Increasing Cooperation between the European Maritime Domain Authorities

ILKKA TIKANMÄKI and HARRI RUOSLAHTI
Research, Design and Innovation
Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 Espoo
FINLAND
ilkka.tikanmaki@gmail.com; harri.ruoslahti@laurea.fi  http://www.laurea.fi/en

Abstract: - This research brings out the European Common Information Sharing Environment (CISE) together with authorities’ cooperation in the maritime domain. Coherence between different national processes is challenging because of the differences between the partners from different Member States. On the other hand, differences in administrative, legal frameworks, and technical issues are solvable. Cross-sectoral cooperation should be enhanced by strengthening cross-sectoral knowledge through exploring the other sectors work methods. Widely shared information supports operations planning and sharing of resources on the European maritime domain. The results of this study show that the authorities are beginning to realize the importance of cooperation and information sharing cross-border and cross-sector: cooperation should be based on common objectives and emphasize the benefits of cooperation.

Key-Words: - Information Sharing; Authorities’ Cooperation; Maritime Surveillance; Maritime Safety; Common Information Sharing Environment; Trust.

1 Introduction

Information sharing and interaction between authorities have become an increasingly important part of cooperation. A baseline for the maritime situational awareness (MSA) is to promote cooperation and thereby increase maritime safety and security [1]. In several countries, maritime issues, particularly those relating to maritime safety, are handled differently. Therefore, it would be unrealistic to create a single model of best practice. The importance of the appropriate bindings, at suitable strategical, policy, operational, and tactical levels, between maritime stakeholders should not be underrated. [2]

The goals of developing European maritime cooperation include: increasing situation awareness, sharing best practices, improving interoperability, removing overlapping activities, and promoting cooperation [3]. In order to reach this result, the following steps must be observed: preventing misuse of information by implementation of information ownership, privacy, and confidentiality; increasing dissemination of situation awareness to improve maritime and seafaring safety; creation of a common standard for information sharing; creation of a mechanism for sharing information between authorities/stakeholders; establishing a system for managing data sharing (confidentiality and data security); adding the use of social media to the information distribution. CISE will provide participating authorities needed access to information, which is related to their tasks at sea [4]. At the European Union level, there are seven user communities as presented in Fig. 1.

The seven user communities in maritime surveillance include; border control, fisheries, defence, maritime safety and security, marine environment, customs, and general law

Fig. 1: Seven maritime user communities present seven user communities at the European Union level[5]

The seven user communities in maritime surveillance include; border control, fisheries, defence, maritime safety and security, marine environment, customs, and general law
enforcement [5]. Integrated Maritime Surveillance will interlink all relevant user communities and build a technical framework for interoperability and integration.

This research focuses on the European level Maritime Authorities’ cooperation between different supervising authorities in the field of cross-border and cross-sectoral information exchange. Due to the fact that numerous systems are not yet interconnected, and the systems are not functioning concurrently, the authorities must promote a stronger role to act together culture with commonly shared goals of engagement.

The research question of this study is: How to increase cooperation between Maritime Domain authorities in the European Union authorities?

1.1 Methodology
This study was carried out as a qualitative research and the research method is mainly descriptive. The study focuses on the processes needed for the effective utilization of the Common Information Sharing Environment (CISE) developed in the EU. Chapter 2 of this paper discusses the European Common Information Sharing Environment and three EU funded projects related to Maritime Domain. Chapter 3 is discussion and finally chapter 4 presents the conclusions of the study.

The research problem is assessed with a constructive research method. As all case study sources may have weaknesses and strengths, this study has used multiple sources of evidence in case study as shown in Fig. 2 [6].

Typically, case studies compound data collection methods such as archives, interviews, questionnaires, and observations [7]. The main strength of case studies in this context is the ability to use a variety of evidence to gain more information than using one method [8]; [9]. The data collection in this study was made by several sources of evidence such as interviews, observation, and documentations. Participants’ observations were made, for example, at three-monthly consortium meetings of EUCISE 2020 project, including Executive Management Group (EMG) and Stakeholder Board meetings, project’s steering Group meetings and workshops of FINCISE between spring 2016 and summer 2017.

