Multidisciplinary
SCIENTIFIC JOURNAL
OF MARITIME RESEARCH

University of Rijeka
FACULTY OF MARITIME STUDIES

Multidisciplinarni
znanstveni časopis
POMORSTVO

https://doi.org/10.31217/p.35.2.8

Analysing the prospect of the maritime common information sharing environment's implementation and feasibility in Montenegro

Andrej Mihailovic[1], Nexhat Kapidani[2], Enis Kočan[3], David Merino Delgado[4], Jari Räsänen[5]

[1] Division of Engineering, King's College London, Strand Building, Strand Campus, Strand, London, WC2R 2LS, UK & Administration for Maritime Safety and Port Management in Montenegro, Maršala Tita br. 7, P fah 14, 85000 Bar, Montenegro, e-mail: andrej.mihailovic@kcl.ac.uk

[2] Administration for Maritime Safety and Port Management, Bar, Montenegro, e-mail: nexhat.kapidani@pomorstvo.me

[3] University of Montenegro, Faculty of Electrical Engineering, Dzordza Vasingtona bb, 81000 Podgorica, Montenegro & Administration for Maritime Safety and Port Management in Montenegro, Maršala Tita br. 7, P fah 14, 85000 Bar, Montenegro (Affiliated as a consultant), e-mail: enisk@ucg.ac.me

[4] Maritime Surveillance Section, GMV, Isaac Newton, 11 P.T.M. Tres Cantos, 28760 Spain, e-mail: dmerino@gmv.com

[5] Laurea University of Applied Sciences, Ratatie 22, 01300 Vantaa, Finland, e-mail: Jari.Rasanen@laurea.fi

ABSTRACT

This paper outlines an extensive analysis of the case of Montenegro's maritime surveillance system becoming integrated within the European Common Information Sharing Environment (CISE). Threats to secure maritime borders across Europe are ever-present and regularly demand coordinated efforts between the member states to tackle and prevent them, e.g. illegal immigration across the Mediterranean. Administration for Maritime Safety and Port Management (AMSPM) in Montenegro is a member of the ANDROMEDA EU project that seeks to facilitate deployments and demonstrations of CISE trials across the European regions, towards their endorsement readiness. AMSPM is now at the forefront of assessing and deploying the CISE components in Montenegro. It thus appropriately evaluates the operational aspects, observes the CISE implementations in some European states, formulates the impact for other national stakeholders, as well as the very prospect of the resulting augmented maritime surveillance in the country. This substantiates the content of this paper as the feasibility of the CISE deployment in Montenegro, supported by a snapshot of the cost-benefit analysis. We aspire to offer novel perspectives and insights that could be a universally useful experience to different CISE implementation initiatives, especially for countries or regions of similar smaller sizes and coastal area.

ARTICLE INFO

Review article
Received 24 May 24 2021
Accepted 15 October 2021

Key words:
Maritime surveillance
CISE
Cost-benefit analysis
Economic growth
New technologies

1 Introduction

Efficient border security within the realm of independent states as well as in the wider context of the European Union (EU) remains an enormous and cumbersome task. Each EU member state holds responsibility for its own border security but adheres to organised and coherent approaches conducted under multi-lateral agreements such as Schengen. There is a substantial complexity in organising border security efforts as there are 17 EU countries with almost all of them having an external border segment, either maritime or land, towards non-EU countries. The migration crisis of 2015 was a clear indication of the magnitude and risks associated with unsecured European borders. Illegal border crossings soared to unprecedented numbers: 1.8 million across the borders of Europe [1]. Remedy actions that followed included EU measures for effective management of similar situations, strengthening internal security and cross-border cooperation between the member states.

This paper is constituted on the efforts towards augmentation of the maritime surveillance capabilities with future work potentially including the land border situations. European maritime borders are vast with a long length, many islands and insufficient resources to cover and patrol all areas. There is a continuous emergency of the novel types of vessels and a large volume of leisure traffic that is relatively unrestrained all adding to the surveillance challenges. Of particularly interest is the Mediterranean region, from the Iberian Peninsula to the

Middle Eastern border stretching across the areas between southern Europe and north Africa. Apart from the incursion risks by illegal migration there are many additional threats requiring expedited coordinated surveillance efforts: piracy, narcotics trafficking, smuggling of illicit good and arms, illegal fishing, environmental crimes and maritime accidents and disasters. Alleviating these maritime surveillance threats is specifically critical as Europe continuously depends on safe commerce by sea and via maritime affairs.

There is evidently a great necessity for further coordination between European and national (government) authorities and maritime stakeholders by cross-border and cross-sectoral cooperation. Experience has shown that threats to maritime cybersecurity are diverse and most of the data acquired in the process tends to be robustly protected within the maritime authorities [2]. Past efforts in sporadic and unstandardized sharing of data between the trusting and collaborating maritime authorities in different states, have often led to data collection replications, asynchrony, and inconsistent availability in the maritime areas of interest. In 2010, the European Commission and EU/EEA member states laid out a roadmap towards the maritime Common Information Sharing Environment (CISE), aiming to make it fully operational by 2020, as a ubiquitous facilitator of technical and semantic interoperability [3]. This initiative has been jointly developed by various EU member states and institutions through numerous EU funded projects and support of relevant agencies (e.g. FRONTEX, EMSA, EFCA etc.). The CISE builds upon the previous initiative of the European Border Surveillance System – EUROSUR [4] of a lesser scope, which had the main objective of augmented situational awareness and reaction capability at external EU borders, focusing on southern maritime and eastern land borders. This is taken further in the CISE, which aims to make different maritime systems interoperable by facilitating exchanges of relevant maritime surveillance data and services by reusing the existing standards and their vocabularies. Importantly, a design principle formulated in the constituent CISE initiative states that no changes would be needed in present legacy systems. Hence, the existing surveillance systems and networks are effectively to become integrated through sharing of information needed in their operations across EU borders. Such an environment being instantiated through the CISE network is political, organizational and legal and spans across the seven relevant sectors and user communities: transport, environmental protection, control of fisheries and borders, general law enforcement, customs and defence.

