Grant Agreement Number: ***833389***

Project acronym: Cyber-MAR

Project full title: Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain

D.7.1: Communication Strategy and Plan

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389. The content of this document reflects only the authors' view and the European Commission is not responsible for any use that may be made of the information it contains.

Document Identification	
Status	Final version
Version	1.0
Related WP	WP7
Related Deliverable(s)	D7.4, D7.5
Lead Participant	SEABility (SEAB)
Contributors	ICCS, WMU, VTT
Due Date	Saturday, 29 February 2020
Submission Date	Wednesday, 04 March 2020
Document Reference	D.7.1
Dissemination Level	PU
Document Type:	R
Lead Author	Vasiliki Palla (SEAB)
Reviewers	Sophia Adam (ICCS) George Baroutas (ICCS)
	Johan Scholliers (VTT) Anna-Mari Heikkilä (VTT)

Legal Disclaimer

Document Information

List of Contributors	
Name/Surname	**Beneficiary short name**
Geli Latsa	SEAB
Eleni Krikigianni	SEAB
Sophia Adam	ICCS
George Baroutas	ICCS
Monica Canepa	WMU
Johan Scholliers	VTT
Anna-Mari Heikkilä	VTT

Document History			
Version	**Date**	**Change editors**	**Changes**
0.1	06/12/2019	Vasiliki Palla (SEAB)	Draft ToC of the initial Communication Strategy and Plan
0.1a	07/12/2019	Vasiliki Palla (SEAB)	Changes to the ToC – Allocation of required contribution
0.2	19/12/2019	Vasiliki Palla (SEAB), Eleni Krikigianni (SEAB), Geli Latsa (SEAB)	Input in chapters 1 & 2
0.3	02/01/2020	Vasiliki Palla (SEAB), Eleni Krikigianni (SEAB), Geli Latsa (SEAB)	Input in chapters 2 & 3
0.4	28/01/2020	Sophia Adam (ICCS)	Input in sections 3.1, 3.3, 8.1 and chapter 8
0.4a	30/01/2020	Monica Canepa (WMU)	Input in sections 3.1, 3.2, 3.3 and chapters 5, 6
0.5	13/02/2020	Vasiliki Palla (SEAB)	Integration of partners contributions in chapters 1 2, 3, 5, 6, 7
0.5a	13/02/2020	Vasiliki Palla (SEAB)	Integration of partners input in Stakeholders List and input in chapters 4, 8, 9, 10
0.6	17/02/2020	Vasiliki Palla (SEAB), Eleni Krikigianni (SEAB), Geli Latsa (SEAB)	Final refinements
0.7	26/02/2020	Vasiliki Palla (SEAB), Eleni Krikigianni (SEAB), Geli Latsa (SEAB)	Integration of Sophia Adam (ICCS) contribution

Document History			
Version	**Date**	**Change editors**	**Changes**
0.8	28/02/2020	Vasiliki Palla (SEAB), Eleni Krikigianni (SEAB), Geli Latsa (SEAB)	Integration of Johan Scholliers (VTT) contribution
0.9	28/02/2020	Vasiliki Palla (SEAB), Eleni Krikigianni (SEAB), Geli Latsa (SEAB)	Final Comments from Monica Canepa (WMU) and George Baroutas (ICCS)
1.0	29/02/2020		Final version to be submitted

Quality Control		
Role	**Who (Partner short name)**	**Approval Date**
Deliverable leader	SEAB	28/02/2020
Quality manager	UoP	28/02/2020
Project Coordinator	ICCS	28/02/2020

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
AB	Advisory Board
CERT	Computer Emergency Response Team
COPE	Committee on Publication Ethics
CSIRT	Computer Security Incident Response Team
DG	Digital Government
DMSF	Document Management System Folder
DoA	Description of Action
Dy.x	Deliverable number y belonging to WP x
EB	Executive Board
EC	European Commission
EMSA	European Maritime Safety Agency
ERC	European Research Council
ESPO	European Sea Ports Organization
EU	European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation
GNV	Grandi Navi Veloci
H2020	Horizon 2020
IA	Innovation Action
IAME	International Association of Maritime Economists
ICHCA	International Cargo Handling Coordination Association
ICIMP	International Conference on Internet Monitoring and Protection
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
IMO	International Maritime Organization
IPR	Intellectual Property Right
IT	Information Technology
KPI	Key Performance Indicator
MaCRA	Maritime Cyber-Risk Assessment framework
MSC	Maritime Safety Committee

Abbreviation / acronym	Description
MSx	Milestone number x
Mx	Month number x
OA	Open Access
Ph.D.	Doctor of Philosophy
PM	Person Month
POPD	Processing Of Personal Data
PSA	Port of Singapore Authority
PU	Public
R&D	Research and Development
RIA	Research and Innovation Action
SAB	Security Advisory Board
SME	Small and Medium-sized Enterprises
SSA	Security Sensitivity Assessment
WPx	Work Package number x

Executive Summary

Communication and dissemination processes are essential to assure the success of Cyber-MAR project. It is funded under the European Union's Horizon2020 Framework Programme and aims at fully unlocking the value of the use of cyber range in the maritime logistics value chain via the development of an innovative simulation environment adapting in the peculiarities of the maritime sector, but being at the same time easily applicable in other transport subsectors. A combination of innovative technologies are the technology enablers of the proposed Cyber-MAR platform, which is not only a knowledge-based platform, but more importantly a decision support tool to cybersecurity measures, by deploying novel risk analysis and econometric models. CSIRTs/CERTs data collected will be analyzed and feed the knowledge-based platform with new-targeted scenarios and exercises. Through Cyber-MAR, the maritime logistics value chain actors will increase their cyber-awareness level; they will validate their business continuity management minimizing business disruption potential. Cyber-MAR will act as a cost-efficient training solution covering the maritime logistics value chain.

The current document provides the developed communication strategy and plan, which is based on a five-pronged approach and includes the communication approach along with the relevant objectives. Furthermore, it offers a breakdown of the main relevant target audiences and also provides the key messages tailored to each target group in order to efficiently anchor the project's results and outcomes and to ensure that Cyber-MAR acquires high visibility, outreach and impact to all interested parties.

In addition, the present document describes in short the liaison plan that will be implemented within the project lifetime, while analyzing the role and effort of each Cyber-MAR partner. It presents also the main objectives of the communication and dissemination procedures, as well as the step by step procedure. Moreover, it also summarizes all the communication and dissemination activities that have been performed by partners the first six months of the project - M1 (September 2019) until M6 (February 2020) - as well as all the already planned activities and relevant opportunities. Reference is also given to the monitoring of both dissemination and communication activities' status through measurement of set of identified KPIs, which will systematically help on the evaluation of all communications and dissemination activities.

1. Introduction

This deliverable results from Cyber-MAR's *Task 7.1 – Cyber-MAR Brand Identity and Communication Strategy*. This task is part of Work Package (WP) 7 – High Impact Communications and Networking, which aims to develop the project's Communication Strategy and Plan, to establish high quality impactful activities, to coordinate the scientific outreach and to liaise with relevant R&D -national and european- initiatives. More specifically, Task 7.1 aims to serve as a guide for the consortium, so as to effectively allocate time and resources to maximize project impact.

This document contains all the important information needed to facilitate the communication and dissemination efforts of the Cyber-MAR consortium. It presents the Cyber-MAR project's dissemination and communication strategy and its implementation plan that will be used by the consortium in order to guarantee high visibility, accessibility and promotion of the project's vision, key findings and research results. Furthermore, it will ensure that impactful activities have been planned to engage stakeholders, create awareness and promote Cyber-MAR. The goal is the effective communication of project's assets, course and key outcomes to the identified target audiences.

This document thus is made to ensure that clear communication objectives have been set, key target audiences have been identified and well defined, tailored messages have been crafted per each target audience, the appropriate channels will be used, sufficient communication materials and resources will be produced and the right evaluation methods will be implemented.

1.1 Purpose of the document

Cyber-MAR's communication strategy and plan is designed to provide an initial, detailed and theoretical framework for the activities to be performed within the Cyber-MAR project. It constitutes an effective tool to amplify the impact of the project results and outputs, optimize their value and foster their active and concrete use in systems and practices at local, regional, national and European levels. The set of processes presented below will remain active throughout the project lifetime (in line with GA, Articles 29 & 38) to efficiently facilitate the project's consortium to reach a wide range of relevant audiences and at the same time disseminate and communicate Cyber-MAR's outcomes to the industrial, academic and SME domain.

More specifically, the "Communication and Strategy Plan" will be looking to:

- Disseminate Cyber-MAR outcomes to a wide audience, while engaging scientific, technical, business, institutional and governmental audiences from the EU and encouraging feedback;

- Define Cyber-MAR target audiences as a critical step for the dissemination and communication aspects in a multidisciplinary project;
- Promote the multi-disciplinary project character in order to attract a wide range of audiences and to showcase how Cyber-MAR will contribute to the aspects of cybersecurity in the maritime sector;
- Build relationships, through intensive networking, with related R&D initiatives, networks and organisations to share knowledge, experience and data and spread good practices via clustering activities;
- Develop positive media coverage for the project at a local, regional, national, European and global level;
- Disseminate the project's viewpoint to a wide audience of researches, scientists and cybersecurity experts;
- Liaise with stakeholders and other relevant initiatives to facilitate knowledge exchange.

1.2 Intended readership

The Cyber-MAR *"Communication and Strategy Plan"* is *a public deliverable and* constitutes a very useful guidance addressed not only to the consortium members, but also to any interested reader (i.e., PU dissemination level).

It is primarily written for the European Commission (EC), Project Officer (PO) and the consortium members of the Cyber-MAR project, in order to inform them about the Cyber-MAR brand identity and dedicated guidelines, the project's communication and dissemination materials and channels, as well as the planned activities. More specifically, it serves as a tool that helps them understand the project's communication objectives and how these could contribute to raise awareness in an efficient and effective way.

Nevertheless, special effort and attention has been given in making this report as a stand-alone document and comprehensible for the general public.

1.3 Document structure

This document is structured in nine sections.

Section 1, introduces the purpose and scope of the document.

Section 2, focuses on the overall communication strategy and plan including the communication approach along with the relevant objectives.

Section 3, includes the identification of the stakeholders' community along with the communication content of each target group.

Section 4, presents the engagement plan consisting of the project's brand identity, the key messages of the identified target groups, as well as the communication channels.

Section 5, provides a description of the liaison plan that will be implemented within the project lifetime.

Section 6, analyses the partners' roles and efforts.

Section 7, describes the communication and dissemination procedures.

Section 8, presents the evaluation and monitoring processes of the Cyber-MAR communication and dissemination activities, along with the identified risks.

Finally, section 9, provides a detailed description of the timeline, the already performed and the planned activities within Cyber-MAR project.

1.4 Definitions

Dissemination and Communication activities within a Horizon 2020 European Project, like Cyber-MAR are mandatory. The specific interpretation of these two concepts often creates confusion. What differentiates these activities is firstly their definition, their main objectives, their focus area, the target audiences they address, as well as their formal obligations.

1.4.1 Communication

Communication on projects is defined as strategically planned process, beginning at the outset of the action and continues throughout its entire lifetime. Communication activities aim at promoting project's actions and outputs and require strategic and targeted measures for communicating about the action and the results to a wide audience, including both the media and the public and a possible engagement in a two-way exchange.

