss A., Corbin J., "*Basics of qualitative research (Vol. 15)",* Newbury Park, CA: Sage, 1990, pp. 4-9
[14] Council of the European Union, Minutes of Meeting 14/15, December 2006, dated 12.2.2007, Brussels, p. 10
[15] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2008) 68 final, "*Examining the creation of a European Border Surveillance System (EUROSUR)*", pp. 2-5
[16] Same, pp. 4-10
[17] Same, p. 5
[18] Same, pp. 9-10
[19] COM(2009) 538 final, p. 4
[20] Same, pp- 4-5
[21] Same, pp. 5-11
[22] European Commission, Communication from the Commission to the Council and the European Parliament, COM(2010) 584 final, "*on a Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain* ", p. 2, 5
[23] FRONTEX, http://frontex.europa.eu/trends-and-routes/western-african-route/, referred 29th of August 2016.
[24] FRONTEX, http://frontex.europa.eu/trends-and-routes/western-mediterranean-route/, -- /central-mediterranean-route/, -- apulia-and-calabria-route/, -- eastern-mediterranean-route/, yearly reported numbers divided with twelve months, seasonal and peak variation occurs, all referred 29th of August 2016.
[25] E.g. European Commission, Directorate-General for Maritime Affairs and Fisheries, Call for proposals MARE/2008/13 *"Pilot project on integration of maritime surveillance in the Mediterranean Sea and its Atlantic approaches*" (BlueMassMED), Call for proposals MARE/2009/04 *"Pilot project on integration of maritime surveillance in the Northern European Sea basins"* (MARSUNO) , Call for proposals MARE/2012/17 *"Test Project on Cooperation in Execution of Various Maritime Functionalities at Sub-Regional or Sea-Basin Level in The Field of Integrated Maritime Surveillance"* (COOPP)
[26] BlueMassMED Final Report, p. 4, http://www.statewatch.org/news/2014/jul/eu-2012-bluemassmed-final-report.pdf, referred 29th of August 2016
[27] MARSUNO Final Report, p. 8, http://www.statewatch.org/news/2014/jul/eu-2011-marsuno-final-report.pdf, referred 29th of August 2016.

[28] COOPP Final Report, p. 9, http://www.statewatch.org/news/2014/jul/eu-2014-coop-project-final-report.pdf, referred 29th of August 2016.
[29] COM(2010) 584 final, p. 3
[30] European Commission, Community Research and Development Information Service, http://cordis.europa.eu/project/rcn/192603_en.html, referred 30th of August 2016 / European Commission, Communication from the Commission to the European Parliament and the Council, COM(2014) 451 "*Better situational awareness by enhanced cooperation across maritime surveillance authorities: next steps within the Common Information Sharing Environment for the EU maritime domain*" final p. 6 / European Commission, Directorate-General for Maritime Affairs and Fisheries, Call for proposals MARE/2014/26 *"Interoperability improvements in Member States to enhance information sharing for maritime surveillance*" p. 4
[31] Same
[32] COM(2010) 584 final, p. 8
[33] COM(2014) 451 final, p. 5-7
[34] Seventh Framework Programme (FP7) was the European Union's Research and Innovation funding programme for research, technological development and demonstration between 2007-2013. The current programme is Horizon 2020 but there are many projects funded under FP7 which are still running. https://ec.europa.eu/research/fp7/index_en.cfm, referred 15th of September 2016
[35] COM(2014) 451 final, p. 5-7
[36] European Commission, Directorate-General for Maritime Affairs and Fisheries, *"The development of the CISE for the surveillance of the EU maritime domain and the related Impact Assessment"* part 2, Combined Analysis, February 2014, p. 44, 64
[37] COM(2014) 451 final, p. 5-7
[38] COM(2014) 451 final, p. 5
[39] European Commission, FP7-programme, EUCISE2020, deliverable D4.3, Technical Specifications, revision 1.0, ANNEX B, "*EUCISE2020 Data Model"* p. 3
[40] COM(2014) 451 final, p. 6
[41] Same, p. 7
[42] Same
[43] Same
[44] COM(2014) 451 final, p. 7 & European Commission, Directorate-General for Informatics, Directorate-General for Maritime Affairs and Fisheries and Join Research Centre, *"CISE Architecture Visions Document"* , revision 3.0, published 6th of November 2013, pp. vii-xii
[45] COM(2014) 451 final, p. 7 & European Commission, Directorate-General for Maritime Affairs and Fisheries, "*Development of the key IT components (of CISE)",* p. 218, http://ec.europa.eu/isa/actions/01-trusted-information-exchange/1-16action_en.htm, referred 15th of September 2016
[46] DG Mare, CISE Combined Analysis, pp. 37-39
[47] Same
[48] Same, p. 42
[49] Same, p. 43–44
[50] Same p. 45
[51] Council of the European Union, 11205/14, "*European Union Maritime Security Strategy*" & 17002/14 "*European Union Maritime Security Strategy (EUMSS) - Action Plan*"
[52] Camp R.C., "*Benchmarking: the search for industry best practices that lead to superior performance*", Milwaukee, Wis.: Quality Press; Quality Resources, 1989, 2013, pp. 12-26 & Alstete, J.W., "*What is Benchmarking*?" Free Internet Publication