The content of the paper originates from the H2020 ANDROMEDA project [5] that commenced in 2019, which in essence aims to unlock the capabilities of the CISE by both enhancing the maritime CISE models and extending the scope to land surveillance. The project is heavily inclined towards demonstrating the CISE features in sev-

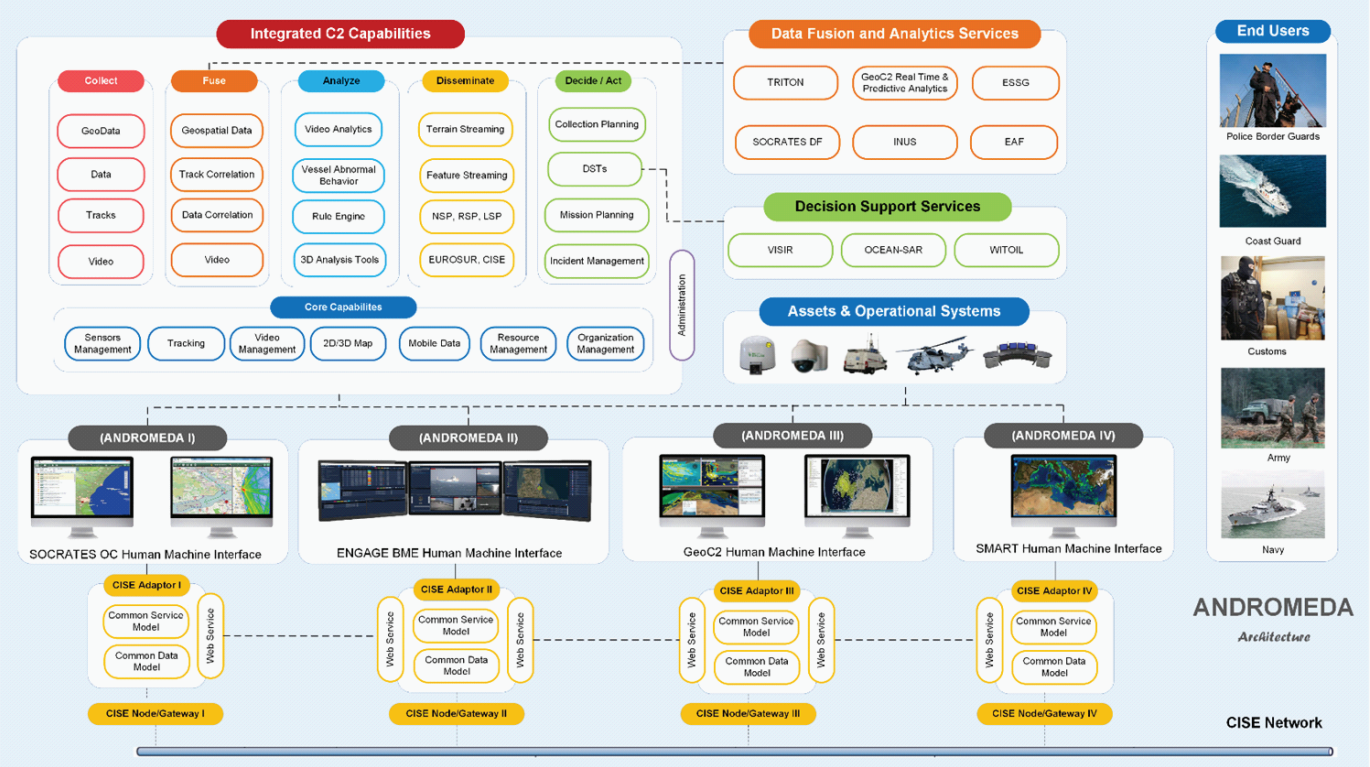

Figure 1 The ANDROMEDA project integrated enhanced CISE Architecture

Source: ANDROMEDA project [5]

eral trial use-cases being conducted across the borders of Europe. The trials are showing CISE compatibility, exchanges and interconnections with existing Command & Control (C2), Data Fusion (DF) and Decision Support (DS) systems in the involved European maritime and land agencies. The ANDROMEDA adopted CISE architecture is shown in Figure 1, where the specific surveillance systems deployed in each partner's country (Socrates in Spain, Engage in Greece, GeoC2 in Portugal, Smart in Italy) all connect to the EU CISE network using the CISE Adaptors and facilitate the interconnections through CISE Nodes (or CISE Gateway if the functionalities are more basic and relate to solely facilitating the network connections). AMSPM is involved in the ANDROMEDA project (as an End User) in a specific arrangement of the collaborative CISE development through a "restricted" research and implementation membership. One of the demonstration trials in the project is in the Ionian-Adriatic seas region that occurred in March 2021. The trial's aim was rendering of the common operational picture instances between the Greek, Italian and Montenegrin (i.e AMSPM) partners involved for detection of human trafficking, common interventions during maritime accidents, improved detection of threats and shortening of the existing C2 and DS timelines. The technical framework for the AMSPM's participation in the CISE trial is shown in [6]. Furthermore, experience in proxying the AMSPM connection to the CISE during the Ionian-Adriatic trial over a high-level operational C2 system: Socrates (provided by GMV, Spain www.gmv.com/en/Products/socrates/), is documented in [7].

We dedicate a few words on the motives for this research and the main contributions of the paper. The underlining working assumption applied in this paper is that the process of EU accession of Montenegro, currently an EU candidate member state, will be successfully resolved in the following years. Desirably, there will be a prior decision to allow unrestrained modality of operation within the EU CISE network in the meantime. This is currently being sought after by AMSPM acting as the national stakeholder, which is associated with and conforms to the mutual agreements with the national ministerial bodies and specific executive maritime security and safety institutions: Border Police sector and Navy (with Army). The current situation with the EU position on the CISE expansion is stated by the CISE governance structure specifying that during the current *transitional* stage of CISE, only EU member states can participate either as active participants or as observers. It is colloquially conveyed that the *transitional* phase of CISE is temporary and that the EU, together with its CISE Stakeholder Group, is working rigorously to extend the CISE initiative further. This work reflects and supports the foundational processes required in assessing and pursuing the CISE implementations. These are motivated by the Montenegro initiate but deemed as relevant to any similar considerations. Participations in the CISE are voluntary and collaborative. It is most fittingly decided upon and planned by any stakeholder if there is a comprehension of all implications of the immediate use of the CISE, as well as implicit and long-term projections of its benefits as a technology investment. To the best of our knowledge, such an analysis is currently absent in the literature.

Content of this paper is organised as follows. Section 2 gives a justification for the CISE adoption in the country. Section 3 then explains the models of interconnections both with the EU CISE network and internally in Montenegro. Section 4 outlines a feasibility analysis at this stage of pondered deployment and Section 5 concludes the paper.