2 Common information sharing environment
The Common Information Sharing Environment (CISE) is designed to save expenses, increase security, enable a more effective monitoring, as well as help to keep maritime regions clean to allow the growth of the business in the maritime economy [10]. As reported by [5], it’s unlikely that one technical solution fits every exchange of information within CISE. Therefore, the architecture should be designed “as a cost effective decentralized interconnection of different information layers” [10]. The aim of a strategy is to create national and European level authorities a common framework, which allows them to fight against maritime threats and risks in an integrated manner. CISE is not only a technical issue; the improvement of information sharing is tied to operational procedures [11].

There are several EU-wide systems for information sharing within the seven maritime user communities. SafeSeaNet was designed for vessel traffic monitoring and information, whereas Vessel Monitoring System (VMS) is used to exchange data over satellite communications from fishing vessels to the national Fisheries Monitoring Centers (FMC). EUROSUR is the European Border Surveillance System and provides a platform to cooperate and to share operational information. The aims of EUROSUR are a) to reduce the number of irregular migrants entering the Schengen area undetected, b) decreases the death toll migrants at the sea and c) increase internal security of the EU by countering cross-border crime. [12]. A framework for EUROSUR is divided into technical and operational frameworks [3].

Maritime Surveillance Network (MARSUR) is a defence community users’ main initiative that aims
to improve the maritime picture by linking existing military networks and systems to foster information exchange; Common Operational Picture (COP) is built up and defined by individual users. Policy-oriented marine Environmental Research in the Southern European Seas (PERSEUS) was a four-year European Union’s Seventh Framework Programme (FP7) that ended in 2015. The aims of the PERSEUS were to develop and to test European maritime surveillance systems by integrating existing national and European level systems, and to support the creation of CISE. The PERSEUS Demonstration Project was implemented through live exercises which showed that legacy systems can interoperate and the authorities of the Member States can cooperate seamlessly. [13].

The Cooperation Project Maritime Surveillance (CoopP) was led by Finnish Border Guard, the project ended in March 2014. The aim of the CoopP test project was paving the way for smooth data transmission and easy access, whenever relevant, between public authorities, including EU Agencies, in the execution of the defined maritime surveillance functionalities. In Cooperation project, it was defined three upper-level and nine detailed use cases (operational situations) for sharing maritime surveillance information [14]. Upper level use cases were: (1) Detection of pollution in Baltic Sea, (2) Maritime accident on the English Channel, and (3) Smuggling of drugs in the Atlantic Ocean [14].

Cooperation project created a stepping stone for that objective by enabling more practical development to occur. Most of CoopP’s work was done in the Member States, in the institutions and the agencies, and on workshop meetings. The Technical Advisory Group (TAG) identified use cases, which were selected covering the project’s user communities and the sea areas. Table 1 presents use cases and their goals, operational situation and lead actor of each case.

<table>
<thead>
<tr>
<th>Use case ID</th>
<th>Goal</th>
<th>Operational situation</th>
<th>Lead actor(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>13b</td>
<td>Inquiry on a specific suspicious vessel (cargo related)</td>
<td>Ship’s cargo is illegal, dangerous or in other ways breach of rules and regulations</td>
<td>Border Control, General Law Enforcement, Defence</td>
</tr>
<tr>
<td>13c</td>
<td>Inquiry on a specific suspicious vessel (crew and ownership related)</td>
<td>Persons on board a vessel could be illegal or have criminal background. Uncertainty over the ownership of</td>
<td>Defence, Border control, General Law Enforcement</td>
</tr>
<tr>
<td>25b</td>
<td>Investigation of antipollution situation (law enforcement)</td>
<td>A vessel is suspected of polluting; Sighting by satellite, aircraft, surface vessel, from coast line, reported by vessel polluting or other sources</td>
<td>Marine pollution preparedness and response / Marine Environment</td>
</tr>
<tr>
<td>37</td>
<td>Monitoring of all events at sea in order to create conditions for decision making on interventions</td>
<td>Sensor information, relaying information in real time or delayed, and other information services and systems such as EUROSUR or MARSUR</td>
<td>All User Communities</td>
</tr>
<tr>
<td>44</td>
<td>Request for any information confirming the identification, position and activity of a vessel of interest</td>
<td>Member state authorities have an interest in knowing the current position of a vessel, its activity, identification etc.</td>
<td>All user communities</td>
</tr>
<tr>
<td>57</td>
<td>Knowledge of surveillance capacities of partner authorities in a given sea area to plan basic tactical surveillance (Baseline and Targeted operations)</td>
<td>Need for enhancing or complement surveillance in areas where surveillance is poor or there is a specific surveillance need. Support for decisions where to deploy additional surveillance assets</td>
<td>All user communities</td>
</tr>
<tr>
<td>70</td>
<td>Suspect Fishing vessel/ small boat is cooperating with other type of vessels (m/v, Container vessel etc.)</td>
<td>A fishing vessel / small boat is suspected to have suspected activity with another vessel.</td>
<td>General Law enforcement, Customs, Fisheries control, Defence, Maritime Safety</td>
</tr>
<tr>
<td>85</td>
<td>Anti-Piracy Maritime Surveillance and free navigation control: Merchant vessels at sea sends an alert that it is under</td>
<td>An alert is received by MS designated authority regarding a piracy attack of a ship entitled to fly its flag outside territorial waters</td>
<td>Defence/ Maritimes Safety/ General law enforcement</td>
</tr>
</tbody>
</table>