The main objective of communication is oriented towards reaching out to society and presenting the impact and benefits of the project's activities (e.g. by addressing and proposing solutions to essential societal challenges). Focus is given in the information and promotion of the project along with its results and success. These activities are addressed to multiple audiences beyond the project's own community including also media and broad public. Finally, communication procedures are obliged to be in line with the *Article 38.1 of the Grant Agreement.*

1.4.2 Dissemination

Dissemination is referred as the public disclosure of results by any appropriate means (apart from protecting or exploiting the results), including also scientific publications in any medium.

The main objective of the dissemination actions includes transfer of knowledge and results offering the opportunity of outcome's usage, thus maximizing the impact of the EU-funded research. Dissemination activities are concentrated on the description of the project's results and the assurance of their availability for use. The targeted groups consist of audiences that may be interested in the potential use of the project's outputs e.g. scientific community, industrial partners, policymakers. Dissemination has to be in line with the *Article 29 of the Grant Agreement.*

According to the recently updated EC Guidance for the Social media guide for EU funded R&I projects[1], both communication and dissemination processes are mandatory and vital for H2020 projects. It is also important that results remain protected at all times. Their differences are presented in the following Table 1:

Table 1. Difference between Dissemination and Communication in H2020

Communication	Dissemination
Covers the **whole project** (including results)	Covers project **results only**
Starts at the **outset** of the project's lifetime	Takes place only when **results are available for use**
Reaches out to **society** and shows the benefits/impacts from the research	**Transfers knowledge and results**
Informs and **promotes** project's results/success	**Describes** and **ensures results' usage availability**
Multiple audiences: Beyond the project's own community, including the media and general public	**Specialized audiences:** interested in the potential **use** of the results
Formal obligation: Grant Agreement **38.1**	Formal obligation: Grant Agreement **29**

[1] https://ec.europa.eu/research/participants/data/ref/h2020/other/grants_manual/amga/soc-med-guide_en.pdf

2. Cyber-MAR Communication Strategy and Plan

2.1 General approach

The communication and dissemination activities within Cyber-MAR project aim at raising awareness on the topic of cybersecurity in the maritime sector, achieving commitment from the different stakeholders involved in the process and moving to action.

The communication strategy and plan will follow a five-pronged approach, which will be implemented within Cyber-MAR project. The figure below depicts the communication approach:

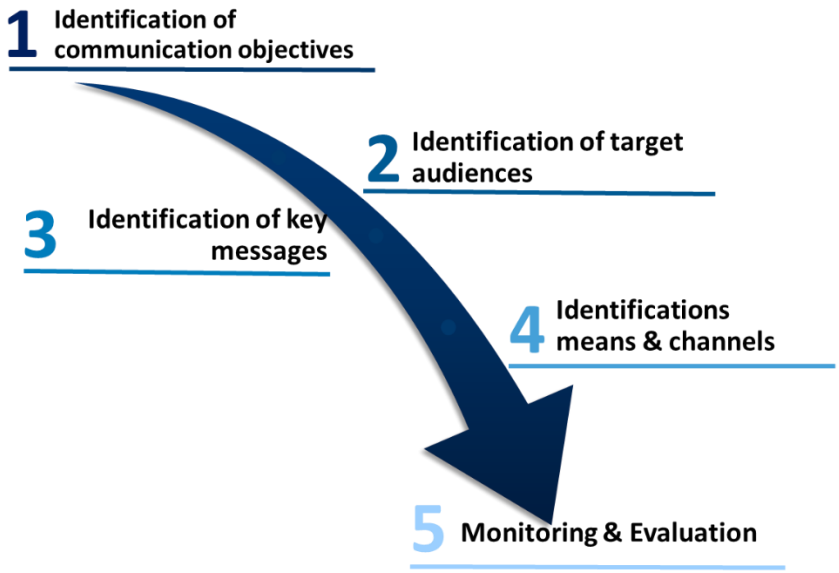

Figure 1. Cyber-MAR Communication approach

This five-step approach focuses on addressing the most of the main aspects of Cyber-MAR communication. More specifically, the identification of the main target audiences, along with the corresponding key messages, the identification of communication means and channels to be used, as well as the corresponding time period for distributing the key messages. Moreover, monitoring and evaluation procedures are included, indicating the efficiency of the communication strategy and plan and allowing the coordination of individual communication activities throughout the project's lifetime.

As regards the time schedule, a further three-stage approach for the planning and implementation of the communication and dissemination activities will be followed. The three distinctive stages are: the starting phase, the development phase and the final phase.

During the starting phase, special attention will be given on communicating the project's objectives and the expected impact to the public, while identifying the targeted audiences and the relevant stakeholder communities. This phase will aim at spreading knowledge about the project's goals and its initial outcomes, in order to conquer the maximum support from the stakeholder groups and motivate potential interested parties to be actively engaged.

In the second stage, the implemented activities will be furtherly reviewed and investigated and at the same time the initial project results will be promoted in a more tailored way addressing each one of the stakeholder groups. It is of major importance to maintain effective communication of the already available project findings and raise awareness on the project related issues in a collaborative engaging way.

During the final phase, the main goal will be the effective dissemination of the project's results to the identified target groups, in order to ensure the long-term impact of Cyber-MAR final outcomes.

Further down on section 2.2, a preliminary communication roadmap of the project has been developed and the communication objectives of WP7 have been identified.

2.2 Communications roadmap

The above analysed tree-stage approach based on the process of developments and the availability of tangible results from its research activities constitutes the communication roadmap of the project. Each phase includes selected dissemination activities and channels, which will foster the communication of the respective messages and information as well as the transmission of the available project results to the target audiences.

Within the starting phase, the availability of results constitutes a key prerequisite for the dissemination of project's concept, approach, objectives and impact. In the development phase, the communication, dissemination and stakeholder engagement activities will be concentrated on the project's initial outcomes and findings. The final stage aims at disseminating the project's final results and this way maximizing the project's impact.

The following table 2 describes comprehensively the planned activities along with the respective communication channels:

Table 2. Cyber-MAR communications roadmap and preliminary action plan

Project phase	Description	Activities	Channels
Starting phase	The major aim is to raise **awareness** and provide general **information** to the broad public and stakeholders about the project's concept and approach, objectives and expected impact.	• Creation of **brand identity** (project logo, brand story with guidelines, illustrations and graphics, templates, fact-sheet) • Production of first version of the **communication kit** (leaflet, poster, roll-up banner) • Creation of project **website** and constant content update • Set up of **social media** channels and continuous networking • Publication of media **articles** to printed and online broad media • Publication of **press releases** • **Establishing Liaison** and **networking** activities with related projects, cybersecurity and ports and logistics associations and **events organisation** (demonstrations, training events, technical presentations), as well as **engaging activities** with the identified stakeholder community • Participation in **conferences**, **workshops** and other **events**	**Website** **Social media** **Press** **Meetings, workshops** and other **events**
Development Phase	The communication activities focus on **communicating** and **disseminating** the project's work, initial **results and findings, in order to** raise awareness on the developments and challenges and motivate the target groups so as to collect the required feedback.	• **Website** and **social media** updates regarding project news and events, deliverables, publications and results • **Communication kit first update** • Creation of project general **video** • Presentations of project results in **conferences** and other **events** • Publication of media **articles** to printed and online broad media • **Peer reviewed publications** in conference proceedings and scientific journals • Publication of **press releases** • Continuing the **Liaison** and **cross fertilisation** activities • Preparation of **E-newsletters**	**Website** **Social media** **Press** **Meetings, workshops** and other **events** **Journal papers** **Conferences presentations**
Final phase	The main goal will be the effective dissemination of the project's results to the identified target groups, in order to ensure the long-term impact of Cyber-MAR final outcomes.	• **Website** and **social media updates** regarding project news and events, deliverables, publications and results • **Communication kit second update** • Production of the **updated version of the video** • Presentations of project results in **conferences** and other **events** • Publication of media **articles** to printed and online broad media • Peer reviewed **publications** in conference proceedings and scientific journals • Publication of **press releases** • **Continuing the Liaison** and **networking** activities • **Preparation of E-newsletters** • Organisation of the **final event/conference** and **demonstrations**	**Website** **Social media** Press Meetings, workshops and other events **Journal papers** **Conferences presentations** **Final event** and **demonstrations**

2.3 Communication objectives

The main objectives of WP7: *High impact communications and Networking,* shaping the targets of the Cyber-MAR communications strategy, have already been analyzed in the project grant agreement and are summarized as follows:

- The **establishment** of the appropriate channels and means for efficiently communicating the project objectives, activities, evolvement, impacts and results to a wide audience, both technical and non-technical;
- The **dissemination** of Cyber-MAR outcomes to the external world and the receipt of useful feedback from the interested in the respective topics parties (scientists, academics, key experts etc.);
- The **establishment**, **promotion** and **maintenance** of links with Cyber-MAR stakeholders' community, aiming at fostering the familiarization and the collection of important input on the developed cyber-platform;
- The **liaison** with relevant R&D initiatives and sister projects, in order to establish the premises for strong cooperation links, exchange knowledge and ensure interoperability of the developed technologies through Europe;
- The **creation** of supportive material along with training documentation in a comprehensive and easily accessible form by the potential users, in order to disseminate effectively the technological innovations.

More precisely, within Cyber-MAR WP7 and according to the DoA, particular emphasis will be given to:

- **Ensure** that all communications produced are engaging and interesting to specific target audiences. The communication approach aims to develop short messages and stories to present how Cyber-MAR technologies and proposed innovations are expected to change the way maritime and logistic operations are being structured.
- **Certify** that the results influence the CERT/CSIRTs network, port and logistics operators, maritime decision makers, public authorities, European and International organizations and networks, while convincing them that the realization of the Cyber-MAR innovations will definitely attain more for the European cyber security maritime sector, than would otherwise have been feasible.

3. Cyber-MAR Stakeholders Community

3.1 Identification of target audiences

A very important key to the successful implementation of Cyber-MAR's communication and dissemination intentions is a thorough understanding of the key target audiences that the project needs to reach out and engage with, as well as their special characteristics, behaviors, needs, motivations and frustrations.

The impact Cyber-MAR is expected to have on these groups varies considerably and the influence each group can exert on the project is equally diverse. In terms of communication, each group has distinctive needs and interests and therefore, it is essential that Cyber-MAR develops a thorough understanding of them in order to be able:

- To hone and target its communication and dissemination activities accordingly;
- To develop appropriate channels for contacting and informing them effectively and efficiently;
- To design and produce dissemination materials and activities that is expected to maximize the visibility and impact of the project.

This section identifies and presents the different target audiences relevant to Cyber-MAR. An initial mapping of Cyber-MAR stakeholders' community has been developed based on the fact that they:

- Have an interest in the project research and in learning about the outcomes;
- Can enable the project in achieving its objectives or have an influence elsewhere;
- May be directly or indirectly affected by the research (EC 2014).

Table 3 presents a thorough breakdown of the Cyber-MAR target groups. The first column depicts the identified main audiences, while the second presents the stakeholders' groups per audience in a more detailed way.