2 Justifying adoption of CISE in Montenegro

2.1 Drafting a case for CISE implementation

Currently, maritime situational picture or Common Operational Picture (COP) is provided by the stand-alone conventional maritime surveillance systems and cooperation mechanisms running between the countries (e.g. Vessel Traffic Service – VTS). One such system is run by AMSPM and operationally centred close to the port of Bar with additional three remotes sites, several boats and various equipment distributed along the comparably small coast of Montenegro stretching over 294 km. This system is able to trace, track, enquire and inspect vessels crossing South Adriatic region and uses the Vessel Traffic Monitoring Information System (VTMIS) as the interface for visibility and exchange of data (e.g. AIS, radar, meteo) over a dedicated set of legacy information exchange protocols, e.g. IVEF – Inter-VTS Exchange Format. Integrated maritime surveillance is one operational segment within the responsibilities in the Montenegrin national maritime joint operations. These are combined with executive powers of the Border Police and the Navy, and, under governance of the national ministerial bodies. In specific cases of the joint operations such as Search and Rescue at sea and/or sea pollutions, AMSPM coordinates activities at the sea, and the rest of the institutions' assets (e.g. boats) are at its disposal, command and coordination. The CISE features would extensively augment the situational awareness by detailing and ubiquitously extending the reach of the national coverage and by improving the regional interconnections.

Analysis presented in this paper commences with a comprehensive awareness and assessment of the maritime surveillance requirements in Montenegro especially highlighting the country's small size and its current systems. As inherent in the CISE definition and subject to its potential deployment in Montenegro, the common environment for information exchange would include the following specific features regarding maritime surveillance and operations:

1) *Increased volume and richness of information retrieval and awareness in the maritime domains.*
2) *Installation of a technological platform for advancement of the capabilities in wide-ranging related fields in maritime surveillance and affairs.*

3) *Extending the CISE features such as to land border surveillance.*

Increased surveillance visibility in the maritime regions (see 1)) in the Adriatic (and Ionian) would mean an augmented view of the country's waters and bordering sea regions, via interconnections with neighbouring countries, i.e. Italy, Albania, Croatia. These CISE-enabled capabilities come through implementations of its functional components such as CISE Gateways, Nodes and Adaptors.

In addition to the increase in visibility of objects such as vessels, CISE would increase the volume and context of information shared per each instance, i.e. resolution of information, details, accuracy etc. Namely, information entities/objects would increase compared to what is monitored currently as CISE Data and Service models are continuously being extended to include information context such as: anomalies, incidents, documents and comprehensive improvements to the situational awareness in maritime surveillance. The original CISE Data Model composition of data entities is depicted in Figure 2 (UID stands for Unique Identifier) initially defined in FP7 EU project CoopP (Cooperation Project Maritime Surveillance) [8]. It is constantly being perfected [9] and extended as conducted in the ANDROMEDA project [5] with new data entities that describe further surveillance situations and details being observed.

The CISE enables extending the interconnections inside a country by allowing ubiquitous information flows for creating a truly common national environment for information sharing, retrieval and interpretations. National support for CISE implementation would ensure interconnections of different organisations and their legacy systems via the adaptation features and through a suitably developed national CISE architecture model interfaced with the European CISE network. Accordingly, information richness and situational awareness throughout the country would increase. Such a transcending country-wide capability between the organisations dealing with segments of maritime surveillance in Montenegro is non-existent at the moment, i.e. there is a lack of a common maritime digital environment between the security, military, transport, tourism, fisheries, commercial sectors etc.

In the first stage of CISE implementations, the primary objectives are the translations and exchanges of data, and, facilitation of the basic services between different organisations and their legacy systems. This means that the full-scale national CISE network, data and service model implementations, as envisaged, might not be the immediate objective for joining organisations such as AMSPM or police. Their legacy systems are already operational within the current scope. The CISE offers controllable and gradual augmentation of the existing capabilities (see 2)), via collaborations,

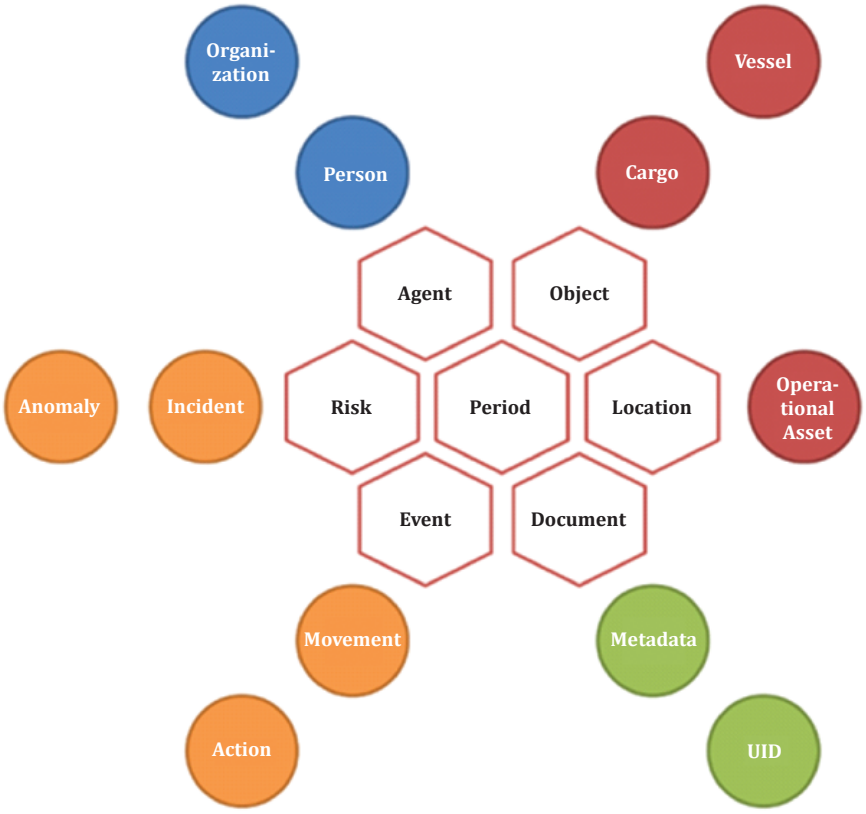

Figure 2 The original CISE Data Model

Source: [8]

interconnections and translational features towards ultimately establishing it as a full-scale solution. Thus, CISE deployment follows a top-down approach that initially needs to be spurred, envisaged and planned as a strategic investment on the national and regional scale. Its wide-reaching economic benefits emanate upon it becoming (fully) collaborative as a universal technological platform (similar to the Internet model) for maritime surveillance.