Table 1: Use cases and their definitions (adopted from [14].)
Maritime surveillance activities between cross-border and cross-sector had been made before the CoopP - project. Thus, CoopP’s aim was to share information widely between different authorities. These use cases designed on CoopP are used also in EUCISE 2020 and MARISA projects. According to [14] “It is important to connect information sharing with the operational aspect and make the use cases narrative in order to understand why the use case/scenario is relevant, and that information sharing is done for a reason.”

2.1 EUCISE 2020
The references of European testbed for the maritime Common Information Sharing Environment in the 2020 perspective (EUCISE 2020) comes from a broad spectrum of factors in the European Integrated Maritime Surveillance field, R&D and pilot projects, and studies accomplished in the past years. Directorate-General Maritime Affairs and Fisheries (DG MARE) published the CISE Roadmap in 2010 [11]. According to the roadmap, EUCISE 2020 brings added value by added effectiveness, cost efficiency, and safer, more secure, cleaner seas, EU digital society, sustainable growth, coordination and knowledge toward an EU digital society, and based Integrated Maritime Policy (IMP) [11]. The innovation needs arise from the maritime stakeholders’ operational experience in managing maritime surveillance processes and system at national, international and European levels.

The project has partners from 15 EU/EEA maritime countries. These partners represent directly or indirectly a user community of more than 60 maritime authorities. The timeframe for EUCISE 2020 is between 01/06/2014 and 31/05/2018. EUCISE 2020 tests and validates the CISE concept at EU/EEA level in order to validate solutions for the cross-border and cross-sector information exchange. [2].

The majority of the existing maritime surveillance systems are characterized by verticality (responds to the need of a specific community), operational nature (supports operational processes more than the exchange of information) and centralization (centrally managed common resources). CISE goals are to fully respond to the cross-sector and cross-border CISE mission in terms of functions, architecture and governance models [2].

It is noticeable, that EUCISE 2020 does not develop a new system or new sensors, or connect networks of sensors. The project will consolidate, extend and improve technical solutions to foster electronic interaction with public administrations across the EU. The following Fig. 3 illuminates the information flows within CISE community and within legacy systems.

2.2 Finnish common information sharing environment
The Finnish Maritime Authorities Co-operation (FIMAC) cooperating parties, in the beginning of FIMAC on 1994, were the Finnish Maritime Administration, the Finnish Defence Forces and the Finnish Border Guard. Since the reorganization of government agencies under the Ministry of Transport and Communications in 2010, the present authorities have been the Finnish Transport Agency, the Finnish Transport Safety Agency (TRAFI), the Finnish Border Guard (FBG) and the Finnish Defence Forces (FDF) [15]. What is significant is that FIMAC authorities are under three different ministries; FBG (Ministry of Interior), FDF (Ministry of Defence), Transport Agency and TRAFI (Ministry of Traffic and Communications).
Sensor information from maritime surveillance is shared by the Finnish Traffic Safety Organization (TRAFFI), Finnish Border Guard (FBG), Finnish Navy (NAVY), and Finnish Traffic Agency (FTA). The goals of cooperation are to coordinate functions, to improve productivity and to reduce costs. This cooperation increases maritime safety, develops information management and exchange, and the joint use of capabilities. A significant mission is to format the national maritime situational picture (NMSP) and distribute NMSP to cooperation partners [15].