Table 3. Cyber-MAR initial list of Stakeholder Community

Main Audience	Stakeholders groups per audience
Decision Makers, Public Authorities and International Organisations	• National, regional and local authorities • Public authorities • Port cities • Policy and decision makers • European Platforms (DTLF, ALICE) • Standardization Bodies
Academia	• Universities

	• Research Centers/Institutes • Laboratories (in the field of cyber security in the maritime logistics sector...) • Students' communities • Ph.D. Candidates in project related fields
Port authorities, operators and associations	• Ports • Port operators • Railway operators • Port associations • Shipping associations • Flag agencies
Freight transport and Logistics actors	• Trucking companies • Logistic companies • Freight forwarders
Companies	• Insurance companies • Shipping companies • Cyber range providers • SIEM providers • SMEs
Networks & EU Agencies	• European and International organizations & networks for cybersecurity • Relevant EU projects • Cybersecurity/Maritime related Associations • CERT/CSIRTs network
The Media	• Journalists & bloggers in maritime, technology & other project's related fields • Local & European media (electronic & print) • Local press agencies • EC magazines (electronic & print)

The above list of target audiences will be further expanded during the course of the project, in order to include a micro level categorization of the already identified audience categories, ensuring its higher representation.

Cyber-MAR's target audiences are considered at all levels ranging from local to regional, national and European. Most audiences are direct target groups, but intermediaries that serve as amplifiers and ambassadors are included as well. Given their heterogeneous nature and diversity, there is a high probability that they would have differing interests and expectations on Cyber-MAR's assets.

The aforementioned list has been furtherly analysed with a breakdown of the second column. Thus, a third column has been created including an extensive stakeholders' directory based on the relevant contacts of the Cyber-MAR consortium members. The stakeholders' groups per target audience along with the stakeholders' directory are presented in the following Table 4:

Table 4. Cyber-MAR Initial version of Stakeholders Directory

Stakeholders groups/ target audience	Stakeholders Directory
• **National, regional and local authorities** • **Public authorities** • **Port cities** • **Policy and decision makers** • **European Platforms (DTLF, ALICE)** • **Standardization Bodies**	• IMO (WMU) • DG ENERGY (WMU) • EMSA (WMU) • DG MARE (WMU) • Traficom (VTT)
• **Universities** • **Research Centers/Institutes** • **Laboratories (in the field of cyber security in the maritime logistics sector …)** • **Students' communities** • **Ph.D. Candidates in project related fields**	• University of Genoa (WMU, FAIMM) • University of Rijeka (FAIMM) • Competence Center for Security & Optimization Strategic Infrastructures – Italy (WMU)
• **Ports** • **Port operators** • **Railway operators** • **Port associations** • **Shipping associations** • **Flag agencies**	• International Shipping Union (SEAB) • Port Authority of Valencia (VPF) • Port Authority of Livorno (VPF) • Port Authority of Koper (VPF) • Genoa Port Authority (FAIMM) • COSCO Shipping port of Valencia (VPF) • MSC Terminal Valencia (VPF) • PSA Terminal (FAIMM) • Terminal Sech (FAIMM) • Assiterminal (FAIMM) • MSC Valencia (VPF) • International Cargo Handling (VPF) • Coordination Association –ICHCA (VPF) • Confitarma Accosiation (FAIMM) • Assoarmatori Association (FAIMM) • Assagenti Association (FAIMM) • Port of Helsinki (VTT) • Port of Hamina-Kotka (VTT) • Port of Rauma (VTT) • Port of Oulu (VTT) • Port of Pori (VTT) • Port of Turku (VTT) • Euroports (VTT) • Steveco (VTT)
• **Trucking companies** • **Logistic companies/actors** • **Freight forwarders**	• Gruppo Finsea (FAIMM) • Fuori Muro (FAIMM) • Metrocargo (FAIMM) • InRail (FAIMM) • Stolt Tank Containers (FAIMM) • CGA-CGM (FAIMM) • HAPAG Lloyd (FAIMM) • Varona (VTT)

• **Insurance companies** • **Shipping companies** • **Cybersecurity companies** • **ICT companies** • **SMEs**	• MSC (FAIMM) • Costa (FAIMM) • GNV (FAIMM) • Tallink (VTT) • Viking Line (VTT) • Finnlines (VTT) • Eckerö (VTT)
• **European and International organizations & networks for cybersecurity** • **Relevant EU projects** • **Entities** • **Associations** • **CERT/CSIRTs network**	• Swedish CERT (WMU) • SEA Europe (WMU) • ESPO (WMU) • EMSA (FAIMM)
• **Journalists & bloggers in maritime, technology & other related fields** • **Local & European media (electronic & print)** • **Local press agencies** • **EC magazines (electronic & print)**	• Port Technology International (VTT)

3.1.1 Decision Makers, Public Authorities and International organisations

Public stakeholders such as the national and regional government, ministries, EU citizens and general public, decision and policy makers, as well as international organizations are included in this target group. This group will support data access provision and will promote their expertise where necessary to ensure the usefulness and importance of the project's outcomes. Their role emphasizes also on mainstreaming adaptation into relevant policies and integration to the national and EU funds, promoting dissemination of outcomes and ensuring liaison to other entities. Moreover, this group will contribute to the dissemination activities of Cyber-MAR project as it can effectively foster the project's developments to the general public and the public authorities. Cyber-MAR offers the opportunity to develop advanced policies based on rigorous scientific knowledge and funding opportunities for necessary projects.

3.1.2 Academia

Academia constitutes the scientific community group including relevant universities, academic and research institutes, laboratories specialized in the field of cybersecurity and maritime as well as graduate and under graduate students and Ph.D. candidates. The academic community can effectively integrate the Cyber-MAR results and findings into their teaching or training activities e.g. as part of the Master theses of Ph.D. theses. Furthermore, can broaden the research horizon and increase the efficiency and attractiveness of the cyber security technologies applied in the maritime sector. Cyber-

MAR aims at communicating the knowledge and experience to the new generation of scientists and researchers, while fostering innovative approaches and ideas in the maritime domain.

3.1.3 Port authorities, operators and associations

This category includes ports, port, terminal and railway operators, port and shipping associations, as well as flag agencies. This audience can be actively involved in the evaluation and the approval of project's results, as well as in the promotion of the dissemination and adoption of Cyber-MAR outcomes. They will contribute to the improvement of the networking and clustering activities with organizations and the linkages with individuals. Cyber-MAR communication will promote the advantage of using the developed and cybersecurity - related innovations in maritime and most importantly will raise the cyber-threat awareness level within this target group. The engagement with associations and authorities could increase the local publicity and possibility of networking with potential new members.

3.1.4 Freight transport and Logistics actors

This stakeholders' group consists of logistic actors and companies, freight forwards and trucking companies. It is essential for the operational group to gain access to the developed and implemented innovation technologies in cybersecurity and the relevant knowledge in order to closely cooperate and use these technologies. Cyber-MAR communication focuses on the way that Cyber-MAR concept integrates the operational players into the cybersecurity innovations in maritime. Cyber-MAR will provide this stakeholder group with the tools to better understand maritime cyber-risks and to be well prepared against potential cyber-attacks.

3.1.5 Networks and EU agencies

European and International organizations and networks for cybersecurity, relevant EU projects, entities, as well as CERT/CSIRTs network compose this stakeholders' group. They can effectively contribute to raise awareness about cyber risks and cybersecurity measures in the maritime sector. Their role will also cover the exchange of knowledge that give operational solutions for mutualizing, sharing and improving cyber preparedness and early warning within the maritime sector following a cross-sector approach. Cyber-MAR through its communication activities will promote to these target group innovative approaches and ideas in the maritime domain.

3.1.6 Companies

The Companies' group includes cybersecurity and insurance companies, shipping companies, ICT companies, as well as SMEs. This group will possibly provide its technical expertise and knowledge for the development of Cyber-MAR innovations. Furthermore, the evaluation and validation of the project's results combined with their

implementation and replication explain the necessity of this group involvement. Cyber-MAR communication activities will facilitate the increase of the local publicity through the engagement of this stakeholders' range with Cyber-MAR project, while increasing the opportunities of networking with potential new customers.

3.2 Identification of the communication content

The objective of the Communication strategy is to ensure that the project developments, outcomes and benefits are communicated in an efficient and effective way to all identified target audiences according to their unique interests and needs.

The below table provides an in-depth analysis of each target audience's importance, interests and communication and dissemination requirements.

Table 5. Importance of each target audience

Audience Group	Cyber-MAR's News & Stories that matter	Importance
Internal Stakeholders	Cyber-MAR's technical & scientific developments, events, details about project's innovations, best practices, infrastructure & tools	Very High – Partners need to be fully engaged in order to get their full support & to spread the news about Cyber-MAR via their own networks
Decision Makers, Public Authorities and International Organisations	Overview about Cyber-MAR's assets, impact & developments, the innovation potential of the project	High – Their support is needed to ensure the long-term future of Cyber-MAR & its outcomes
Academia	Overview about Cyber-MAR's aim, mission, impact & technical & scientific developments, details about project's innovations, best practices, infrastructure & tools, upcoming Cyber-MAR Events	High – Outreach is highly important in order to raise awareness, promote liaisons and collaborations & exchange knowledge
Port authorities, operators and associations	Overview about Cyber-MAR's aim, mission, impact & developments, details about project's innovations, best practices, infrastructure & tools, upcoming Cyber-MAR Events	Very high - The principal subject community of Cyber-MAR as the most important providers of data, expertise & support for the project by spreading the news via their own networks
Freight transport and Logistics actors	Overview about Cyber-MAR's aim, mission, impact & developments, details about project's innovations, best	Very high - Outreach is highly important being one of the most relevant to the project's fields stakeholders & high-affected by its

	practices, infrastructure & tools, upcoming Cyber-MAR Events	results. Their support for the project by spreading the news via their own networks is highly expected & very welcome
Companies	Overview about Cyber-MAR's assets & developments, details about project's innovations, best practices, infrastructure & tools, upcoming Cyber-MAR Events	High - Outreach is highly important as their support for the project by spreading the news via their own networks is highly expected & very welcome
Networks & EU Agencies	Overview about Cyber-MAR's assets & developments, details about project's innovations, best practices, infrastructure & tools, upcoming Cyber-MAR Events	High - Outreach is highly important as their support for the project by spreading the news via their own networks is highly expected & very welcome
The Media	Overview about Cyber-MAR's aim, mission, impact, general benefits & achievements	High – Outreach & raising awareness among Cyber-MAR's different audience groups & communities is very important. The Media play a key role in spreading the project's key news & assets

4. Engagement Plan

Cyber-MAR will follow a two-pronged impact creation approach within WP7 framework, in order to ensure the successful completion of its objectives:

- Creation of strong engagement with the Cyber-MAR Stakeholder Community by tailoring key messages for each target audience, aiming basically to increase users' awareness and thus secure Cyber-MAR acceptance, continuity and wide market penetration.

- Establishment of the appropriate communication channels with the external world to efficiently promote and publish Cyber-MAR results and key outcomes as well as to raise wide awareness on the project's evolution and impact.

4.1 Cyber-MAR visual identity

The Cyber-MAR brand identity includes a manual/guide that provides a comprehensive description of its visual and verbal elements. This set of guidelines reflects project's commitment to quality, consistence and style. The Cyber-MAR logo guidelines must be followed throughout the project runtime, to achieve the desirable uniformity and integrity of its identity and to the awareness and recognition for its brand. Furthermore, these guidelines constitute a useful toolkit for the production of branded items for Cyber-MAR as well as for the design of its dissemination and communication material.

A consistent and coherent visual identity has been developed for Cyber-MAR as part of the *D7.2 'Cyber-MAR Communication Tools',* due on M18, including a logo along with its variations, colour schemes and relevant typefaces.

In the context of Cyber-MAR's consistent brand identity and in order to keep a credible and professional "look and feel", a set of Cyber-MAR MS Office templates (pptx presentation, deliverable, deliverable user manual, SSA, minutes of meeting, agenda, Non-European Travel, dissemination activities report, i.e.) have been created based on the project's brand guidelines and are available to all partners through Cyber-MAR's common online collaborative tool.

Furthermore, already designed and produced communication and dissemination materials and channels (i.e. project website, factsheet, leaflet, brochure, roll-up banner) and these that will be produced in a later stage (i.e. video, e-newsletter) have been or will be designed guaranteeing a professional and consistent look always based on the above mentioned brand guidelines.

In order to maintain the integrity of the Cyber-MAR brand identity, it is very important that all given instructions, described in detail in the dedicated manual, are applied properly by all. The project communication and dissemination material and all its brand elements can be used freely by all consortium members, however all external bodies, except from the European Commission (EC), must acquire the required permission from the consortium, before proceeding with any use of the Cyber-MAR material.

4.2 Key messages

Key messages are the main points of information that Cyber-MAR wants its interested audiences to hear, understand, and remember. They are bite-sized summations that articulate what Cyber-MAR does, why it does it, and what value brings to stakeholders. Within first months of the project and in the context of Cyber-MAR communication tools' development (D7.2), ***"Building cyber-resilience within maritime"*** has been selected among the Cyber-MAR consortium as the project's general key message (tagline), which indicates the following aspects:

- Preparedness (indirectly through the word Building)
- Cyber
- Resilience (covers business continuity)
- Maritime

Cyber-MAR key messages include:

- Raising awareness of the potential benefits of Cyber-MAR proposed technology;
- Engaging with target audiences to collect feedback for development;
- Dissemination of project results;
- Engaging with relevant R&D projects, associations/networks, standardisation bodies and organisations to ensure knowledge exchange, interoperability and wide market penetration;
- Engaging new and final users to contribute with inputs and feedbacks throughout the implementation of the project;
- Demonstrating how Cyber-MAR solutions are relevant for the daily life of European citizens.

Key messages have been specifically addressed to each target audience to reflect efficiently what the project intents to communicate per audience. Tailoring the messages, the consortium will ensure a significant impact of the diffused information and engage the audience according to their interests and needs. The following table 6 presents the list of key messages adapted to each one of the identified target groups.

Table 6. Cyber-MAR key messages per target audience

Key audience	Key message
Decision Makers, Public Authorities and International Organisations	• Cyber-MAR will result in improved security, resilience and sustainability of organisations. • Cyber-MAR will enable a collaborative maritime policy making, considering a wider cybersecurity factors' approach. • Cyber-MAR will provide better understanding of the maritime cyber-risks by introducing the Maritime Cyber-Risk Assessment framework (MaCRA). • Cyber-MAR will raise the cyber threat awareness level within organisations by hands - on training. • Cyber-MAR will offer outputs regarding the financial impact of cyber-attacks and data privacy breaches.

Academia	• Cyber-MAR provides the academia and research community with a solid knowledge in the area of cybersecurity in the maritime and it will advance the current state-of-art by achieving significant cross-research-area results. • Through Cyber-MAR a larger number of computer science university students are expected to be engaged in the cyber security profession. • Cyber-MAR is working on innovative operational technologies to mitigate cyber-attacks and therefore can provide an approach to include horizontal aspects into standardization activities.
Port authorities, operators and associations	• Cyber-MAR will allow the estimation of the impact of a cyber-attack from a financial perspective. • Cyber-MAR will support the undertaking of prompt decisions in selecting the appropriate cyber-security measures to mitigate the risks of a cyber-attack. • Cyber-MAR will cover the training needs for all professionals (cyber-security/IT experts, personnel of ports, shipping operators. • Through the development of cyber security technologies in the maritime field, Cyber-MAR will assist ports in complying with the increasing needs to address cyber-attacks.
Freight transport and Logistics actors	• Through Cyber-MAR the maritime logistics value chain actors will validate their business continuity management minimizing business disruption potential. • Cyber-MAR will boost the smooth operation of terminals.
Companies	• Cyber-MAR will raise new business opportunities for industries and SMEs in the EU. • Cyber-MAR will allow insurance companies and corporations assess the impact of cyber-attacks across different product groups and industries. • Cyber-MAR will provide to organizations outputs that will help them quantify the supply chain risk, develop risk mitigation strategies and improve resiliency.
Networks & EU Agencies	• Cyber-MAR will provide knowledge on operational solutions for mutualizing, sharing and improving cyber preparedness and early warning within maritime sector. • Cyber-MAR will facilitate the collaboration between a network of cyber-ranges and Europe-wide initiatives such as the CSERT/CSIRTs cooperation network of the NIS directive.
Press	• Cyber-MAR will flow its outcomes to a wider European audience.

4.3 Communication channels

A wide range of communication channels will be actively used during the project lifetime, to effectively flow Cyber-MAR information, raise awareness and reach out to the targeted audiences, by taking into account the specific characteristics and needs of each target group. The following indicative list of proposed communication channels presents the already defined means of transmitting the information produced within Cyber-MAR project. This list will be constantly updated during the project lifetime, based on its emerging requirements:

- Project website (backbone of all communication activities)
- Print Media (press, magazines, etc.)
- Online media (online newspapers, magazines etc.)
- Printed material (fact-sheet, posters, brochures, roll-up)
- Press releases (see Annex A: Cyber-MAR 1st Press Release)
- Social media (Twitter, LinkedIn, YouTube) - They have been developed and used in line with EC guidelines [2]
- Physical meetings
- Conferences, exhibitions, workshops, focus groups, training seminars and other events
- Cyber-MAR final event (as an International Conference)

The Cyber-MAR stakeholders' groups and target audiences, along with their interest, expectations, relevance and role with regard to project success, have already been mapped. This facilitates the optimal dissemination and communication activities that will underpin the project's technical and exploitation goals. The project is going to use different communication channels in the promotion activities. Different media suit better to given target groups than approaching all receivers through all media. The project is approaching the identified target groups by the following communication channels, as presented in table 7 below:

[2] The guidelines stemmed from the General Data Protection Regulation (EU) 2016/679 ("GDPR"), which became enforceable in May 2018, have been taken into consideration in the formation of the aforementioned mailing lists.

Table 7. Cyber-MAR Stakeholders groups in relation to the communication channels

Main audiences/ Comm. channels	Project website	Online media	Printed material	Social media	Cyber-MAR video	Scientific Publications	Physical meetings	Presentations in events	Cyber-MAR final event
Decision Makers, Public Authorities & International organisations		X	X		X		X	X	X
Academia	X	X	X	X		X	X		X
Port authorities, operators and associations	X	X	X	X	X		X	X	X
Freight transport and Logistics actors	X	X	X	X	X		X	X	X
Companies	X		X	X			X	X	X
Networks & EU agencies	X	X	X	X	X		X	X	X
Press	X	X		X	X	X			

5. Liaison Plan

Cyber-MAR project aims at strengthening relationships with the entire community involved in the maritime cyber security sector, which is made up of different types of actors. The identification and interaction with related projects, and any thematic cluster projects added to the stakeholders' community, are of crucial importance.

The aim of the liaison plan is to establish effective links with other relevant projects and initiatives, to promote complementarity and to avoid redundancy and overlaps. Grouping activities with existing initiatives and projects will be identified and organized in order to exploit synergies in terms of content sharing, exchange of good practices and joint dissemination for maximizing impact networking thanks to external events that will be used to promote and share Cyber -MAR results. This activity aims to establish a connection with the scientific community of research infrastructures and other stakeholders to help promote and exploit the results deriving from the implementation of Cyber- MAR. It will be identified all related projects funded not only under topic SU-DS-01-2018 but also from other topics and work programmes of H2020 related to Cyber security and maritime environment related to security issues.

This activity is also directly linked to the development of potential seminars on the exchange of experiences (Task 7.2) with the involvement of ongoing and closed EU and other relevant projects. and/or of the whole stakeholder community. In the first case, these seminars will be aimed at promoting the interaction of the participants and aimed at exchanging experiences and transferring knowledge from existing / ongoing projects identified. In the second case, opportunities for discussion, exchanges of views and practices will be promoted.

A list of projects and initiatives will be included in the Cyber-MAR website. The projects will be indicated by acronym / name of the initiative, indicating basic information such as abstracts, funding program and duration.

The stakeholders' community members will be stored in a directory and based on the development of a hub, all of these stakeholders will be engaged within the "*Community of Practice*" space, which will provide ground for new collaboration ideas and innovative solutions. The hub will be a useful environment for the development of knowledge sharing and cooperation opportunities between all projects and stakeholders in the sector.

The synergy activities to be implemented include:

- Potential involvement to participate in ongoing and closed EU and other relevant projects;
- Invitation to participate in planned pilots and training activities;

- Involvement of other projects to register on the Cyber-MAR online hub to show their results and stay in touch through the "*Community of Practice*";
- Co-organization webinar with perspectives of different projects;
- Organize Joint events with other EU projects, dissemination events by providing a session on the results of the other projects.

6. Partners roles and efforts

Successful communication and dissemination of Cyber-MAR relies on the commitment and contribution of all project partners. For that reason, the WP7 leader SEAB will be engaging with all project partners and will promote effective interaction between WP7 and all other WPs to ensure that the communication and dissemination activities of the project are effective and impactful. All partners have been allocated person months under WP7 Communication and Dissemination.

Partners will contribute to the communication and dissemination of the project through the development of the research, identifying outcomes, outputs and benefits, publishing research papers and articles, using their extensive knowledge of contacts in relevant fields and identifying appropriate groups of stakeholders.

The combined contributions of all partners will have a compelling impact on the communication and dissemination of the project.

WP7 structure is composed of the following tasks each one connected to the relevant deliverables (Table 8) along with the corresponding assignments as well as the WP7 milestones (Table 9), as derived from Cyber-MAR GA. As regards to the first two milestones - MS12 and MS13 – they have been successfully achieved on time (M3). The last one milestone (MS14) refers to the organization of the Cyber-MAR final event. The project's final conference will possibly take place in conjunction with Posidonia event which will be held on 2022 in Athens, Greece.

Table 8. Cyber-MAR Tasks and Deliverables connections & responsible partners

Description	Leader	Contributors	Due Date
T.7.1: High Impact Communications and Networking	SEAB	All partners	
D.7.1: Communication Strategy and Plan	SEAB		M6
D.7.2: Cyber-MAR Communication tools	SEAB		M18
D.7.4: Intermediate Reports on Communication and Dissemination activities	SEAB		M18
D.7.5: Final Report on Communication and Dissemination activities	SEAB		M36
T.7.2: High Impact Cyber-MAR Communication activities	SEAB	All partners	
D.7.2: Cyber-MAR Communication tools	SEAB		M18
D.7.4: Intermediate Reports on Communication and Dissemination activities	SEAB		M18
D.7.5: Final Report on Communication and Dissemination activities	SEAB		M36
T.7.3: Scientific dissemination	VTT	All partners	

D.7.4: Intermediate Reports on Communication and Dissemination activities	SEAB		M18
D.7.5: Final Report on Communication and Dissemination activities	SEAB		M36
D.7.6: Conclusion report of Cyber-MAR scientific contributions	VTT		M36
T.7.4: Cyber-MAR Liaison with other projects, cyber security, and ports and logistics associations and events organisation	WMU	All partners	
D.7.3: Cyber-MAR Networking and Cross fertilisation activities	WMU		M36

Table 9. Cyber-MAR WP7 milestones

Milestone Number	Milestone Title	Lead Beneficiary	Due Date	Means of verification
MS12	Cyber-MAR website ready	SEAB	M3	Website up and running
MS13	Cyber-MAR communication kit first version	SEAB	M3	Cyber-MAR poster and brochure prepared
MS14	Cyber-MAR final event organised	SEAB	M36	Final event organized

Definitely, successful, effective and impactful dissemination and communication procedures require the constant commitment and contribution of all project partners. Therefore, the allocated effort in PMs is given in the Table 10 below:

Table 10. Cyber-MAR WP7 effort per partner

Partner's short name	ICCS	NG	VTT	PCT	DIATEAM	VPF	WMU	FAIMM	UoP	ATOS	SEAB	PEARL	AIR
WP7 effort	**5.00**	**3.00**	**4.00**	**3.00**	**3.00**	**4.00**	**4.50**	**3.00**	**4.50**	**4.50**	**25.00**	**2.50**	**3.00**
Total	**69.00**												

7. Communication and Dissemination Procedures

The dissemination procedures consist of guidelines and define the main steps to be followed by partners for the publication or presentation of the work done within Cyber-MAR project framework. The detailed description of Cyber-MAR communication and dissemination procedures is available in the common online collaborative tool (Redmine) and also in Annex B of the present document.

The main objectives of the aforementioned procedures focus on:

- The production of high quality Cyber-MAR publication and presentations;
- The avoidance of overlapping and possible disclosure of restricted or confidential information;
- The monitoring and recording of the dissemination activities of the project in a sufficient way.

The step by step procedure is described below:

1. **At least two weeks before** the publisher's or organizer's deadline for submitting a research paper, proposal for presentation or performance of any other communication/dissemination activity related to Cyber-MAR project, the initiator of the dissemination activity:
    - Offers general information (type of activity, provisional title, short summary, date/place of the meeting etc.) about these activities he/she intends to participate by filling the required fields in the dissemination request form, available at the Wiki page of Cyber-MAR internal project's document repository (Redmine), (see Annex B);
    - Stores the relevant material (abstract, draft paper, poster, presentation etc.) to the respective folder on internal project's document repository;
    - Submits the dissemination request, including the Security Sensitivity Assessment form (Annex C) stored in the internal project's repository allowing for minimum two weeks before submission deadline, by email to the WP7 leader (SEAB).
2. The WP7 leader sends the request within two days to the Coordinator/EB/SAB for approval, modification, or rejection;
3. **Coordinator/EB/SAB** decision sent to the WP7 Leader within **five working days**; If no answer is received due to the set deadline it is taken as an approval;

4. **WP7 Leader** informs initiator of the dissemination activity along with the involved partner(s) about the decision.

5. Within **ten working days** after the realisation of the approved dissemination activity, the initiator should provide the WP7 Leader (SEAB) with the filled in dissemination report and the presented material (final paper, presentation, poster etc.) along with some photo material. The dissemination activities report form is stored in the respective folder on internal project's document repository.

8. Evaluation and monitoring (KPIs)

8.1 Communication and Dissemination KPI's

The effectiveness of Cyber-MAR's communication and dissemination activities will be periodically measured. Periodic evaluation is considered very important to guarantee that all identified target audiences are properly reached and provided with appropriate information and content on project's assets and to generate feedback and get insights on what works and what needs refinement.

Therefore, SEAB, being the WP7 Leader as well as VTT and WMU, being the key Task Leaders in WP7, regularly monitor progress against KPIs as set out in the project's DoA. The Table 11 below describes the planned Cyber-MAR Dissemination and Communication activities to be performed in the different project phases and KPIs expected from the relevant activities.

Table 11. List of Dissemination and Communication KPIs

Dissemination activities	Description	KPI
Development of a recognizable brand identity	Brand development: To ensure the impact of Cyber-MAR is coherent professional and widely recognizable, a visual identity will be developed to showcase the project idea and concept in a clear and attractive way. The core element of the brand will be the Cyber-MAR logo. A brand story and identity will be produced. A memorable tagline will be developed to contribute to brand association.	*1 project logo, brand guidelines, Cyber-MAR templates, illustrations and graphics*
Dedicated website	Launch, maintenance of Cyber-MAR website. The main objective is to create an easily accessible and understandable public platform for dissemination of public results (deliverables, open access publications, presentations, newsletters). Interactivity and steadily growing content will attract attention.	*1 public website*

Social Media Channels	Activities will focus in the use of social media for reaching related business communities but also the general public frequently and cost-efficiently, and to strengthen the Cyber-MAR Stakeholders' Community. Key messages and achievements will be communicated through the already active social media sites of the partners and the H2020 related social media.	*Active LinkedIn, and Twitter accounts, posting news in a regular (weekly) base. At least 150 members per account the 1st year; at least 500 members in M36. At least 4 announcements per partner in individual social media accounts; at least 6 announcements in H2020 social media sites.*
Participation in Conferences and events	Cyber-MAR will be presented and develop technologies that will be demonstrated in relevant conferences and other events. Partners' effort will also focus on the organization of special sessions and other project events in the framework of in well-known cyber security and maritime events. Developed solutions will be demonstrated at related exhibitions and fairs.	*At least 15/year and 60 presentations in total; 3 special sessions; 3 stands and/or demonstrations*
Peer reviewed publications	An effort to publish peer-reviewed scientific papers in highly rated scientific journals and conferences will be made. This task will be performed mostly by the research partners; publications will cover all innovations; effort will be made to secure Open Access (OA) to all interested persons, mainly through the project website but also through respective OA repositories as OpenAIRE.	*At least 25 project papers in conference proceedings; 8 publications in re-known scientific journals*
Use of EU dissemination networks	Cyber-MAR consortium will seek every opportunity, always in close collaboration with the EC R&D personnel, to diffuse the project vision and results through various means offered by the EU i.e. Horizon Magazine, research*eu results magazine, EuroNews TV etc. Partners will investigate possibilities to participate at EU conferences and public events as well as in cyber security and maritime transport events.	*At least 4 publications in EC communication tools; Participation in EU events;*

Communication activities	Description	KPI
Communication Kit	A Cyber-MAR brochure and pilot factsheets will be produced based on the Cyber-MAR brand guidelines. This material will be distributed at congresses, workshops, exhibitions, fairs and other events. E-Newsletter issues will be issued around major milestones. A video will be created to visualize basic results.	*2 brochures, 3 pilot factsheets, 1 video, 4 e-Newsletters*
Project Events	To achieve wide communication of activities and benefits to end-users, 2 pilot demonstrations & 1 large simulation exercise will be held during the project course. A final event will be held between M33-M36 to disseminate outcomes and demonstrate developed technologies. Clustering sessions with other projects will be organized in consortium meetings.	*2 demonstration/training events, one in each pilot site;*

8.2 Risk management and compliance

In Cyber-MAR, risks are considered as an integral part of the work plan. The complexity of the problem at hand and the trans-disciplinary nature of the consortium add to the number of risky aspects that may cause issues in the project execution lifecycle. However, all these issues are tackled a priori by exploiting the accumulated project implementation experience of partners and by applying a well laid-out management scheme. Quality and risk management falls into the scope of WP1, however there are some issues directly related to risks in communications, where the level of importance is fundamental for the implantation of Cyber-MAR communication strategy and plan. Table 12 includes a list of communication risks along with the respective mitigation actions.

Table 12. Cyber-MAR communication identified risks and mitigation actions

WP	Description of Risk	Proposed Risk – Mitigation actions	P	D
7	Low involvement of external to the consortium stakeholders in training activities/sessions	Brand identity, social media, basic communication kit (project website, poster, leaflet, press releases) prior to WP6 training sessions, Cyber-MAR AB to be invited (resources foreseen coordination budget).	M	M

7	Low outreach of Cyber-MAR communication channels and low relevance to the specifics of the target audiences	Communication strategy and plan will be developed early (M6) and constantly evaluated, so as to assure that all developed channels and means are relevant to the specifics of the target audiences; specific KPIs have been provisioned for monitoring the success of the strategy. Statistics on the use of the Cyber-MAR webpage and social media accounts will be reviewed periodically to monitor visitors' flow and increase the diffusion in time.	L	H
7	Low participation at the Cyber-MAR demonstration events and training activities	All communication channels used to broaden the number of stakeholders involved in activities. Substantial effort will focus on engaging the stakeholder community, the members of which are expected to participate at workshops, demonstrations and training activities; Partners are committed to share information about Cyber-MAR events through individual channels and invite their colleagues to attend.	L	M
7	Exploitation plan for Cyber-MAR results and respective roadmap not viable	During the proposal phase key stakeholders have been identified and engaged to ensure a strong business partnership. This activity will continue during the project phase to ensure realistic and sustainable business and exploitations plans for all key parties.	L	H
7	Target amount of conference papers and scientific publications nit met	Suitable conferences and publications are continuously monitored and project partners are regularly informed of dissemination and publication opportunities	M	M

Unexpected events may arise during the project's lifetime, thus there is need to be prepared accordingly. Publishing in a high-ranking journal which may call for an instant reaction from the Cyber-MAR consortium could be one of the unexpected events. In such case, all partners need to keep up-to-date, follow turns of event and notify the relevant consortium members.

It is stated in the GA (Art. 38) that any communication activity, expected to have a major media impact must be first notified to the EC. The Cyber-MAR partners are fully conscious and compliant with this requirement.

As regards to the intellectual property rights (IPR) in relevance to scientific publications, results generated within the project will be defined as they emerge, taking into consideration issues such as novelty, patentability and protectability. Appropriate protection procedures will be implemented. A thorough review and analysis of the most appropriate IPR tools to protect the variety of research results will be conducted and the IPR will be catalogued. Patent (or other IPR) applications will be filed for. Informed consent will always be obtained from individuals taking part in communications activities, such as interviews, photos and videos. Further information about the consent forms, POPD requirements and data management in general is provided through the confidential deliverables under WP9 and the Data Management Plan created within WP1.

9. Timeline

In Cyber-MAR, special focus is given on the communication opportunities throughout the project's lifetime. Cyber-MAR can achieve wider acceptance and increase the awareness level of cybersecurity in the maritime sector and therefore effectively exploit the aforementioned opportunities. These key opportunities are regularly updated mainly by Cyber-MAR Dissemination Manager along with the consortium members. Moreover, the project partners are informed in a regular basis about the arising opportunities, in order to be able to jump at them.

9.1 Performed Activities

The activities that have already took place during the first six months of the Cyber-MAR project are summarized in the Table 13 below:

Table 13. Cyber-MAR performed communication activities M1-M6

Conferences			
1. *The Baltic Seas International Maritime Conference, Finland, 24-15/09/2019,* ***VTT***			
2. *3rd GMN International Conference, Malmö-Sweden, 08-10/10/2019,* ***WMU***			
3. *The Smart Ship Exchange, Athens-Greece, 10-11/10/2019,* ***UoP***			
4. *NAŠE MORE 2019, Dubrovnik-Croatia, 17-18/10/2019,* ***UoP***			
5. *ICMET Oman, MTC Campus – Muscat, 05-07/11/2019,* ***UoP***			
6. *Marine and Maritime Cyber Security in MBTC– United Kingdom Plymouth, 05/11/2019,* ***UoP***			
7. *ICT Security World Conference, Athens-Greece, 14/11/2019,* ***ICCS***			
8. *5th ITS Hellas Conference & Exhibition, Athens-Greece, 17-18/12/2019,* ***SEAB***			
Project Events			
1. *Kick-off meeting, Porto Heli-Greece, 18-20/09/2019,* ***All partners***			
2. *End Users Workshop, Piraeus-Greece, 28/11/2019,* ***DIATEAM, ICCS, PEARL, PCT, SEAB***			
3. *1st Technical meeting, Brest-France, 11-12/02/2020,* ***DIATEAM, ICCS, NG, UoP, VTT***			
Mass Media Publications			
Title of publication	**Date**	**Published area**	**Involved partner**
"Cyber-MAR kick-off meeting in Porto Heli"	23/06/19	SEAbility Website: https://seability.eu/2019/09/23/cyber-mar-kick-off-meeting-in-porto-heli/	**SEAB**
"Preparation first, safety always!"	26/09/19	VPF Website: http://www.fundacion.valenciaport.com/Schedule-news/News/La-preparacion-primero,-la-seguridad-siempre!.aspx	**VPF**
"El proyecto Cyber-MAR analizará cómo preparar las instalaciones portuarias ante ciberataques"	27/09/19	Comunitat Valenciana: https://www.cyber-mar.eu/wp-content/uploads/2019/12/CyberMAR-20190927-DP.pdf	**VPF**
"El proyecto Cyber-MAR analizará cómo preparar las	27/09/19	Diariodelpuerto.com: https://www.cyber-mar.eu/wp-content/uploads/2019/12/CyberMAR-20190927-DPcom.pdf	**VPF**

instalaciones portuarias ante ciberataques"			
"El proyecto Cyber-Mar preparará al sector marítimo-portuario ante posibles ataques cibernéticos"	30/09/19	Cadena de suministro: https://www.cyber-mar.eu/wp-content/uploads/2019/12/CyberMAR-20190930-CdS.pdf	**VPF**
"Proyecto europeo Cyber-Mar entrena al sector marítimo ante ataques cibernéticos"	02/10/19	noticiaslogisticaytransporte.com: https://www.cyber-mar.eu/wp-content/uploads/2019/12/CyberMAR-20191002-noticiaslogisticaytransporte-com.pdf	**VPF**
"Sector marítimo debería limitar la potencia de los buques para disminuir emisiones"	07/10/19	loginews.com: https://www.cyber-mar.eu/wp-content/uploads/2019/12/CyberMAR-20191004-Loginews.pdf	**VPF**
"Cyber-MAR: Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain"	03/10/19	ATOS Website: http://booklet.atosresearch.eu/content/atos-brings-cybersecurity-technology-maritime-sector	**ATOS**
"WMU Contributes to Cyber-MAR project to prepare for emerging and future cyber-attacks"	08/10/19	WMU Website: https://wmu.se/news/wmu-contributes-cyber-mar-project-prepare-emerging-and-future-cyber-attacks	**WMU**
"Cyber-MAR EU funded H2020 project_ WMU Contributes to preparing for emerging and future cyber-attacks"	03/12/19	On the MOS WAY: https://www.cyber-mar.eu/wp-content/uploads/2019/12/Cyber-MAR-EU-funded-H2020-project_-WMU-Contributes-to-preparing-for-emerging-and-future-cyber-attacks-On-The-MoS-Way.pdf	**WMU**
"€7 million project aims to enhance global maritime cyber security"	04/11/19	University of Plymouth Website: https://www.cyber-mar.eu/wp-content/uploads/2019/12/%E2%82%AC7million-project-aims-to-enhance-global-maritime-cyber-security-University-of-Plymouth.pdf	**UoP**
"Greek participation in European Cyber-MAR project on cyber security in	06/11/19	sofokleousin.gr: https://www.sofokleousin.gr/elliniki-symmetoxi-sto-eyropaiko-ergo-cyber-mar-gia-tin-kyvernoas	**ICCS**

maritime transport"			
"A new platform for cyber-security in maritime transport"	07/11/19	portal.tee.gr: http://portal.tee.gr/portal/page/portal/INFO_TEE/INFO_2019/11_19/NEWSLETTER20191107.pdf	**ICCS**
"Dr. Angelos Amditis Coordinator of The European Cyber-MAR Project for Navigation in Safety"	11/11/19	logistics-management.gr: http://www.logistics-management.gr/news/1422	**ICCS**
"Cyber-MAR: A new platform for cyber-security in maritime transport"	06/11/19	portent.gr: https://www.portnet.gr/eidiseis-naytilias/23386-cyber-mar-mia-nea-platforma-gia-tin-kyvernoasfaleia-stis-thalassies-metafores.html	**ICCS**
"Cyber-MAR: A new platform for cyber-security in maritime transport"	06/11/19	infomarine.net: https://infomarine.net/greek-news/147750-cyber-mar-mia-nea-platforma-gia-thn-kybernoasfaleia-stis-thalassies-metafores.html	**ICCS**

9.2 Planned Activities

An indicative list of proposed scientific journals and an indicative list of proposed upcoming events are available in Annexes D and E respectively

Among the events proposed in the developed list (Annex D), Cyber-MAR partners have expressed their strong interest in participating in the following events until now:

- Transport Research Arena - 27-30 April 2020, Helsinki, Finland
- Posidonia 2020 - 1-5 June 2020, Athens, Greece
- IAME Conference - 10-13 June 2020, Hong Kong
- 5th IEEE European Symposium on Security and Privacy - 16-18 June 2020, Genoa Italy
- The Fifth International Conference on Cyber-Technologies and Cyber-Systems - CYBER 2020 – 26-30 July, 2020, Nice, France
- ICIMP 2020, The Fifteenth International Conference on Internet Monitoring and Protection. September 27 - October 01, 2020, Rome, Italy
- Transport & Logistic Trade Fair 04-07 May 2021, Munich, Germany

10. Conclusions

This deliverable describes the Cyber-MAR Communication Strategy and Plan, which will serve as a guide for the consortium members towards the effective allocation of time and resources in the maximization of project's impact. It demonstrates Cyber-MAR communication approach by defining the key communication objectives and the communication roadmap, analyses the target audiences along with the corresponding key messages and specifies the engagement plan. D7.1 focuses also on the evaluation and monitoring of communication and dissemination activities and partner's role and effort. Special reference is also made to the scientific approach which is going to be developed and implemented within the project and to the activities related to event participation and the liaison activities with similar initiatives.

The Cyber-MAR Communications Strategy and Plan is considered as a flexible and adaptive living document to enrich the project's approach to communications and to ensure that information about the project and its results are effectively communicated through its life and beyond.

References

[1] EC Research & Innovation Participant Portal Glossary/Reference Terms. Available at: http://ec.europa.eu/research/participants/docs/h2020-funding-guide/grants/grant-management/communication_en.htm

[2] European Union – The European flag. Available at: https://europa.eu/european-union/about-eu/symbols/flag_en

[3] European Research Council (ERC) – Guidelines on Implementation of Open Access to Scientific Publications and Research Data in projects supported by the European Research Council under Horizon 2020 – Version 1.1 – 21 April 2017. Available at: http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/oa-pilot/h2020-hi-erc-oaguide_en.pdf

[4] Guidance: Social media guide for EU funded R&I projects. Available at: http://ec.europa.eu/research/participants/data/ref/h2020/other/grants_manual/amga/soc-med-guide_en.pdf

[5] Horizon 2020 Work Programme 2016 2017. Available at: http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-transport_en.pdf

[6] IPR helpdesk brochure "Making the Most of Your H2020 Project. Boosting the impact of your project through effective communication, dissemination and exploitation. Available at: https://www.iprhelpdesk.eu/sites/default/files/EU-IPR-Brochure-Boosting-Impact-C-D-E_0.pdf

[7] Open access & Data management. Available at: http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross cuttingissues/open-access-data-management/open-access_en.htm

Annex A: Cyber-MAR 1st Press Release

PRESS RELEASE
Preparedness first, security always!

18-20 September 2019

Cyber-MAR: Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain

Cyber-MAR Kick-Off Meeting was officially launched in Porto Cheli, Greece on 18th to 20th September 2019. Cyber-MAR, is an EU-funded H2020 innovation action, that addressed the call SU-DS01-2018 of the H2020 Programme and consists of 13 partners from 8 EU countries, united in their vision to boost cyber preparedness in the maritime sector as a highly prioritize aspect.

The aim of Cyber-MAR, coordinated by the Institute of Communication & Computer Systems (ICCS), is to fully unlock the value of using cyber range in the maritime logistics value chain via the development of an innovative simulation environment adapting in the peculiarities of the maritime sector, but being at the same time easily applicable in other transport subsectors. A combination of innovative technologies are the technology enablers of the proposed Cyber-MAR platform, which is both a knowledge-based platform and a decision support tool to cybersecurity measures, by deploying novel risk analysis and econometric models. Collected and analysed CSIRTs/CERTs data will feed the knowledge-based platform with new target scenarios and exercises.

Through Cyber-MAR, the maritime logistics value chain actors will increase their cyber-awareness level and will validate their business continuity management, towards minimizing their business disruption potential. Cyber-MAR will act also as a cost-efficient training solution covering the maritime logistics value chain.

Project Coordinator
Dr. Angelos Amditis
Institute of Communication and Computer Systems - ICCS
a.amditis@iccs.gr

Project Manager
George Baroutas
Institute of Communication and Computer Systems - ICCS
george.baroutas@iccs.gr

Dissemination Manager
Mrs. Evangelia Latsa
SEAbility Ltd
adm@seability.eu

www.cyber-mar.eu
Cyber_MAR

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389. The content of this document reflects only the authors' view and the European Commission is not responsible for any use that may be made of the information it contains.

Annex B: Cyber-MAR communication/dissemination procedures

Communication Dissemination procedures

Description and purpose

The participation of any Partner in an event as well as the performance of every dissemination & communication activity related to Cyber-MAR project has to be **approved beforehand by the Cyber-MAR Project Coordinator, the project Executive Board (EB) and the Security Advisory Board (SAB).**

Basic objective:

Production of high quality Cyber-MAR publications, presentations and other communication material;

Avoidance of overlaps and possible disclosure of restricted or confidential information;

Monitoring and recording of the dissemination activities of the project in an effective and efficient way.

Step by step procedure:

Fill in the spaces of the table below;

Store your material (abstract, draft paper, poster, presentation etc.) to the related Redmine DMSF;

Submit your dissemination request, including the Security Sensitivity Assessment form, stored in Redmine allowing **for minimum two weeks before submission** deadline by email to the WP7 leader (e.krikigianni@seability.eu; vasiliki.palla@seability.eu).

WP7 Leader has 2 days to react and send the request to Coordinator/EB/SAB for approval, modification or rejection;

Coordinator/EB/SAB decision send to the WP7 Leader ***within five working days***; If no answer is received by the set deadline it is taken as an approval;

WP7 Leader informs the initiator of the dissemination activity along with the involved partner(s) about the decision.

In case of:

A) **Approval**: When approval is given through the WP7 Leader, the partner(s) is (are) free to proceed with the realisation of the proposed dissemination activity;

B) **Conflict/objection**: Any EB member can reject the proposed dissemination activity if they have objections, related to overlaps or possible disclosure of restricted or

confidential information concern the work performed in the different WPs. In case of conflict, the issue will be discussed among the coordinator, the WP7 Leader and the involved partners;

***If a conflict is created or further material is needed then WP7 Leader informs the partner that modifications or additions are required. Then the material is proposed again to WP7 Leader and if significant changes (that might provoke conflicts among partners' interests) must be made, the previous procedure is followed.*

Dissemination activities report: Within ***ten working days*** after the realisation of the approved dissemination activity, the partner should provide the **WP7 Leader** (e.krikigianni@seability.eu; vasiliki.palla@seability.eu) with the **filled in dissemination report** and the **presented material** (final paper, presentation, poster etc.). The dissemination report form is stored in the Redmine DMSF**.** All material will be archived to the Redmine DMSF in the respective folders; it will be also highly appreciated if the lead partner of every dissemination activity provides the WP7 Leader with some **photos** of their participation at the different events.

NOTE:

If partners wish to present or release material already approved as public presentation and other communication material, then no formal approval is required. The WP7 Leader (e.krikigianni@seability.eu; vasiliki.palla@seability.eu) has to be informed. If there are no objections, then the WP7 Leader notifies the authors to proceed with the dissemination activity.

In case a partner wishes to organise a workshop or special event related to Cyber-MAR, then the approval of WP7 Leader and the information of the Coordinator and the EB is also needed **2 months** before the realisation of this dissemination activity.

Non-European Travel

*** For non-European travels the Project Officer should be informed and an approval from his side is required. Please fill-in the* ***Non-European Travel Report Template*** *at least* ***two months*** *before the travel and send the form to the project Coordinator (a.amditis@iccs.gr), so as to inform the EC. For possible enquiry by the auditors in the future it is recommended to keep the form and EC's response with the respective travel documents.*

Acknowledgement-Information on EU funding

According to the Articles 29 & 38 of Cyber-MAR Grand Agreement, any dissemination of results (in any form, including electronic) must display the EU emblem and must include the following acknowledgement text:

"Cyber-MAR project has received funding from the European Union's Horizon 2020 research & innovation programme under grant agreement No. 833389. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains".

For any communication activity, the EU emblem must be displayed, along with the phrase:

"Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains".

For infrastructure, equipment & major results, the EU emblem must be displayed along with the phrase:

"This [infrastructure][equipment] [insert type of result] is part of the Cyber-MAR project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389."

When displayed together with another logo, the EU emblem must have the appropriate prominence. For correct use of the EC emblem please use the following link:

European flag: http://europa.eu/about-eu/basic-information/symbols/flag/index_en.htm

For further information please contact the WP7 Leader (e.krikigianni@seability.eu; vasiliki.palla@seability.eu)

Dissemination Requests Table

2019

No.	*Date of Dissemination request*	*Main Leader*	*Type of activity*	*Title of the Event/Journal*	*Date & Location*	*URL/Webpage*	*Title of publication/presentation*	*Abstract*	*Authors*	*Relation to Cyber-MAR*	*REDMINE link to document*
0.	*dd/mm/yyyy*	*name, organisation*	*Please choose one: Journal article, conference, special session, paper presentation, workshop, demonstration, exhibition, trade fair, press/media activity, poster, video, website, ...,*					*Up to 300 words*	*Cyber-MAR partners*	*Related WPs & Tasks*	*Documents should be placed here*

Annex C: Cyber-MAR Security Sensitivity Assessment Form (SSA)

SSA form

(Self-Declaration by the authors)

Publication Identification		
Title of Publication:		
Authors (Name/Affiliation)		
Type of publication:		
Type of presentation:		
If this is a deliverable:	To which SP/WP/Deliverable this publication is related to:	
	Dissemination level (CO/PU):	
Else:	Which conference:	
	Where it will be published:	
Please fill in below:		
This is:	☐ pre-assessment	
	☐ final assessment	
List the input material used in the publication/deliverable:	1.	
List the results developed and presented in the publication/deliverable:	1.	
The draft publication:	☐ is attached to this statement	
	☐ can be found in the link	
This publication does not include any data or information that could be interpreted as security sensitive:	☐ True	
	☐ Not sure	
If not sure, please specify what are the material/results that you are not sure if they are security sensitive? Why?		

(To be filled only by the SAB members)

Date:	
Signature of the Responsible Author:	
Comments of the Security Advisory Board:	☐ The publication can be published as it is.
Type of presentation:	☐ Before publication the following modifications are needed:
	1.

Date:

On behalf of the Security Advisory Board:

Signature of a member of the Security Advisory Board

Annex D: Cyber-MAR indicative list of proposed scientific journals

No.	Title of journal/magazine	Website	Description
1	Maritime Journal: Insight for the European Commercial Marine Business	https://www.maritimejournal.com/news101/security-and-alarm-systems/seawall-maritime-cyber-security	Maritime Journal is the multimedia magazine for the European Commercial Marine industry. Available in-print, online and as a weekly e-Newsletter. Maritime Journal's valued content focuses on vessel operations and projects, both inshore and offshore, including ports and harbors. From operations managers and superintendents to harbor masters. Maritime Journal is relied upon by marine professionals for news and information to help them do their jobs and run their businesses more effectively.
2	IEEE journals & Magazines	https://ieeexplore.ieee.org/Xplore/home.jsp	IEEE publishes the leading journals, transactions, letters, and magazines in electrical engineering, computing, biotechnology, telecommunications, power and energy, and dozens of other technologies. Almost all of these publications are available electronically through the IEEE Xplore® digital library.
3	International Journal on Advances in Security	http://www.iariajournals.org/security/	The journal focuses on specific aspects related to security, trust, privacy, authentication, authorization, and specific frameworks, architectures and protocol to enforce access and ownership rules and protect the assets, stored data, and communications. Specific topics may focus on cryptographic solutions, quantum security, forensic methodology, negotiated trust, information security, malware, threat propagation, traffic profiling, security in dynamic environments, security in P2P networks, Internet security, special security protocols, access security, security management, and security in mission critical systems.
4	International Transport Journal	https://www.transportjournal.com/home.html?L=zwvrmckyyv.html.html.html	An International Transport Journal, which is trilingual (English, French, German) and multimodal journal for transport & logistics worldwide. It focuses on thematic areas such as Shipping & ports, Aviation , Intermodal/road, Forwarding & Logistics and also People & Companies.
5	Journal of Cyber Security and Information Systems	https://www.csiac.org/journal-issue/	The Journal of Cyber Security and Information Systems is a quarterly journal focusing on scientific and technical research & development, methods and processes, policies and standards, security, reliability, quality, and lessons learned case histories.
6	European Cybersecurity Journal	https://cybersecforum.eu/en/about-ecj/	The European Cybersecurity Journal (ECJ) is a specialized publication devoted to cybersecurity. The main goal of the Journal is to provide concrete policy recommendations for European decision-makers and raise awareness on both issues and problem-solving instruments. The Journal had its premiere during the CYBERSEC Forum 2015. The ECJ is a platform of regular dialogue on the most strategic aspects of cybersecurity. Readers of the ECJ get insights on the most important trends in cybersecurity and have an opportunity to get to know first-hand perspectives from leading specialists.
7	Journal of Cybersecurity	https://academic.oup.com/cybersecurity/pages/About	Journal of Cybersecurity publishes accessible articles describing original research in the inherently interdisciplinary cyber domain. Journal of Cybersecurity is premised on the belief that computer science-based approaches, while necessary, are not sufficient to tackle cybersecurity challenges. Instead, scholarly contributions from a range of disciplines are needed to understand the varied aspects of cybersecurity. Journal of Cybersecurity provides a hub around which the interdisciplinary cybersecurity community can

			form. The journal is committed to providing quality empirical research, as well as scholarship, that is grounded in real-world implications and solutions.
8	Journal of Cyber Security Technology	https://www.tandfonline.com/action/journalInformation?journalCode=tsec20	4 issues per year Digital Preservation Policy The Journal of Cyber Security Technology has a robust archival strategy in place that provides for the deposit of its electronic source files into an acceptable non-profit third party archive, including Portico and LOCKSS, so that your articles will be actively preserved. As a Taylor & Francis journal, Journal of Cyber Security Technology is also a participant in the CLOCKSS project. _Taylor & Francis is a member of the Committee on Publications Ethics (COPE). Taylor & Francis is committed to peer review integrity and upholding the highest standards of review in our journals. To help us maintain these high standards, we provide guidelines for ethical publishing.
9	International Journal of Cyber security and Digital Forensics (IJCSDF)	http://sdiwc.net/ijcsdf/	The International Journal of Cyber-Security and Digital Forensics (IJCSDF) is a knowledge resource for practitioners, scientists, and researchers among others working in various fields of Cyber Security, Privacy, Trust, Digital Forensics, Hacking, and Cyber Warfare. We welcome original contributions as high quality technical papers (full and short) describing original unpublished results of theoretical, empirical, conceptual or experimental research. All submitted papers will be peer-reviewed by members of the editorial board and selected reviewers and those accepted will be published in the next volume of the journal.
10	Twentyfour7. Enabling sustainable societies with smart technology	https://www.wartsila.com/twentyfour7	A technical journal by Wartsila stakeholders focused on maritime, energy, environment, people & innovations, packed with white papers, detailed technical articles, news on the latest technologies and trends, detailed case studies, and service solutions – here's everything tech-savvy people need to know.
11	WMU Journal of Maritime Affairs	https://www.wmu.se/publications/wmu-journal	The WMU Journal of Maritime Affairs (WMU JoMA) is an international journal that covers the subject areas of maritime safety, marine environment protection and shipping operations and gives, in this context, special attention to the human element and the impact of technology. WMU JoMA is for professionals in maritime administration, industry and education. It aims at serving the international maritime community by presenting fresh ideas and current thinking on subjects of topical interest, reporting on relevant research findings and addressing interrelationships between safety, environment protection and efficiency of maritime transport.
12	HANSA - International Maritime Journal	https://hansa-online.de/ueber-uns-hansa/	HANSA Journal is today one of the leading international maritime journals. It provides decision makers with information about the industry every month. The main categories that HANSA focuses on are Market, Shipping, Shipbuilding, Maritime security, Port & Offshore, while specialists will find a detailed background with information about the latest developments in the maritime sector.
13	TransNav: International Journal On Marine Navigation and Safety on Sea Transportation	http://www.transnav.eu/	The TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation is addressed to scientists and professionals in order to share their experience, expert knowledge and research results, concerning all aspects of navigation and sea transportation. The Journal is published four times a year and contains original papers contributing to the science of broadly defined navigation: from the highly technical to the descriptive and historical, over land through the sea, air and space, including those presented at the TransNav conferences, to promote young researchers, new field of maritime sciences and technologies. The focus of TransNav is high-quality, scholarly research that addresses

			development, application and implications, in the field of maritime education, maritime safety management, maritime policy sciences, maritime industries, marine environment and energy technology. Subjects of papers include electronics, astronomy, mathematics, cartography, command and control, psychology, operational research, risk analysis, theoretical physics, operation in hostile environments, instrumentation, ergonomics, financial planning and law. Also of interest are logistics, transport and mobility. The Journal provides a forum for transportation researchers, engineers, navigators, ergonomists, and policy-makers with an interest in maritime researches. From contemporary issues to the scientific, technological, political, economic, cultural and social aspects of maritime shipping, transportation and navigation, the TransNav publishes innovative, interdisciplinary and multidisciplinary research on marine navigation subjects and is set to become the leading international scholarly journal specializing in debate and discussion on maritime subjects. The TransNav is especially concerned to set maritime studies in a broad international and comparative context.
14	SEAS: The Journal of International Maritime Safety, Environment Affairs and Shipping	http://www.jimseas.org/html/AimsAndScope.html http://www.transnav.eu/	The Journal of International Maritime Safety, Environment Affairs and Shipping (SEAS) addresses all aspects of international maritime safety, environmental affairs and shipping. SEAS publishes peer-reviewed scholarly articles, notes and comments as well as book reviews. All papers published in this journal are reviewed by qualified peers prior to acceptance and publication. Examples of topics that are considered to be appropriate for the journal include, but are not limited to, the following: Ship design, systems and equipment, Navigation, search and rescue, Marine pollution, liability and compensation, Maritime security, maritime human factors, shipping and port management, marine accident & traffic risk assessment. SEAS encourages submissions of articles related to recent issues discussed within International Maritime Organization (IMO). Notes and comments are also welcome. So far, maritime issues that have been dealt within IMO have been discussed in separate academic sectors. As a multi-disciplinary journal, SEAS aims to provide an integrated forum for all the academic/practical sectors involved. SEAS is produced by the Korea Institute of Ocean Science and Technology (KIOST) and the Korean Society of Marine Environment and Safety (KOSOMES), with the financial support from Ministry of Oceans and Fisheries of the Republic of Korea (MOF).
15	Journal of Maritime Research	https://www.jmr.unican.es/index.php/jmr/about	JMR publishes original research papers in English analysing the maritime sector international, national, regional or local. JMR is published quarterly and the issues-whether ordinary or monographic-include both theoretical and empirical approaches to topics of current interest in line with the editorial aims and scope of the journal. The objective of JMR is to contribute to the progress, development and diffusion of research on the maritime sector. The aim is to provide a multidisciplinary forum for studies of the sector from the perspective of all four of the following broad areas of scientific knowledge: experimental sciences, nautical sciences, engineering and social sciences. The manuscripts presented must be unpublished works which have not been approved for publication in other journals. They must also fulfil all the requirements indicated in the 'Technical specifications' section. The quality of the papers is guaranteed by means of a process of blind review by two scientific referees and one linguistic reviewer. Although the journal is

			published in print format, the processes of submission and reception of manuscripts, as well as revision and correction of proofs are all done electronically.
16	International Journal of Maritime Technology	http://ijmt.ir/	"International Journal of Maritime Technology" (IJMT) is a fully open access, double blind, peer reviewed, electronic and print, bi-quarterly publication which covers areas related to maritime technology such as Offshore Engineering; Naval Architecture; Marine Structural Mechanics; Safety and Reliability; Materials; Pipelines and Risers; Polar and Arctic Engineering; Computational Fluid Dynamics; Vortex Induced Vibrations; Port and Waterfront Design and Engineering; Linear and Nonlinear Wave Mechanics; Hydrodynamics; Fluid-Structure Interaction; Cable, Mooring, Buoy Technology; Underwater Technology; Geotechnology; Foundation Engineering; Ocean Mining; Coastal Engineering; Marine Renewable Energy; Aquacultural Engineering; Instrumentation; Full-Scale measurements; Model Tests; Satellite Observations; Marine Environmental Engineering; Stochastic Processes; Hydroelasticity, Subsea Engineering; Fluid Mechanics; Ocean Acoustics, Oceanographical Engineering; Computational Methods/Numerical Analysis; Shore Protection; beach nourishment; sediment transport; Risk and Limit State Design and Assessment; Ship Maneuvering; Seakeeping and Control Systems; and Ship Resistance and Propulsion. Discussion on a paper is open until three months after publishing of it. In case of the approval of the Editorial Board of the Journal, the authors of the paper will be invited to send their reply for publication in the next issues of the journal. The discussion and the authors' reply will be printed in the second further issues of the journal. Marine scientists and academic are invited to contribute their knowledge and experience. The publication appears at regular time intervals two times a year. IJMT is fully open access and full texts of published articles are available to the public through the journal's website for free. IJMT practices peer-review process to control the scholarly content of submitted manuscripts by international experts. IJMT's Editorial Board selects manuscripts with excellence in content, preferably without commercial targets.
17	International Journal of Maritime History	https://journals.sagepub.com/home/ijh	The International Journal of Maritime History (IJMH) is the journal of the International Maritime Economic History Association. The IJMH is a fully-refereed, quarterly publication which addresses the maritime dimensions of economic, social, cultural, and environmental history. Truly international in scope, the IJMH publishes studies of a multidisciplinary nature on a broad range of maritime historical themes, including shipping, shipbuilding, seafaring, ports, resorts and other coastal communities, sea-borne trade, fishing, environment and the culture of the sea. This journal is a member of the Committee on Publication Ethics (COPE).

Annex E: Cyber-MAR indicative list of proposed events

Date	Event	Location	Website
2019			
24/9/2019	The Future of Cyber Security	Central Manchester	https://cybermanchester.events/
26/9/2019	7th ENISA National Cyber Security Strategies (NCSS) workshop	Warsaw, Poland	https://www.enisa.europa.eu/events/7th-ncss-workshop/event
30-02/10/2019	IEEE 5G World Forum	Dresden, Germany	https://ieee-wf-5g.org/
7-9/10/2019	Digital Transport Days 2019	Helsinki	Please register by 25 September 2019: www.digitaltransport.eu/2019/register
8/10/2019	Validation workshop for Good practices for security of IoT SDLC	Brussels , Belgium	https://www.enisa.europa.eu/events/validation-workshop-ssdlc-for-iot/validation-workshop-for-good-practices-for-security-of-iot-sdlc
8/10/2019	Seminar On Trends and Challenges after the Paris Agreement: Global Maritime Technology Cooperation Centre (MTCC)	Malmö	---
10-11/10/2019	The Smart Ship Exchange	Athens , Greece	https://worldmaritimenews.com/events/the-smart-ship-exchange/
15/10/2019	Cyber Investor Day (The European Cyber Security Organization (ECSO))	Luxembourg	https://ecs-org.eu/agenda
15-25/10/2019	CYBERSECURITY WEEK 2019	Luxembourg	https://www.cybersecurityweek.lu/
24-25/10/2019	3rd ENISA - Europol IoT Security Conference	Athens , Greece	https://www.enisa.europa.eu/events/3rd-europol-enisa-iot-security-conference
29-30/10/2019	CYBERSEC EXPO 2019, WHERE CYBER MEETS SECURITY	Katowice, Poland	https://cybersecforum.eu/en/expo/
04-05/11/2019	SCADA Security	Prague, Czech republic	http://future-forces-forum.org/events/default/32_scada-security-conference?lang=en
05-06/11/2020	Security Research Event	Helsinki, Finland	https://www.sre2019.eu
12/11/2019	The Future of Cyber Security	Central London	https://cybereurope.events/
14-15/11/2019	F&L Napoli Meeting	Napoli, Italy	https://www.europeanfreightleaders.eu/napoli-2019/
26/11/2019	The Future of Cyber Security Europe	Central London	https://cybereurope.events/
26/11/2019	ENISA Maritime Cybersecurity Workshop	European Maritime Safety Agency, Portugal	https://www.enisa.europa.eu/events/enisa-maritime-cybersecurity-workshop/event
26-27/11/2019	2019 Annual Meeting of Marine Technology (Technological conference & exhibition)	Eugenides Foundation Auditorium, Athens	http://www.elintconference.gr/
28/11/2019	End-User Workshop in Piraeus	PCT S.A. Neo Ikonia, Perama, Greece	---
02-05/12/2019	Black Hat Europe 2019 Conference	Exceln London/United Kindom	https://www.blackhat.com/eu-19/

17-18/12/2019	ITS Hellas 2019	Athens Greece	https://www.its-hellas.gr/gr/news/10-latest-news/206-5th-its-hellas-conference-and-exhibition-save-the-date-2
2020			
28/01/2020	The Future of Cyber Security	Manchester	https://cybermanchester.events
28-29-30/01/2020	International Cybersecurity Forum (FIC2020)	Lille Grand Palais (France)	https://www.forum-fic.com/en/home/visit/prepare-your-visit/date-place-timings.htm
30-31/01/2020	2020 CTI-EU | Bonding EU Cyber Threat Intelligence	Brussels , Belgium	https://www.enisa.europa.eu/events/2019-cti-eu/2019-cti-eu-bonding-eu-cyber-threat-intelligence
17/02/2020	ENISA Industry Event 2020	Bruxelles , Belgium	https://www.enisa.europa.eu/events/enisa-industry-event-2020/enisa-industry-event-2020
25-27/02/2020	6th International Conference on Information Systems Security & Privacy	Valleta, Malta	http://www.icissp.org/
10/03/2020	CYpBER Conference 2020	Cyprus	https://www.cypber.com/
10-13/03/2020	Africa ICS Cybersecurity Conference and Expo 2020	Nairobi, Kenya	https://www.africaicscybersecurityconference.com/
17-20/03/2020	SITL Transport & Logistics Innovation Week	Paris, France	https://www.sitl.eu/en/home/
24/03/2020	3rd CybersecEU Brussels Leaders Foresight 2020	Brussels, Belgium	https://cybersecforum.eu/en/brussels/
24/03/2020	The Future of Cyber Security Europe	London, UK	https://cybereurope.events
21-23/04/2020	5th Singapore Maritime Technology Conference Exhibition	Marina Bay Sands Singapore	https://www.ibc-asia.com/event/singapore-maritime-technology-conference/
13-14/05/2020	Cyber Investor Days	Brussels	https://www.ecs-org.eu/agenda#cyber-investor-days-in-brussels
01-05/06/2020	Posidonia 2020	Athens, Greece, Metropolitan Expo	http://posidonia-events.com/
09-11/06/2020	TOC Europe	Ahoy Rotterdam, Netherlands	https://www.tocevents-europe.com/en/Home.html
10-13/06/2020	IAME Conference	The Hong Kong Polytechnic University, Hong Kong	https://www.polyu.edu.hk/fb/IAME2020/
16-18/06/2020	5th IEEE European Symposium on Security and Privacy	Genoa, Italy	https://www.ieee-security.org/TC/EuroSP2020/workshops.html
29-03/07/2020	Forum on Integrated and Sustainable Transportation Systems	The Netherlands	https://conferences.ieee.org/conferences_events/conferences/conferencedetails/46898
26-30/07/2020	CYBER 2020	Nice, France	https://www.iaria.org/conferences2020/CYBER20.html
10-12/09/2020	IEEE 5G World Forum	Bangalore, India	https://ieee-wf-5g.org/
20-23/09/2020	IEEE ITSC (Intelligent Transportation Systems Conference)	Rhodes, Greece	tbc
24/09/2020	The Future of Cyber Security	Manchester	https://cybermanchester.events
27/09 - 01/10 2020	ICIMP 2020, The Fifteenth International Conference on Internet Monitoring and Protection	Rome, Italy	http://www.iaria.org/conferences2020/ICIMP20.html

04-08/10/2020	ITS World Congress 2020	LA, USA	https://www.itsworldcongress2020.com/
03-05/11/2020	European Cybersecurity Forum	Katowice	https://cybersecforum.eu/en/katowice/
05-06/11/2020	Future Technologies Conference (FTC) 2020	Vancouver, Canada	http://saiconference.com/FTC
26/11/2020	The Future of Cyber Security Europe	London, UK	https://cybereurope.events
2020	The SmartShip Exchange		https://www.gem-exchanges.com/
2021			
11-12/02/2021	International Conference on Cybersecurity	Barcelona, Spain	https://waset.org/conference/2021/02/Barcelona/ICC
04-07/05/2021	Transport & Logistic Trade Fair	Exhibition of Munich	https://www.transportlogistic.de/index-2.html