The translational features between legacy systems and CISE are to enable linking, interpreting and sharing information at the national and cross-border/EU levels in both directions of data exchanges and subject to a variety of deployment scenarios. It is reiterated that being part of the CISE means that the maritime surveillance features from the EU CISE network and bordering countries become partly available in Montenegro contributing to the effectiveness and value of their proxy capabilities inside the country. The same condition applies to the reversed benefit to all members/neighbours in the EU CISE network. In fact, one of the foundational design principles of the EU CISE network established in the pioneering project EUCISE2020 [10] is the "Responsibility to Share". In simple terms, this means that when connected to the EU CISE network, a member ought to equally provide as well as receive information. Very importantly, being part of CISE for Montenegro would also mean an open working facility for extending the existing features in maritime surveillance (see 3)), as plugins for existing legacy tools for: translations design, web service, DF, DS and C2. The CISE is a work-in-progress initiative, with continuous extensions of data models, services and opportunities for local and EU-wide development projects and initiatives. In several EU research and innovation projects including the recent MARISA [11] and the ANDROMEDA [5] projects, services are being developed along the idea of constructing the advanced service layer of the CISE Node. Furthermore, the running EFFECTOR EU project develops generic data processing tools to augment the CISE network interconnections [12]. Adapting to and keeping up with these upgrades facilitates growth of the local skills and knowledge in areas related to operations and maintenance, engineering, research, administration, data processing and many more.

The CISE is being extended for land border surveillance (see 3)) thought the current EU project driven process (ANDROMEDA project [5]). Such a deployment environment would necessitate repeating the above analytical processes as conducted for the maritime surveillance and replacing some of the organisations at both the national and regional levels. In the analysis conducted in this paper, we remain focused on maritime surveillance being the objective of the existing CISE specifications and the current functioning of the EU CISE network.

2.2 Framework for feasibility and cost-benefit analysis

Analysis of the CISE deployment feasibility/cost-benefits in Montenegro can consider two distinct realisation stages:

1) *Initial, AMSPM-anchored, ANDROMEDA implementation, with CISE translations and link up with the EU CISE network.*
2) *Fully-fledged country-wide CISE network implementation in Montenegro, with internal CISE interconnections and a common national CISE environment, in addition to also being a part of the EU CISE network.*

Subject to these thresholds in the extent of the CISE implementations, a practical deployment strategy and associated assessments need to accompany the feasibility and cost-benefit study. These practical considerations can basically assess several technical and economic prerequisites and the CISE features towards shaping of the deployment scenario(s):

- Scale of the CISE network in Montenegro, subject to setting up of the scenarios of deployment in the country.
- Resolving the objectives behind the two realisation stages: a) only as the transitional feature connecting to the EU CISE network and as a limited bridging facility between various legacy systems and organisations nationally, and/or, b) as a stand-alone open network backbone service to grow into a country-wide system with comprehensively integrated CISE services and data models. The latter feature would ultimately allow visibility and data exchanges via standalone CISE tools progressively embedded in organisations rather than via adaptations of internal legacy systems used in each organisation involved.
- Numbers and interconnections of CISE entities within the country and with the EU network: CISE Node/Gateway (forming the CISE network) and CISE Adaptors (towards legacy systems) (i.e. also called Andromeda Hubs in the ANDROMEDA project as they facilitate translations of the newly added features to the existing CISE network through the project [5]) would follow the previous point. This constitutes the practical scale of the network, its purpose and sets up a path for its evolution. Engineering know-how is required for solving the translational features of each CISE Adaptor and the structure, syntax and many accompanying protocol features of the legacy information protocol used within each organisation. E.g. IVEF-to-CISE translations are XML (Extensible Markup Language) – like structure and syntax translation processes. These achieve parsing and transferring of AMSPM's VTS system data model and associated meanings to and from the EU CISE network (e.g. AIS and radar data). In the ANDROMEDA project, a trial with AMSPM's IVEF-to-CISE translation is planned off-the-premises at GMV's cloud in Spain where the CISE Adaptor is located with a direct connection to IVEF [13] source in Montenegro. The connection is appropriately "firewalled" at both endpoints in Montenegro and Spain by specific filters that enable total control over the shared information and its destination [6][7]. No hardware nor significant software upgrades are required at AMSPM. E.g. the adaptation/

translation process means a transformation from one standard such as IVEF to the CISE standard and vice versa. This might mean a field-by-field translation process making the correlations [6]. In some cases, for example with data class – Type (enumeration) the translations would need to be 'forced' as the values might not exactly match. An example is IVEF construction that contains:
LloydsShipType = "70">< / *Construction>*, where value 70 corresponds to AIS description "*Cargo, all ships of this type*". The CISE Data models specify many ranges of Cargo data entity descriptions under *Cargo Core Entity*, including numerous ***Cargo Type class*** descriptors such as LARGE FREIGHT CONTAINERS, PALLETIZED etc. with corresponding description for each of them [14].

- Decisions on information exchange frequencies and responsiveness, real-time requirements for data visibility, security, control and administration are all fragments that determine the scale and complexity of the deployment. Naturally, they are linked to deployment scenarios in the country.
- Small coastal countries have limited human resources and infrastructure related to maritime affairs requiring a calculated verdict on the viability of the CISE deployment.

3 Options for commencing the CISE deployment in Montenegro

The main starting objective of the initial CISE deployment in Montenegro is twofold: facilitate interconnections with the existing EU CISE network, while realising CISE services inside the country at AMSPM, and, gradually integrate other national stakeholders/organisations through it. Foundational work on CISE architectural deployment frameworks inside EU member states have formulated several models. These are constituted around the setup of the CISE interconnectivity provider(s) inside a country and facilitation of the link up with the EU CISE network [15][16] (see Figure 3). From these options, the most convenient foundational model that practically suits a small country of the size and maritime costal region of Montenegro is the "Single National Provider of CISE Services" [15]. Such a model would be formed around a national authority, or authority-appointed stakeholder that manages the CISE services inside the country and towards the EU CISE network, i.e. AMSPM.

Having a single focal position for the CISE deployment is quite suitable for a small country. It allows easy establishment of the CISE functionalities (i.e. data models and services) that initially need to be translated and bridged towards the outer EU CISE network. Consequently, knowl-

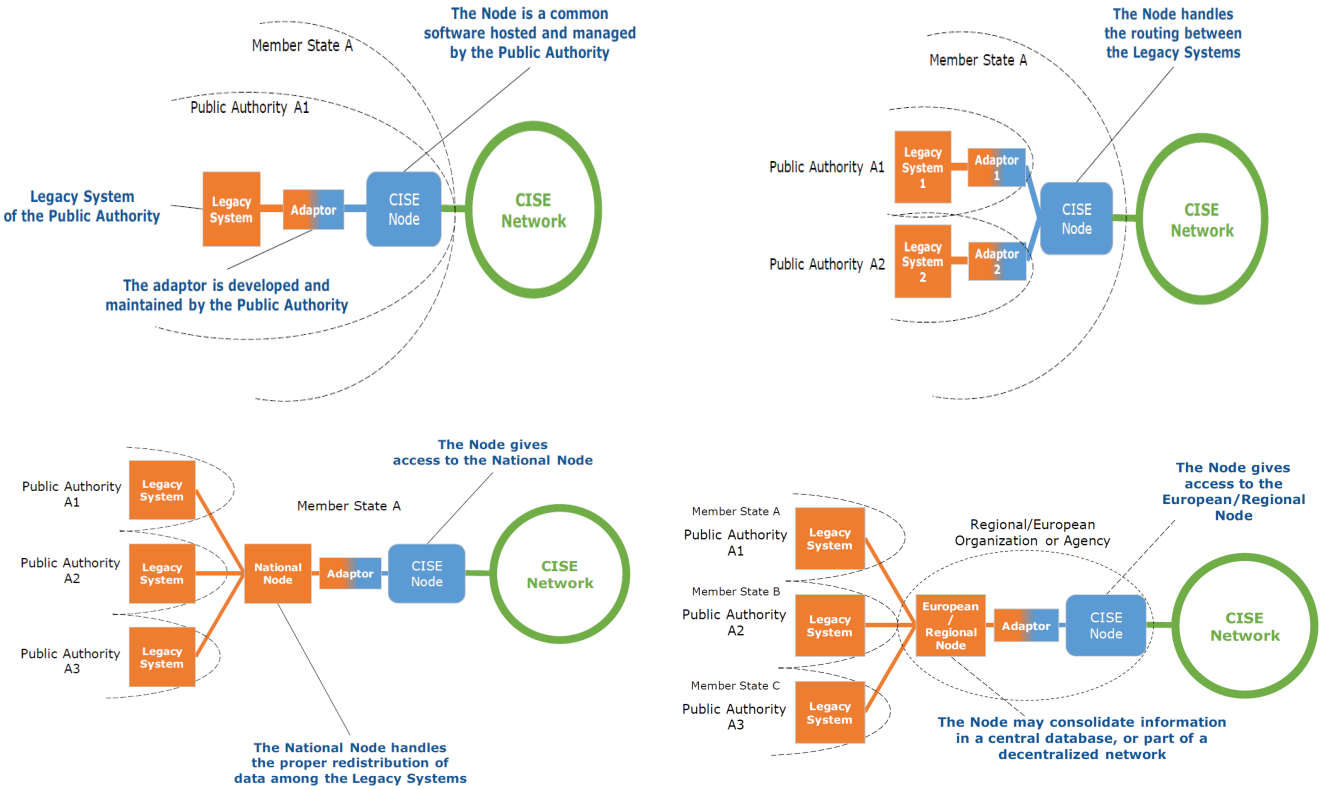

Figure 3 Four examples of connecting to CISE network based on location and ownership of the connecting CISE Node

Source: [16]

edge and skills required for implementing these system components would be focused and would consequently accommodate for potential expansion of stakeholders and user communities.

As formulated in the foundational CISE architecture visions [15][16], the initial single provider model, or in fact even the other models specified that are based on multiple providers and user communities, could all eventually transform into a "hybrid architecture" with different setup of stakeholders. In this paper, intention is to analyse the related aspects when CISE deployment starts from scratch in Montenegro for which case the most fitting starting model is based on the "Single National Provider of CISE Services". AMSPM would duly obtain the national support for commencing the CISE deployment, e.g. via Ministry of Transport appointment and support of other involved national authorities. Accordingly, CISE facilitated **Montenegro maritime situational picture** (also adding the neighbouring countries' CISE partners' data besides the current exchanges) would be rendered and maintained by AMSPM either partly by the restricted information available to AMSPM, or, in a comprehensive manner by gathering the information from other national maritime authorities/stakeholders in the country. This is conditional to the agreement(s) between the national authorities on sharing and ownership of the information. This Montenegro maritime situational picture is to be shared with the CISE EU partners according to the "Responsibility to Share" design principle and access rights matrix [17]. At the national level, some of the involved maritime surveillance organisations with their legacy systems, which can ultimately play a part in the CISE interconnections via the single national provider/AMSPM are: police, customs, navy, army, fisheries, tourist organisations, all national and commercial ports, universities (for research, trialling, knowledge and educational purposes), ministries, government, and, (if allowed) associated companies. Recently, a similar nationwide involvement of stakeholders/institutions in Montenegro [18] was pondered upon in the EU COMPASS2020 project's model dealing with a deployment of novel maritime surveillance assets [19].

From the general technical point of view, the architecture is constructed around the placement of typically one CISE Node, which is practically the immediate point of entry into the CISE network. Since AMSPM is to be the starting provider of the CISE services in the country, it is primarily the question of how the starting linkup with the EU CISE network is achieved that subsequently draws upon various implementation issues and analysis. There are already several models of architecture visons and their framework instantiations [15][16] and organisational structures. These are based on the pivotal CISE Node's location, ownership and connections from the side of the joining state and its stakeholders with their legacy systems. Relevant organisational structures, copied from [16], are shown in Figure 3 organised around the CISE Node placement:

i. (top left) a single stakeholder connects **directly** to the CISE network (e.g. AMSPM connects to EU CISE Network) by adapting its legacy system and owning a CISE Node.
ii. (top right) several stakeholders connect to the CISE network by using a **single CISE Node owned by one of the stakeholders** (e.g. AMSPM as the owner proxying connections for other stakeholders).
iii. (bottom left) the country establishes a **shared National (CISE+) Node owned by one of the stakeholders** and having access rights and information control for access to and from the EU CISE network and national interconnections (e.g. AMSPM as the owner manages and proxies connections for other national stakeholders).
iv. (bottom right) using a Regional/European Node and/or **proxy owned external CISE Node** to connect to the CISE Network (e.g. AMSPM can be a gateway for connection to CISE Network through an external EU partner).

Evidently, at the initial stage of implementation, one of the main operations in launching the CISE services is in adaptation of legacy system(s) towards the CISE network. This requires translations of data models and meanings to and from the CISE network and bridging each of these legacy systems inside the country with an appropriate level of security [17]. At the time of the writing of this paper, EMSA (European Maritime Safety Agency) [16] is drafting a common contract model for information sharing inside the CISE consortium, which would replace the current approach of the bilateral contracts.

4 Initial feasibility considerations

We can draw parallels with a similar starting feasibility consideration conducted for National Maritime Single Window (NMSW) [20][21] implementation in Montenegro also facilitated via its anchoring at AMSPM and involving many maritime stakeholders. Although related to a rather non-overlapping segment of maritime affairs, this example further strengthens the candidacy of AMSPM as the national authority stakeholder being technically and administratively suitable for carrying out the implementation of the linkage to the EU CISE network. Operational coupling of the single or hybrid national CISE provider models with NMSW provider was hinted at early in the architecture visions for CISE deployments [15]. Besides, these initial feasibility considerations can provide much support to AMSPM in negotiations with the national authorities and other CISE stakeholders in Montenegro. Similar to the example of the extent of the Montenegro maritime situational picture that would be shared with the outside EU CISE network members as mentioned in the previous section, AMSPM is the anchoring entity in distributing information from CISE network internally to other stakeholders in Montenegro. E.g. a cargo vessel that departs from a

Mediterranean port with destination to Montenegrin port of Bar is approaching the port and is visible through the CISE network on its approach. There are other authorities interested in the CISE data about the vessel (customs, police, military etc.) that would extract the relevant CISE data entities' content that are embodied in the CISE *Vessel Service* for the particular vessel.

Another important distinguishing feasibility consideration is related to the top-down property of each CISE implementation strategy as the facilitating technological platform for maritime surveillance. Business model perspective is void of an immediate revenue generating component such as application of fees used in NMSW [20]. Deployments of CISE features are applied towards evolutions of operational capabilities, not as an immediate capacity to attract customers or charge CISE connections and service deployment (e.g. to vessels or connecting stakeholders). It is therefore important to initially observe the implementation of CISE as a national (and European) master plan mandated to AMSPM in Montenegro. The cost and benefits can therefore be seen as both immediate and long term investment returns especially if the fully-fledged country wide CISE implementation is ultimately achieved (see Section 2.2) in the same context of European CISE network expansion and success.

4.1 Identifying the essential costs

At the initial stage of implementation, operational aspects that constitute the foundation for feasibility analysis are:

a. Investment costs of setting up of the CISE features and adapting and interconnecting the legacy system(s) (quite analogous to conventional CAPEX expenses):
- Initial hardware and software (HW/SW) installations of the CISE technicalities and components.
- CISE features for interconnecting with the EU CISE network, adaptation/translations with the legacy system(s) and (optional at the start) national CISE interconnections between the legacy systems.
- Trainings of personnel for conducing operational tasks.

b. Maintenance costs of the operational runtime being dependent on the organisational structure of CISE (similar to OPEX) that can involve several critical tasks mostly related to personnel:
- Engineering costs of keeping up the operations of hardware (e.g. CISE Node) and essential software components.
- Continuous design and inspection of adaptation/translation features between CISE and legacy system(s) and facilitation of CISE interconnections at national level.
- Overlooking the required changes and evolution of the national CISE systems.
- Continuous education, monitoring, participation and liaising with the European CISE development activities and expansion of the network for maritime surveillance.

c. Dedicated expansion costs from a starting organisational structure and towards ultimately a fully-fledged country wide CISE network implementation (section 2.2):
- Assuming that one standard national implementation of the CISE Adaptor features between the CISE network and a legacy system is reasonably light in terms of costs and effort (e.g. for top left organisational structure in Figure 3), applying the same for each separate legacy system of the joining national stakeholders is a multiplication of this task and not a straightforward extension of the existing features (e.g. software installation and maintenance costs) as the legacy systems commonly differ in all relevant technicalities to the adaptation process.
- Ultimately, as a long-term ambition, replacement of (many) legacy systems data and service models. This aspect partly includes replacements of obsolete parts of the legacy systems that cannot be further upgraded/updated as the CISE components expand (these could also be associated with the investment costs subject to a scenario).
- Dedicated or related research.

The actual figures behind each cost and weighing of each one of them is proportional to the total cost and is subject to the situation and pricing in each country. Hence, the actual figures can vary as the overall costs are subject to national contracts and the authorities and agencies involved in the design, production and deployment of the needed HW/SW and other components, as well as the way in which the costs of personnel are calculated for each stage and purpose of operations.

4.2 Discussion on the expected benefits

Expectedly, the CISE implementations start small and expand gradually from an anchoring authority that installs the first instance of the CISE configuration. At the current stage of realisation of the CISE systems at national levels across Europe, even a large country of the size of Spain has commenced the implementation via the single provider model: The Spanish Navy has bridged and interconnected national stakeholders such as Customs, Border Control, Fisheries, Defence and Maritime Surveillance agencies and all companies associated with maritime surveillance and Search and Rescue. At the time of the writing of this paper, the Spanish Navy operates the top right configuration from Figure 3, as it owns the CISE Node while the other legacy systems belonging to the connected national stakeholders have their CISE Adaptor at their premises. Extent of the information sharing between the stakeholder gets continuously agreed upon. Similarly, the

Finnish CISE implementation opted for the same configuration (also termed as CISE Configuration B [10]). In Finland, the Finnish Border Guard is the stakeholder on behalf of the Maritime Authorities Consortium (FIMAC) in CISE. The FIMAC consist of Finnish Border Guard, Navy, Transport and Communication Agency and Transport Agency. The Transport and Communication Agency and Transport Agency are actively sharing information in the CISE network. Due the classification of the CISE network, the Finnish Navy and Border Guard are not physically connected to the CISE network. A breakdown of costs from the recent Finnish CISE implementation and their brief decomposition into a useful approach and experience for the CISE essential costs identified in the previous subsection, are given in Table 1.

In a manner of observing the CISE benefits from a reversed perspective, when it would eventually become implemented in a fully-fledged manner, the achieved benefits are enormous at all levels (being the very intention of the CISE development by EU). Stakeholders, states, regions would benefit by simplified, standardised and converged maritime surveillance capabilities and a manifold reduction in human and equipment expenses required for each legacy system (excluding opportunities via the

Table 1 Indication of Costs in the Finish example and general remarks

Investment Costs (CAPEX like)	
HW/SW installations	***Finnish case***: Initially consisting of the CISE Adaptor/Gateway designs, productions and installations and the VPN configuration. The CISE Adaptor design was the most expensive and time consuming, amounting to approx. 100 000€. Part of the CISE Adaptor design costs can be related to the next bullet/box. Having the current knowledge and understanding, the CISE Adaptor cost could be reduced to upwards from 40 000€. Highly dependent on numbers and types of legacy systems to be connected on CISE, the services and data provided/consumed etc. CISE Gateway/Node design and VPN configuration were under the outsourced agencies' service contract, thus only estimated to around 20 000€. CISE Gateway/Node production and installation were approximately 6 000€.
– Connection to EU CISE – Adaptation/ translation to legacy systems – National CISE interc.	***Finnish case***: The deployment costs were approx. 10 000€ including the VPN maintenance and connections to servers. CISE network VPN configuration in Finland was initially part of an innovation and research project. Two out of four involved authorities provided limited information to the CISE network sharing them via the information Transport Agency's CISE Gateway. Navy and Border Guards had their own CISE Adaptor (as the Transport Agency) but due the public classification of the CISE network, these were not open and no information were shared from them.
Personnel training for operational tasks	***Finish case****:* Personnel implicitly involved and trained as part of the CISE research and innovation project. No dedicated personnel training.
Maintenance Costs (OPEX like)	
Engineering HW/SW oper.	***Finnish case****:* The maintenance is part of outsourced service agency contract costs.
Continuous design and inspection of CISE bridging with leg. sys. and national CISE interc.	***Finnish case****:* Configuring and running the VPN at the beginning was the most time consuming. The VPN configuration includes both CISE network and RTI network (RTI installed/ deployed the CISE Gateway software remotely). This part can also relate to the Investments cost for the relevant components.
Overlooking the national CISE changes and evolution	***Finnish case****:* The Finnish Maritime Authorities Consortium (FIMAC) decided the national evolution, from the operational point of view. CISE is still a research and innovation initiative. In terms of the practicalities of the technical changes and evolution, these are part of Transport Infrastructure Agency's service contract.
Continuous education, monitoring, participation and liaising with the EU CISE develop.	***Finnish case***: Assumed as the responsibility of each stakeholder. LAUREA – University of Applied Science was part of CISE as a research institution. For any responsible involved stakeholder these costs can be calculated indirectly as part of the research and innovation projects (national or European).
Dedicated Expansion Costs	
Expanding CISE adaptat. features	***General Comment****:* Subject to each countries' extent of the CISE deployment and often independently handled by each stakeholder.
Replacement of legacy systems' data and models	***General Comment***: Relevant to enhancements of the CISE Adaptor and/or Node as legacy systems stay unchanged due to the CISE design principles. Interconnections can be related to CISE networks, internal/ external, i.e. via VPN, e.g. in a Restricted or Confidential mode.
Research	***General Comment***: At this stage still indirect via participations in research projects. Likely, to be handled by each stakeholder in the future. Can expand to academic and star-up related research.

Source: Authors

equally auspicious land border surveillance in this analysis for the time being upon its ultimate formulation via the ANDROMEDA project). But this is the ultimate goal and needs to be justified by the intermediate investments and costs. As stated earlier there is no direct revenue generating mechanism and majority of the quantifiable benefits are implicit or tangible in retrospective upon the fully-fledged implementation. This is quite similar to the basic view of the Internet model, being the facilitator for a novel way of communications and opportunities. It was originally reiterated that "**CISE is not a system**"[1] (EUCISE project media presentation link in [10]), rather "*it is a set of agreed specifications for an interoperability layer which, once implemented, will ease information exchange*". This makes it very analogous to the OSI Presentation Layer features extended to physical and cyber domains of maritime surveillance, i.e. it builds upon XML/JSON compositions of the CISE Data Models. Fitting to this general interpretation of the CISE model would be a European or a country-wide implementation of the CISE features over a cloud structure for the relevant services. This is a possible outcome of the CISE development in its m*ature stages.*

The CISE Adaptor takes care of "translation" of the shared information to and from the legacy systems. The current implementations use the REST/SOAP APIs with web services and conventional PULL, PUSH, SUBSCRIBE communication patterns meaning that the translation to and from CISE Data Models are underlying presentation layer processes within the mechanisms already used. While envisaging that the future versions of some legacy systems might include the CISE data model syntax and structure, constant adaptations/translations are most likely still inevitable requiring dedicated designers' interventions. Thus, CISE Adaptor emerges as extremely important to the Montenegro case where its complexity or customised features (e.g. solely focus on entities of interest to AMSPM, such as *vessels*) might incur benefits, subject to it being constantly updated with new CISE data models and services. In the case of Montenegro, the starting models applied in Spain and Finland are equally applicable, i.e. top right configuration from Figure 3, where there are many CISE Adaptors connecting over a single CISE Node. Following this discussion, it remains equally recommendable to consider and deploy the bottom left configuration from Figure 3 where all CISE Adaptor features are centralized and facilitated over the CISE National Node, to be run by AMSPM. For the small country of the size of Montenegro this feature might reduce the cost of multiple CISE Adaptors implementation, as the security and access rights can be mandated to AMSPM and where all the adaptor/translation features are centrally placed making their design, maintenance and customisation to requirements of each legacy system in Montenegro conveniently manageable. Quantifying CISE benefits for all stages of implementation, for a small country such as Montenegro draws out an immediate conclusion of a significant benefit: focusing the knowhow and investments on a single CISE operational model for all involved national stakeholders/organisations is especially suitable. The capabilities are increased while comparably not losing much in readjustments of systems and personnel in already small scale operational and organisation capabilities and structure. It is expected that such benefits are less emphasised for a larger country, getting rid of a significantly larger and bulkier existing operational infrastructure.

[1] Although it is not misplaced to refer to it as a system in general descriptions of it.

5 Conclusions

Use and advancements of the European initiative for interoperability of the diverse legacy systems in maritime surveillance through a common shared environment – CISE, is gaining momentum via many collaborative efforts and real trails. Endorsements of the CISE technology inside countries as an augmenting operational patch of the exiting surveillance legacy systems is a well-informed executive decision. It usually requires forethoughts beyond just extending the existing operational features. The CISE commenced as a collaborative platform and a tool for extending the surveillance capabilities by facilitating interconnections between EU and national stakeholders. As such, it is an investment choice and it necessitates a combination of understanding of the deployment options, together with opportunities in expanding each of their features. It is generally assumed that if the CISE is realised at each national and EU-wide level in a fully-fledged manner, benefits would be far reaching and enormous at both the technical and economic-impact levels. But to reach that stage, many individual implementations need to assess both the immediate benefits and feasibility of pursuing the prospect of the CISE roadmap.

We analyse many technical prerequisites for introducing the CISE in Montenegro, subject to this being initially executed through AMPSM as the Single Provider of the CISE services. Three major costs are differentiated in this study: investments, maintenance, and dedicated expansion costs, each particularly relevant to an implementation stage of the CISE deployment. Finally, we elaborate on the specific benefits of the deployment options and technicalities (e.g. CISE components) and progression of the CISE features inside the county. To support the analysis, a recently conducted Finish implementation is outlined and the costs incurred are reviewed. It is concluded that the CISE feasibility is to be ensured as a relatively modest commercial investment in technology. However, it is a continuous process of gaining skills and know-how, as the EU-level collaborations expand and improve and these are appropriately reflected in the national level implementations.

Funding and Acknowledgment: This work has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No

833881. This article reflects only the author's views and the Research Executive Agency (REA) is not responsible for any use that may be made of the information it contains.

Author Contributions: Conceptualisation: Andrej Mihailovic, Nexhat Kapidani, Enis Kočan. Research: all authors. Writing: Andrej Mihailovic. Review and Editing: all authors.

References

[1] FRONTEX – European Border and Coast Guard Agency, "Risk Analysis for 2016," FRONTEX, Warsaw, Poland, 2016.

[2] G. Kessler, P. Craiger, and Jon Haass, "A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System," The International Journal on Marine Navigation and Safety of Sea Transportation, 12, no. 3 (2018): 429-437.

[3] Integrating maritime surveillance in Europe: Common information sharing environment (CISE), draft roadmap, 20.10.2010, https://ec.europa.eu/maritimeaffairs/publications/integrating-maritime-surveillance-common-information-sharing-environment-cise_en.

[4] European Border Surveillance system (EUROSUR), webpage: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/border-crossing/eurosur_en.

[5] ANDROMEDA EU Project – "An Enhanced Common Information Sharing Environment for Border Command, Control and Coordination Systems," Grant agreement ID: 833881, 2019-2021, https://www.andromeda-project.eu/.

[6] A. Mihailovic et al., "A Framework for Incorporating a National Maritime Surveillance System into the European Common Information Sharing Environment," *2021 25th International Conference on Information Technology (IT)*, 2021, pp. 1-6, doi: 10.1109/IT51528.2021.9390138.

[7] Z. Paladin, A. Mihailović, N. Kapidani, D. M. Delgado, J. M. G. Nogueron, G. Vella, M. Moutzouris, R. Leuzzi, "Augmenting maritime Command and Control over a regional Common Information Sharing Environment implementation: Montenegro Case," NMIOTC – NATO Maritime Interdiction Operations Journal, Edition: 22, Publisher: NATO Maritime Interdiction Operational Training Centre, July 2021.

[8] D. Berger, J. Hermida, F. Oliveri, G. Pace, "The Entity Service Model for CISE – Service Model Specifications". Technical Report, Joint Research Centre of the European Commission, 2017, online: https://webgate.ec.europa.eu/maritimeforum/en/node/4039.

[9] M. Riga, E. Kontopoulos, K. Ioannidis, S. Kintzios, S. Vrochidis, I. Kompatsiaris, "EUCISE-OWL: An Ontology-based Representation of the Common Information Sharing Environment (CISE) for the Maritime Domain," Semantic Web-Interoperability, Usability, Applicability Journal, Accepted for Publication in 2020.

[10] EUCISE EU Project – "EUropean test bed for the maritime Common Information Sharing Environment in the 2020 perspective", Grant agreement ID: 608385, 2014-2018, http://www.eucise2020.eu/about.

[11] MARISA EU Project – "Maritime Integrated Surveillance Awareness," Grant agreement ID: 740698, 2017-2020, https://www.marisaproject.eu/.

[12] EFFECTOR EU Project – "An end to end Interoperability Framework for Maritime Situational Awareness at Strategic and Tactical Operations," Grant agreement ID: 883374, 2020-2022.

[13] The open Inter VTS Exchange Format, http://openivef.org/.

[14] ANDROMEDA PROJECT Deliverable D3.1 "D.3.1 e-CISE Data Model description," Public deliverable, 2020, https://www.andromeda-project.eu/downloads/index.html.

[15] CISE Architecture Vision Document, 6.11.2013, http://www.eucise2020.eu/media/1070/cise-architecture-visions-document-v3-00.pdf.

[16] European Martime Safety Agency (EMSA): CISE Technical Specifications, http://www.emsa.europa.eu/cise/technical-specifications/download/5798/3689/23.html.

[17] J. Rajamäki, I. Tikanmäki, J. Räsänen, "CISE as a Tool for Sharing Sensitive Cyber Information in Maritime Domain." Information & Security: An International Journal, 43, no. 2 (2019): 215-235. https://doi.org/10.11610/isij.4317.

[18] A. Mihailovic, N. Kapidani, E. Kocan, A. Nadziejko and A. B. Monteiro, "Towards Augmenting Maritime Surveillance Capabilities via Deployments of Unmanned Aircrafts and Autonomous Underwater Vehicles," 14th NATO Operations and Research Conference, virtual conference, 5-6 October 2020, doi: 10.5281/zenodo.4399215.

[19] COMPASS2020 EU Project – "Coordination Of Maritime assets for Persistent And Systematic Surveillance," Grant agreement ID: 833650, 2019-2021, http://www.compass2020-project.eu/.

[20] N. Kapidani, E. Tijan, M. Jović, and E. Kočan, "National Maritime Single Window – Cost-Benefit Analysis of Montenegro Case Study," *PROMET*, vol. 32, no. 4, pp. 543-557, Jul. 2020.

[21] N. Kapidani and E. Kočan, "Implementation of national maritime single window in Montenegro," *2015 23rd Telecommunications Forum Telfor (TELFOR)*, 2015, pp. 17-20, doi: 10.1109/TELFOR.2015.7377385.