FIMAC has a presidium and secretariat on a nationwide level and four working groups; expert working group and under it technical working group, the Gulf of Finland and Western Finland working groups on regional cooperation. FIMAC network is established to share maritime surveillance sensor information and more processed information between authorities as seen in Figure 4.

![FIMAC Information Exchange Diagram](image)

**Fig. 4: FIMAC information exchange** [15].

Maritime actors have a common core of the marine surface Situation picture data, such as Automatic Information System (AIS) and radar information. Each player also shares in their own operations’ observational data. In addition, the actors share with each other information received from their international networks. Actors take advantage, in performing their duties, each other’s collected data by combining it with their own data. Each organization develops its own maritime process of knowledge production, and international networks enable exploitation of new data.

FIMAC cooperation is today an internationally unique example of successful cooperation between authorities. According to [16] “Cooperation between authorities comprises joint preparation, joint operations, exchange of information, and coordination of activities”. Over the years FIMAC cooperation has saved up to 50 M€ compared to the fact that each actor would have acquired the same performance only for themselves [17].

The FIMAC authorities and Finnish Environment Institute launched an EU funded project “FiNCISE” on 2015. FiNCISE is co-funded by the European Union and it lasts from December 2015 to November 2017 in parallel with the EUCISE 2020 project [18]. The goal of the project is to support cooperation within the framework of FIMAC to create a maritime situation picture (MSP) and to share it with its partners in support of their own activities. The other objective of the project is to promote a well-functioning FIMAC approach in national and international projects and forums, and thereby, improving maritime safety in the Baltic Sea. To achieve the technical objective of the FiNCISE program, the project aims to improve the interoperability of national maritime surveillance systems across sectors and cross-border in the European Union.

### 2.3 Maritime Integrated Surveillance Awareness

Maritime Integrated Surveillance Awareness (MARISA) is a HORIZON2020 funded 30-month project that address the need to strengthen the information exchange. The main goal of the MARISA project is to provide a data fusion toolkit for the security authorities. This toolkit correlates data and information from different sources aiming to improve information exchange, decision-making and situational awareness. A toolkit ensures full compatibility with the CISE and European policies and also facilitates the interagency interoperability and cooperation and thereby allows the Member States to decide whether additional sources of information are relevant to its operation. [19].

The MARISA project takes benefits from the other EU projects i.e. CoopP, PERSEUS and EUCISE2020 by using previously established information sharing practices, models, and services in close cooperation with end-user community [20]. The MARISA project “seeks to address the need to strengthen the information exchange to optimize the surveillance of the EU maritime area and its maritime borders” [20].

Use cases and trials in the MARISA project use five CoopP project-based use cases; 13b, 37, 44, 70 and 93. Cases were chosen by potential User Communities that are interested in these particular cases. Operational trials will be exercised in five different areas, namely; North Sea, Iberian Sea, Strait of Bonifacio, Ionian Sea, and the Aegean Sea.
The interoperability of existing functional MSA communities is maximised with the European Maritime Safety Strategy and the CISE model. 

3 Discussion

Borders between sectors are sometimes more difficult to cross than borders between states. Some civilian organizations are also concerned about their data ending up to military organizations [21]. On the crisis domain, the lack of an integrated mechanism for distributing information prevents spreading situation awareness those in need [22].

The European Commission’s Directorate-General for Maritime Affairs and Fisheries (DG MARE) visited Finnish national maritime authorities. The main goal of the visit was to share best practices between DG MARE and Finnish authorities. The specific types of potential new added value flow of information/information services were;

- distributed search across CISE connected databases
- analytical decision-making support for intervention, automated personal data exchange
- EU Vessel Penalties and Sanctions database
- sharing reports on inspection with other authorities
- history of Vessel Database, and communication platform with chat and video conferencing. 

In addition, FiNCISE authorities notify step by step CISE implementation. In the first step, a small-scale CISE information services are easier to implement with added value; on the second step, the services should become increasingly more ambitious. Smaller-scale testing should construct further actions towards building trust between authorities to engage in information sharing. [18].

As stated in [24], “Solving common issues motivates the stakeholders to collaborate and build trust”.

The Finnish Defence University and Police University College have signed an education cooperation agreement that allows execution of the courses in both institutions. This education cooperation initializes and develops opportunities and the quality of working life cooperation between authorities in the future. Police University College’s Executive MBA in Policing students have started on January 2017 studies at the Defence University Art of Warfare - course. As the Defence University’s rector General Major Ilkka Korkiamäki stated “This is a very welcome agreement that opens practical training program and offer the possibility of co-operation between the two authorities” [25], [26]. France has a concept, Secrétariat Général de la Mer (SGMer), which is a small effective coordinating think tank group. It is an efficient way to defeat the difficulty that countries find in forming an authoritative single point of contact for maritime issues. It may be supported by an interagency working group if needed. In several European countries, such as the United Kingdom and Italy, have been established a national interagency Maritime Information Centre within the Navy Command Centre. This kind of collocation ensures better coordination and cost-efficient use of maritime surveillance assets. [27].

European Union share interoperability to four layers and political context as illustrated in Table 2 [28].

<table>
<thead>
<tr>
<th>POLITICAL CONTEXT</th>
<th>Legal interoperability</th>
<th>Legal alignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisational interoperability</td>
<td>Organisational and process alignment</td>
<td></td>
</tr>
<tr>
<td>Semantic interoperability</td>
<td>Semantic alignment</td>
<td></td>
</tr>
<tr>
<td>Technical interoperability</td>
<td>Interaction &amp; Transport</td>
<td></td>
</tr>
</tbody>
</table>

Political context ensures that cooperating partners have compatible visions, aligned priorities, and focused objectives. Legal interoperability means aligned legislation so that exchanged data is accorded proper legal weight. Organizational interoperability includes coordinated processes in which different organisations achieve a previously agreed and mutually beneficial goal. Semantic interoperability aims to ensure the precise meaning of exchanged information, which is preserved and understood by all parties. Technical interoperability is planning of technical issues involved in linking computer systems and services. [28].

Trust is seen as fundamental to the sharing of information – and the lack of trust, an obstacle. As stated in [29] research: “The SMEs emphasized the issue of trust is crucial: Trust is more important than technology”.

4 Conclusion
EU wide projects have shown the importance of sharing information nationally, between the authorities from member states and with third countries. Safety and security cooperation are based on cooperation between authorities. The important development target at operative-strategic and tactical levels is the ability to cooperate.

The activities of all the FIMAC parties have intensified when it has been possible to take advantage of jointly implemented and financed solutions and thus eliminate overlaps. Another example of authorities’ cooperation is joint patrolling of the Coast Guard, boat police and Customs at the Gulf of Finland. Joint patrols intensify the capabilities and build better competences for the authorities. They learn best practices from each other. The police can, for instance, learn Search and Rescue practices from the Coast Guard and the Coast Guard can learn criminal investigation practices from the police. Overlaps reduce when situational awareness improves, operation planning is cooperative, and stakeholders know other’s capabilities in challenging operations.

Therefore, cooperation is valuable for the safety and efficiency of operations. In maritime events, human lives are almost invariably on the line and time is limited. Particularly personal contacts will make information exchange easier even in exceptional circumstances. The cooperation has familiarized various authorities with each other and their practices. This Finnish way of thinking about active cooperation between the authorities provides added value to all parties. Cooperation has become routine and a part of everyday life.

Coherence between different national processes is challenging because of the differences between the partners from different Member States. On the other hand, differences in administrative, legal frameworks, and technical issues are solvable. Cross-sectoral cooperation should be enhanced by strengthening cross-sectoral knowledge through exploring the other sectors work methods.

Even though some sectors have well-functioning relations with other sectors, in some countries national legislation does not even allow cooperation between national authorities. Priorities between sectors may be conflicting for some reason or other. Anyhow, there is a need to improve negotiations between sectors. Also, technical needs differ between sectors and therefore require different approaches and technical solutions.

However, the results of this study show that authorities are starting to realize the importance of information sharing cross-border and cross-sector. When developing trust, a process of cooperation needs to be developed, not just the sharing of information. Cooperation should be based on common objectives and emphasize the benefits of cooperation.

References:


