enisa
European Network and Information Security Agency

ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR

November 2011

Contributors to this report

ENISA would like to express its gratitude to all contributors of this analysis.

ENISA would also like to recognise the contribution of the Deloitte team members that prepared this analysis in collaboration with and on behalf of ENISA:

- Mr. Dan Cimpean;
- Mr. Johan Meire;
- Mr. Vincent Bouckaert;
- Mr. Stijn Vande Casteele;
- Mrs. Aurore Pelle.
- Mr. Luc Hellebooge;

Acknowledgements

ENISA would like to acknowledge the contribution to the maritime cyber security workshop organised in the light of this project and the report, and in particular:

- Mr. Andrea Servida, from DG INFSO;
- Mr. Jean-Bernard Erhardt and from DG MOVE;
- Mr. Jukka Savo, from DG MOVE;
- Mr. Allard Kernkamp, from CPNI.NL;
- Assistant Professor Nineta Polemi, the University of Piraeus, Dept. of Informatics

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of expertise for the European Union (EU), its Member States (MS), the private sector and Europe's citizens. As an EU agency, ENISA's role is to work with these groups to develop advice and recommendations on good practice in information security. The agency assists MS in implementing relevant EU legislation, and works to improve the resilience of Europe's critical information infrastructure and networks. In carrying out its work programme, ENISA seeks to enhance existing expertise in MS by supporting the development of cross-border communities committed to improving network and information security throughout the EU.

Contact details

For questions related to Cyber Security aspects in the maritime sector, please use the following details:

- **Mr. Wouter VLEGELS** - Expert, Critical Information Infrastructure Protection
  E-mail: wouter.vlegels@enisa.europa.eu

Contents

1 Executive Summary 1
2 Introduction 4
2.1 The maritime sector as critical infrastructure 4
2.2 The policy context 5
2.3 Purpose and scope of the study 6
2.4 Target audience 7
2.5 Approach 7
2.5.1 Desk top research 7
2.5.2 Interviews and questionnaires 7
2.5.3 Workshop 8
3 Key findings and recommendations 9
3.1 Low awareness and focus on maritime cyber security 9
3.1.1 Impact 9
3.1.2 Recommendations 9
3.2 Complexity of the maritime ICT environment 10
3.2.1 Impact 10
3.2.2 Recommendations 11
3.3 Fragmented maritime governance context 12
3.3.1 Global level 12
3.3.2 European level 13
3.3.3 National/Regional level 14
3.4 Inadequate consideration of cyber security in maritime regulation 15
3.4.1 Impact 15
3.4.2 Recommendations 15
3.5 No holistic approach to maritime cyber risks 16
3.5.1 Impact 16
3.5.2 Recommendations 16
3.6 Overall lack of direct economic incentives to implement good cyber security in maritime sector 17

3.6.1 Impact 17
3.6.2 Recommendations 18
3.7 Inspiring initiatives, a call for collaboration 18
3.7.1 Results 18
3.7.2 Recommendations 19
4 Conclusions & suggested next steps 20
Short-term 20
Mid-term 20
Long-term 21
5 APPENDIX A Workshop report 22
5.1 List of keynote speakers 22
5.2 Keynote summaries 23
5.2.1 EU Policy on network and information security and CIIP 23
5.2.2 SafeSeaNet 23
5.2.3 Management of public-private partnerships and information sharing for the protection of critical infrastructures 24
5.2.4 Open issues and proposals in the security management of PIT systems – The S-Port national case 24
5.3 Group discussions 25
6 APPENDIX B Summary of key findings and recommendations 26

Executive Summary

The maritime sector is critical for the European society. Recent statistics show that within Europe, 52%[1] of the goods traffic in 2010 was carried by maritime transport, while only one decade ago this was only 45%. This continuous increase in dependency upon the maritime transport underlines its vital importance to our society and economy. As it can be observed in other economic sectors, maritime activity increasingly relies on Information Communication and Technology (ICT) in order to optimize its operations. ICT is increasingly used to enable essential maritime operations, from navigation to propulsion, from freight management to traffic control communications, etc.

These last years have also shown that cyber threats are a growing menace, spreading in all industry sectors that progressively rely on ICT systems. Recent examples of deliberate disruption of critical automation systems, such as Stuxnet[2], prove that cyber-attacks can have a significant impact on critical infrastructures. Disruption or unavailability of these ICT capabilities might have disastrous consequences for the European Member States' governments and social wellbeing in general. The need to ensure dependability and the ICT' robustness against cyber-attacks is a key challenge at national and pan-European level.

This first analysis of the cyber security aspects in the maritime sector identified key insights and considerations regarding this area. It also touches on the policy context at the European level and situates the topic of cyber security in the maritime sector as a logical next step in the global protection effort of ICT infrastructure. This document identifies essential problematic areas as well as initiatives being implemented, which could serve as a baseline towards helping the development of cyber security in this particular context. Finally, high-level recommendations are presented for each observation, suggesting the possible approaches that could be taken for addressing these risks.

High-level observations and recommendations

- The awareness on cyber security needs and challenges in the maritime sector is currently low to non-existent. Member States should consider developing and implementing awareness raising campaigns targeting the maritime actors. In particular the provision of appropriate cyber security training to relevant actors (e.g. shipping companies, port authorities, etc.) would be highly recommended.. Such awareness campaigns and training initiatives should target all relevant actors involved in the maritime sector, while their provision could be coordinated by relevant cyber security organisations (e.g. national cyber security offices, national CERTs, public-private partnerships, etc).

---

[1] *In terms of value in Euros. Source: Eurostat database: EXTRA EU27 Trade Since 2000 By Mode of Transport (HS6)*

[2] *http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis*

- Due to the high ICT complexity and the use of specific technologies, there are particular challenges to ensure adequate security provisions in maritime systems. It would be beneficial for all stakeholders to agree on a common strategy and development of good practices for the technology development and implementation of ICT systems in the maritime sector and ensuring "security by design" for all critical maritime ICT components.

- As current maritime regulations and policies consider only the physical aspects of security and safety, it is recommended that policy makers add cyber security aspects to them.

- We strongly recommend a holistic risk-based approach, which would require the assessment of existing cyber risks associated with the current ICT systems implementations relevant to the European maritime sector as well as the identification of all critical assets within this sector. For maritime economic operators and stakeholders, it is important to proactively apply sound cyber and information security risk management principles within their organisations and environments.

- With the maritime governance context being fragmented between different levels (i.e. international, European, national), the International Maritime Organisation together with the European Commission and the Member States should consider aligning and harmonizing international and European policies related to this sector, particularly on its cybersecurity aspects. Member States should clearly specify the roles and responsibilities that should be endorsed for addressing cyber security matters at those various levels.

- Proper coordination and cooperation between the relevant stakeholders should also be defined (e.g. CERTs and port authorities, shipping companies, etc.) through public-private sector interaction. We would recommend Member States to stimulate dialogue and public-private partnerships between the key stakeholders in the maritime sector (e.g. shipping companies, port authorities, etc.) and connected stakeholders (e.g. insurance companies / brokers).

- From a different perspective, better information exchange and statistics on cyber security may help insurers to improve their actuarial models, reduce own risks, and therefore offering better contractual insurance conditions to the involved maritime stakeholders. Information exchange platforms, as for instance the ones implemented by CPNI.NL, should be also considered and developed by Member States in order to foster and facilitate communication on cyber security for the relevant maritime actors.

For further details and additional observations, please refer to chapter 3 ('Key findings and recommendations') and chapter 4 ('Conclusions & suggested next steps') of this document.

1 Introduction

1.1 The maritime sector as critical infrastructure

The maritime sector sustains society and the economy through the movement of people and vital goods, such as energy (transportation of oil and gas), food[3], etc. The criticality of the maritime sector for the European Member States and economies is clearly illustrated by available data:

- In Europe, 52%[4] of the goods traffic in 2010 was carried by maritime transport, where only one decade ago this was only 45%. This increase in maritime transport dependency underlines its vital importance to our society and economy. Based on data from the European Commission[5], around 90% of EU external trade and more than 43% of the internal trade take place via maritime routes. Industries and services belonging to the maritime sector, contribute between 3 and 5 % of EU Gross Domestic Product (GDP), and maritime regions produce more than 40 % of Europe's GDP. 22 Member States with maritime border manage more than 1.200 sea ports supporting the maritime sector activity.
- Three major European seaports (i.e. Rotterdam, Hamburg and Antwerp[6]) accounted in 2010[7] for 8% of overall world traffic volume, representing over 27,52 Million-TEUs. Additionally, these seaports handled more than 50% of the entire European waterborne foreign container trade. The main European seaports carried in 2009 17,2% of the international exports and 18% of the imports[8].

The European economy is therefore critically dependent upon the maritime movement of cargo and passengers. On the other hand, the maritime activity increasingly relies on Information Communication and Technology (ICT) to optimize its operations, like in all other sectors. ICT is used to enable essential maritime operations, from navigation to propulsion, from freight management to traffic control communications, etc. These last years have also shown that cyber threats are a growing menace, spreading in all sectors. Disruption or unavailability of these ICT capabilities might have disastrous consequences - therefore there is an increased need to ensure the ICT robustness against cyber-attacks and dependability is a key challenge at national and pan-European level.

Securing the critical infrastructure of the maritime sector is increasingly becoming a priority for the key European stakeholders, including the European Commission, Member State governments and the main actors from the private sector.

---

[3] *See EICAR Conference Best Paper Proceedings 2003*
[4] *In terms of value in Euros. Source: Eurostat database: EXTRA EU27 Trade Since 2000 By Mode of Transport (HS6) (DS_043328), accessed on 02/08/2011.*
[5] *http://ec.europa.eu/maritimeaffairs/maritimeday/pdf/proceedings_en.pdf*
[6] *In terms of goods' transhipments in 2008, Rotterdam, Antwerp, Hamburg ports were the most important in Europe.*
[7] *http://www.worldshipping.org/about-the-industry/global-trade/top-50-world-container-ports*
[8] *Eurostat database: Trade in goods, by main world traders (tet00018), accessed on 02/08/2011.*

1.2 The policy context

Critical information infrastructures support vital services and goods such as energy, transport, telecommunications, financial services, etc., that are so essential that their unavailability may adversely affect the well-being of a nation. Due to their significant importance, the protection of critical information infrastructures is required to sustain and further enhance the well-being of the European society, the European Union economy, and the European citizens. Therefore, this subject has also become an attention area for the policy makers in the European Union (EU).

The European Commission adopted a Communication[9] to improve the protection of European Critical Infrastructure (ECI) from terrorism via the European Programme for Critical Infrastructure Protection (EPCIP) – and the Directive on the identification and designation of European Critical Infrastructures[10].

In April 2009 the Commission sent another communication[11] to the Council giving its views on how the Member States might strengthen the security and resilience of their critical information infrastructures and develop their defences against cyber attacks. The aim was to stimulate and support the development of a high level of preparedness, security and resilience capabilities both at national and European level. This approach was broadly endorsed by the Council.

The Digital Agenda for Europe[12] adopted in May 2010 emphasised the need for all stakeholders to join their forces in a holistic effort to ensure the security and resilience of ICT infrastructures, by focusing on prevention, preparedness and awareness, as well as to develop effective and coordinated mechanisms to respond to new and increasingly sophisticated forms of cyber-attacks and cyber-crime. This approach envisages that both the preventive and reactive dimensions of the challenge are duly taken into account.

The Digital Agenda for Europe outlines seven priority areas for action, and attributes an important role to ENISA in relation to the priority area of "Trust and security". ENISA continues underpinning Member States and private sector efforts to enhance the resilience and security of their networks. In particular, the Agency wants to develop cooperation and information exchanges between the Member States and private sector, on cyber security practices.

The Commission's most recent communication[13] on Critical Information Infrastructure Protection (CIIP) draws attention to the steady growth in the number, scope, sophistication and potential impact of threats to European Critical Information Infrastructures – be they natural or man-made. It brings forward achievements and next steps towards global cyber

[9] *See COM(2006) 786 of 12.12.2006*
[10] *See Council Directive 2008/114/EC of 08.12.2008*
[11] *See COM(2009) 149 of 30.03.2009*
[12] *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF*
[13] *See COM(2011) 163 of 31.03.2011*

security by structurally addressing cyber risk and CIIP, focussing first on the energy and transport sectors.

Furthermore, it underlines the trend towards using ICT for political, economic and military predominance, The communication also reports that a purely European approach is not deemed sufficient to address the challenges ahead. Although the aim of building a coherent and cooperative approach within the EU remains important, the need to embed it into a global coordination strategy reaching out to key partners, be they individual nations or relevant international organisations is paramount.

It should be noted that in addition to the EU regulatory efforts, a number of Member States have also initiated own efforts in this area, for example France, Germany, Italy and the United Kingdom[14].

Additionally, efforts are also undertaken by the Directorate General for Mobility and Transport (DG MOVE) along with the European Maritime Safety Agency (EMSA) to facilitate secure data exchange between Member States' maritime authorities, through the SAFESEANET platform. SAFESEANET's main objective is to aid the collection, dissemination and harmonised exchange of maritime data. The network assists communication between authorities at local/regional level and central authorities thus contributing to prevent accidents at sea and, by extension, marine pollution, and that the implementation of EU maritime safety legislation will be made more efficient. As such, SAFESEANET implements the Directive 2010/65/EU of the European Parliament and of the Council, and offers a Community vessel traffic monitoring and information system.

1.3 Purpose and scope of the study

Firstly, this study aims to help the reader to gain a better understanding of key cyber security challenges in the maritime sector, including the main ICT risks.

Secondly, existing European, national and global initiatives on cyber security in the maritime sector are identified –allowing the reader to obtain a better overview of the status, good practices and on going developments in this area.

Thirdly, the study is aimed at the development of recommendations for the key relevant stakeholders in order to help them improving the overall security, safety and resilience of maritime capabilities dependent on ICT.

This study is based on the feedback received by subject matter expert representations from both public organisations (e.g. DG INFSO, DG MOVE and CPNI.NL,) and private companies (e.g. Deloitte, Cassidian) to the workshop on cyber-security aspects in the maritime sector[15]. (Please also refer to Appendix A for more details)

[14] *See results of the CI²RCO project*

[15] *http://www.enisa.europa.eu/act/res/workshops-1/2011/cyber-security-aspects-in-the-maritime-sector*

In the context of this study, cyber security should be understood in the way it is defined in the EU Proposal for A European Policy Approach being currently in-force: "*the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems*"[16].

Therefore, this study brings forward rules and policies that organisations involved in the maritime sector should consider putting in place to ensure network resilience from the point of view of information system protection.

1.4 Target audience

The target audience of this study consists of organisations, national authorities, government bodies and private companies that are involved in the maritime sector and especially in its cyber security aspects.

More specifically, this includes policymakers and other relevant stakeholders (e.g. Port Authorities) participating in the development and implementation of security guidelines and good practices for the maritime sector, as well as key players in the implementation of initiatives covering cyber security aspects.

1.5 Approach

The approach of this study was to collect input via desk research, individual interviews and questionnaires, while further discussion took place in a validation workshop organized by ENISA on 28 September 2011 in Brussels.

1.5.1 Desk top research

The literature on which this study is based includes reports on private / public-private partnerships initiatives, regulations and policies defined for maritime security and safety as well as specifications on ICT systems used within this sector.

A thorough analysis process took place in order to identify gaps and overlaps in regulations and policies, possible security issues linked to ICT systems and interesting initiatives.

1.5.2 Interviews and questionnaires

Stakeholders from both the public and the private sector (European Commission, Port Authorities, Shipping Companies) were contacted and asked to share their views on this subject, by means of individual interviews and questionnaires. The input from these various stakeholders was then analyzed and submitted for validation during a workshop.

[16] *Network and Information Security: Proposal for A European Policy Approach COM(2001) 298 final*

1.5.3 Workshop

ENISA organised a validation workshop on 28 September 2011 in Brussels, inviting stakeholders that were identified through the first steps of this study. The workshop aimed at both validating the first outcomes of the literature review and the interviews and at discussing open points and identifying a set of possible recommendations.

A set of keynotes was presented, covering the following subjects:

- The EU Policy on network and information security and Critical Information Infrastructure Protection;
- The SafeSeaNet project;
- The management of public-private partnerships and information sharing for the protection of critical infrastructures; and
- Open issues and proposals in the security management of Ports Information and Telecommunication (PIT) systems.

This set of keynotes was followed by open discussions on four main themes:

- Recommendations on legal initiatives;
- Recommendations for the Member States;
- Identification of the relevant stakeholders in this particular context;
- Identification of the appropriate means needed to address these recommendations.

The outcomes of this workshop were then integrated in this study, either serving as a basis for the key findings it highlights or as a basis for the recommendations provided.

2 Key findings and recommendations

This chapter presents the key findings that were made during this study. These findings are based on both the literature review and the information provided by the stakeholders that were contacted. For each of these findings, a clear description is provided along with the identification of the possible impact and the associated threats. Furthermore, a set of high-level recommendations is indicated in order to appropriately address the issues associated to these findings. A number of interesting initiatives was also identified, which can be considered as inspiration for actions to improve cyber security in the maritime sector. (Please also refer to Appendix B for a summary.)

2.1 Low awareness and focus on maritime cyber security

It was clearly noted that the awareness regarding cyber security aspects is either at a very low level or even non-existent in the maritime sector, this observation being applicable at all layers, including government bodies, port authorities and maritime companies. One of the reasons for this may be the low number of known cyber security incidents incurred within the sector, which did not create sufficient media exposure to trigger specific and bold actions from the involved stakeholders. However, no publicity is made for some incidents, as there are no virtually mechanisms in place in the Member States to consistently identify and/or report cyber security incidents specific within the maritime sector.

This overall low awareness represents a concern as there is an increased dependency on ICT of all key players, processes and activities within the maritime sector. Indicators of this dependency are the increasing number of ICT systems implementations in ports worldwide, and the continuous increase of volume and complexity of information and data exchanged.

2.1.1 Impact

The insufficient awareness and focus on cyber security results in a low sense-of-urgency combined with an inadequate preparedness regarding cyber risks. As a direct consequence, the effects of a potential cyber attack targeting maritime ICT systems could bring even more harm than in other sectors due to the probable poor coordination of the response and due to efficiency issues.

2.1.2 Recommendations

Member States should consider **developing focused awareness raising campaigns** aimed at the key stakeholders within the maritime sector, in order to highlight the importance of adequate protection means against cyber disruptions targeting assets linked to the maritime sector (ships, ports, communication systems, etc.).

ENISA specific guidance could be followed in order to plan, organise and run specific cyber security awareness raising initiatives targeted towards the key stakeholders of the maritime sector. As guidance, the following main steps should be covered by such national **awareness raising campaigns**: plan & assess, execute & manage, evaluate & adjust.

In addition to these awareness campaigns, appropriate **and tailored guidance and training** on relevant specific cyber security aspects should be developed and delivered to the relevant actors of the maritime sector, from ship crews to port authorities. This is expected to increase the overall expertise of the sector with regards cyber security, and it can be successfully applied by using the prior experience accumulated at national level with regards to cyber security awareness raising actions in other sectors – e.g. telecommunications, energy, finance, healthcare, etc.

The implementation of such recommendations would require the identification of budget needs and appropriate stakeholders, the **clear definition of the expected outcomes** from the awareness campaigns and trainings, as well as the application of adequate planning and follow-up in order to measure the results of these initiatives. The stakeholders that would be affected by this recommendation consist of all actors involved in the maritime sector, e.g. policy and regulation makers, port authorities, shipping companies, ship crews etc.

2.2 Complexity of the maritime ICT environment

ICT systems supporting maritime operations, from port management to ship communication, are generally highly complex and employ a variety of ICT technologies that also include very specific elements. The fast technology development and the struggle towards complete automation in the maritime sector have, in cases, reduced the focus on the security features.

One relevant example is the continuously increasing number of port operational ICT infrastructure elements (e.g. SCADA devices) connected to the Internet without due consideration to making them more secure, and even no real need to be connected. The vulnerabilities created by these security gaps of the ICT systems within the maritime sector may affect not only the services supported by these systems, but also the commonly shared infrastructure layers (e.g. databases, systems hosting sensitive information, etc.).

Furthermore, it was noticed that there is inadequate standardisation or development of good practices to ensure that security is appropriately considered in this particular ICT environment. The security baselines considered within the sector do not usually match the ICT complexity or cover all relevant technology aspects.

2.2.1 Impact

The increased dependency towards ICT systems combined with operational complexity and multiple maritime stakeholders involved, make the existing ICT environments particularly vulnerable to cyber attacks, which could result in severe maritime services disruptions. For example, cargo tracking and cargo identification are increasingly subject to cyber security incidents resulting from cyber attacks or system failures. The same applies for the automated systems handling the cargo in ports. Data theft, for criminal purposes, may increase as a direct result of insufficient cyber security measures – or measures not sufficiently matching the complexity of the ICT environment involved.

2.2.2 Recommendations

It would be beneficial for Member States to agree on a common strategy and to establish a specialised workgroup to work on developing a detailed set of cyber security guidance and good practices **for the technology development and implementation of ICT systems in the maritime sector.** This workgroup should include key stakeholders from the authorities within the Member States that have a significant dependency on the maritime sector, but should include also representatives of the major port authorities, shipping companies and relevant maritime infrastructure providers (telecommunication infrastructure, ICT hardware and software, SCADA). This **broad group of international stakeholders** should also involve representatives of the International Maritime Organisation (IMO), the European Maritime Safety Agency, ENISA, as well as the user communities.

Amongst the relevant similar exercises and the related cyber security guidance and good practices prepared by other workgroups and relevant bodies in other sectors, we list the following illustrative examples:

- "SCADA Security Good Practices for Drinking Water Sector" – prepared by TNO Defence, Security and Safety[17] at the request of the Dutch National Cyber Crime Infrastructure (NICC) programme. These have been divided into topics that are the responsibility of the business management team and topics for which the management of the technical process automation is responsible. These Security Good Practices provide the drinking water sector with guidelines for secure SCADA use and are based on international standards, de facto standards and successful security measures applied by other companies with SCADA;
- The work of the Communications, Security, Reliability, and Interoperability Council (CSRIC) appointed by the US Federal Communications Commission – the CSRIC is focused on addressing the Cyber security best practices in the telecommunications industry. Amongst the relevant guidance and good practices[18] prepared by the workgroups of CSRIC – with relevance for a similar workgroup to focus on cyber security aspects in the maritime sector in the EU Member States:
    - WG2A - Cyber Security Best Practices
    - WG6 - Best Practice Implementation
    - WG8 - Internet Service Provider Network Protection Practices
- "SCADA security – advice for CEOs" - paper that has been prepared by the Australian IT Security Expert Advisory Group - ITSEAG[19];

---

[17] *See: http://www.tno.nl*

[18] *See: http://transition.fcc.gov/pshs/advisory/csric/*

[19] *ITSEAG is part of the Trusted Information Sharing Network for critical infrastructure protection (TISN) which enables the owners and operators of critical infrastructure to share information on important issues. It is made up of a number of sector-specific Infrastructure Assurance Advisory Groups (IAAG), several Expert Advisory Groups (EAG), and the Critical Infrastructure Advisory Council (CIAC - which is the peak body of TISN and oversees the IAAGs and the EAGs). One of the expert advisory groups within the TISN framework is the ITSEAG which provides advice to the CIAC and the sector-based IAAGs on IT issues as they relate to critical infrastructure protection. The ITSEAG is made up of academic specialists, vendors, consultants and some*

- The "Process Control Domain Security Requirements for Vendors" – released by the International Instrument Users Association – WIB[20], which outlines a set of specific requirements focusing on cyber security best practices for suppliers of industrial automation and control systems; etc.

The detailed set of guidance and cyber security good practices developed by this specialised workgroup should be aimed at ensuring "security by design" for all critical maritime system components. This strategy and set of good practices should be defined using a risk-based approach in order to encompass the complexity of the maritime ICT environment, and should take stock of the existing standards, policies and good practices that apply for the context of maritime architectures.

Next to this workgroup focused on developing guidance and cyber security good practices for the maritime sector, it is recommended that Member States which have a high dependency on the Maritime sector develop and implement a national-level cyber security plan for the maritime sector. This should be seen as an initial step for governmental action to increase security of the maritime-related ICT key infrastructure. Such plan should address as a minimum the risk management, as well as ICT security design and implementation aspects applicable to the national-level maritime sector infrastructure and operations. It should also take account of the need for cross-border information exchange and cooperation.

2.3 Fragmented maritime governance context

Throughout this study, it was noted that several maritime governance stakeholders relevant for EU Member States spread on multiple levels exist. A clear insufficiency in coordination was observed between these levels regarding cyber security and the risks associated to cyber threats.

2.3.1 Global level

At the global level, the relevant stakeholders include - while not being limited to - various intergovernmental organisations such as the International Maritime Organisation (IMO), the World Customs Organisation (WCO) and the ICC International Maritime Bureau (IMB), which is a specialised division of the International Chamber of Commerce (ICC). Additionally, it is also relevant to mention the relevance of the International Maritime Security Corporation (IMSC) focuses on actions to specifically protect the ships, their crews, and their cargo against a variety of threats.

The lack of coordination between these stakeholders and stakeholders at other levels (European and national) brings major discrepancies in the way maritime security is addressed.

industry association representatives who are leaders in the information technology/e-security field. More information on TISN can be sought from http://www.tisn.gov.au

[20] *The International Instrument Users Association is an international organization that represents global manufacturers in the industrial automation industry.*

2.3.1.1 Impact

The current situation implies a significant risk of inadequate coordination which could lead to inefficiencies such as governance gaps and overlaps. Furthermore, it could bring major discrepancies in the way cyber security issues are addressed from one maritime zone to another, and between governance levels.

2.3.1.2 Recommendations

It is recommended to align international, regional and national policies on maritime cyber security requirements.A platform for further consultation and coordination on maritime cyber security, lead by the European Commission and with the support of the Member States is desirable at this level. This alignment and harmonisation effort would require the collaboration of intergovernmental organisations (e.g. The International Maritime Organisation) with regional and National policy makers. In this respect the governance structure with its different levels should be harmonious to allow appropriate adoption by relevant maritime operators.European level

At the European level, the current fragmentation existing in maritime policies makes it difficult to enforce legal requirements ensuring minimum cyber security protection. Next to this, six agencies are dealing with matters related to the seas[21] while, according to the European Directive on CIP[22], Member States are ultimately responsible for protecting their maritime ICT infrastructure from cyber security attacks.

The European maritime infrastructure also spans across different maritime zones which are subject to diverse laws and regulations.

2.3.1.3 Impact

The fragmentation of European maritime policies brings difficulties for the clear definition of responsibilities and roles to be taken regarding cyber security matters in this sector. As a consequence, it has an immediate impact on the possibility to accurately enforce minimum cyber security protection. As an example, inappropriate coordination and action could be taken in order to address a cyber security incident.

2.3.1.4 Recommendations

It would be recommended for the transport related authorities within Member States to **clearly define the governance roles and responsibilities at the European level** that should be endorsed for addressing maritime cyber security and CIIP matters. Proper coordination and linkage between relevant stakeholders should also be defined. As also at the global level, the

[21] *FRONTEX, European Defence Agency, European Space Defence, European Space Agency, European Maritime Safety Agency, Community Fisheries Control Agency and the European Environment Agency.*

[22] *See Council Directive 2008/114/EC of 08.12.2008*

development of information sharing and coordination platforms could be beneficial at this level.

It is recommended that the inter-agency co-operation agreements of the relevant European agencies[23] dealing with matters related to the maritime sector should include also key elements related to the cyber security. This will facilitate better alignment of maritime sector policy making initiatives and will ensure that the cyber security component is sufficiently considered. As a minimum, specific co-operation agreements should be considered and implemented between: EMSA – FRONTEX – ENISA within the limits of their mandates.

2.3.2 National/Regional level

At the national level, a growing trend of maritime ports (and port infrastructure) privatisation has been observed during the last decade. Currently, major European ports such as the ports of Piraeus, Thessaloniki and Stockholm have at least been partially privatised or given into concession while others – such as the port of Hamburg - are in the process of being privatised.

This privatisation trend raises several justified concerns regarding the security requirements set for ICT implementations and use in ports, as the security baselines and standards put in place may not necessarily depend on the port's country of origin, but rather on the current owner. It additionally brings forwards additional security challenges due to the international dimension, as the actual owners can originate from outside of the EU borders.

Besides this, another key issue concerns the critical ICT components developed and implemented by the large variety of international vendors that provide services and infrastructure to the ports, and to the maritime sector in general. As development and testing cycles are increasingly being managed to lower costs countries (typically outside European Member States), a series of vulnerabilities are left exposed (e.g. missing patches, IT breaches).

2.3.2.1 Impact

As ports become privatised, the ICT and security standards and requirements on which they are run mostly depend on their owner, and on the level of maturity of this owner. This could have a serious impact on the overall security and safety aspects of ports, especially on cyber security, as it could be perceived as a financial burden.

2.3.2.2 Recommendations

Member States should ensure through their agencies and port authorities that adequate maritime cyber security requirements are applied. For a comprehensive approach, there is a clear need for constructive interaction between the government and economic actors. The involved stakeholders should therefore participate in **public-private sector interaction** and dialogue to optimize efforts and priorities to address maritime cyber security.

[23] *See above list of European agencies.*

Appropriate guidance could be defined at the European level through **collaboration between relevant Member States agencies and National port authorities**, in a top-down, risk-based approach. It is recommended to achieve stronger collaboration between policy makers and

2.4 Inadequate consideration of cyber security in maritime regulation

In the current regulatory context for the maritime sector on global, regional and national levels, there is very little consideration given to cyber security elements. Most security related regulation only includes provisions relating to safety and physical security concepts, as can be found in the International Ship and Port Facility Security (ISPS) Code and other relevant maritime security and safety regulations, such as Regulation (EC) No 725/2004 on enhancing ship and port facility security. These regulations do not consider cyber attacks as possible threats of unlawful acts.

2.4.1 Impact

As the existing regulatory frameworks are not optimally used and inadequately defined, it implies a too high dependency on operational stakeholders to identify appropriate courses of action in case of cyber security incidents impacting the maritime sector and its ICT infrastructure. Port authorities, or other relevant stakeholders involved, may therefore face difficulties in appropriately addressing cyber disruptions and cyber attacks, as they are possibly not aware of the existing measures that could be applied (e.g. request the assistance of CERT teams).

2.4.2 Recommendations

Self-regulatory and co-regulatory organisational models around maritime cyber security aspects are virtually non-existent within the EU Member States. Although such models offer good opportunities for direct involvement of the relevant maritime stakeholders, they seem to be inadequate in this particular case. Moreover, a number of EU agencies and other bodies deal with maritime related matters – however, with insufficient focus on cyber security aspects. As such, it is more appropriate that the initiatives for analysing and further deciding on adequate cyber security policy measures and (if needed) on regulations with regard to the maritime sector may need to be addressed by the Member States themselves.

ENISA recommends that Member States take appropriate measures in order to add **considerations and provisions towards cyber security in the national maritime regulatory frameworks**. Actionable points from the Member States should include the following:

- In-depth analysis of the current legislative framework, in order to assess whether legislative updates are necessary to make progress in cyber security – either specifically in the maritime sector, or as part of a broader national cyber security initiatives. As a minimum, the legislative updates should clarify:
    - Identification of the roles, responsibilities and/or authorities of the Member State governments with regards to protecting the ICT elements of the maritime sector against cyber attacks;

- Identification of the roles and responsibilities of the other key stakeholders (public and private) within the maritime sector with regards to the cyber security aspects. The governance mechanism around this should be clearly defined and a pragmatic co-operation and information exchange mechanism should be established among government authorities, other elements of the national cyber security infrastructure and the maritime sector;
- Definition of national and international co-operation mechanisms;
- Adoption of enhanced security standards and practices for the cyber security in the maritime sector. Any such approach must involve international cooperation and heavy engagement with the private sector but should not put the governments in a position to determine the future design and development of the involved technologies.

- The member States should also establish, identify or assign the competent national authority to deal with cyber security aspects as applicable to the maritime sector. In most of the Member States, these competencies are not clearly established. This identified national authority should (as applicable) be the central contact point for national cyber security initiatives within maritime sector.

In this regard, adequate collaboration is recommended between European bodies involved in maritime regulation and national authorities lead by the European Commission by engaging the Member States.

2.5 No holistic approach to maritime cyber risks

Currently, no holistic approach to maritime cyber risks exists. It was observed that maritime stakeholders are setting and managing cyber security expectations and measures in a rather ad hoc manner. Only a part of the actual risks are being considered, such as the disruption of critical telecommunication means or the divulgation of cargo information.

2.5.1 Impact

Existing efforts are only addressing a narrow scope of the maritime cyber risk spectrum. A holistic approach is required to ensure appropriate consideration of all relevant aspects to maritime CIIP. In the current situation, there is a significant risk that potential cyber incident consequences are not comprehensively assessed for the identification of measures needed, resulting in vulnerabilities in the critical maritime information infrastructure.

2.5.2 Recommendations

Member States and international policy makers should consider **a holistic approach, based on sound risk management principles and good practices**, in order to address the subject of maritime cyber security.

From a policy perspective, the effective application of such an approach would require the **assessment of existing cyber risks** associated with the current ICT systems implementations relevant to the European maritime sector as well as the identification of all critical assets

within this sector. This encompasses the assessment of critical maritime services and assets, the threats they face and their risk exposure, in order to determine how to best manage the risk. Compliance requirements and audits of stakeholders could also be considered, along with the implementation of preparedness exercises. A joint effort between maritime ICT providers, maritime operators, port authorities and policy makers is needed in order to clearly map the cyber risks faced by the maritime sector on a higher level.

For maritime economic operators and stakeholders, it is important to **proactively apply sound cyber and information security principles** within their organisations and environments. They should recognize and manage the actual risks they face appropriately in line with their business objectives and the applicable regulatory context.

2.6 Overall lack of direct economic incentives to implement good cyber security in maritime sector

To date, the key stakeholders of the maritime sector still lack the necessary incentives to improve their overall cyber security posture. This results from a combination of fragmented and insufficient regulatory framework that does not address security aspects, from lack of good security baselines and also from a poor option of direct economic incentives to implement good security.

Some relevant stakeholders that may economically stimulate the development of good cyber security practices in the maritime sector are not currently engaged. For instance, the insurance companies that are usually covering financial losses incurred through damage or unavailability of the cargo or passenger maritime traffic do not have any relevant observed role or influence with respect to cyber aspects in the maritime sector within the Member States.

There is no relevant positive benefit on the sector of the cyber-insurance practices promoted by the insurance companies. In this case, we refer to cyber-insurance as to the insurance contracts between insurance companies and maritime sector stakeholders, focused on covering financial losses incurred through damage or unavailability of tangible or intangible assets caused by cyber security related incidents affecting the ICT maritime infrastructure involved.

2.6.1 Impact

Although in other areas, there are economic incentives in place due to cyber-insurance practices, surprisingly these are not very common or evaluated within the maritime sector. As such, this category of incentives does not produce tangible positive effects for stimulating implementation of better security and for further research the cyber security aspects in the maritime sector.

2.6.2 Recommendations

We would recommend Member States to **stimulate dialogue and public-private partnerships** between the key stakeholders in the maritime sector (e.g. shipping companies, port authorities, etc.) and connected stakeholders (e.g. insurance companies / brokers). Such dialogue may incentivise the undertaking of better cyber security measures by eliminating the barrier of the lack of awareness on cyber-risks involved. Moreover, on long-term, this may stimulate the efforts to build or use insurable maritime ICT infrastructure.

From a different perspective, **better information exchange and statistics on cyber security** may help insurers to improve their actuarial models, reduce own risks, and therefore offering better contractual insurance conditions to the involved maritime stakeholders. This is an example on how increased co-operation and better cyber security can increase the economic benefits/incentives of all involved stakeholders, and vice-versa.

2.7 Inspiring initiatives, a call for collaboration

Despite the lack of a holistic and comprehensive approach towards achieving cyber security in the maritime sector, a number of interesting initiatives are being implemented and can be considered as inspiring for further maritime CIIP efforts. These initiatives clearly illustrate the need for collaboration and information exchange between relevant stakeholders in order to share experiences and achieve collaboration. Currently, one may consider this is not taking place sufficiently.

As a first example, the Port ISAC (Information Sharing and Analysis Centre) initiative recently launched by CPNI.NL[24] aims at establishing public-private partnerships to foster information exchange on cyber security within the maritime context. It builds a trust-based network of representatives from the public and private sector and allows a secure exchange of views / experiences on cyber security issues and good practices.

Another example is the development of the S-Port initiative[25] a project aiming at providing a collaborative environment for the security management of the Port Information and Telecommunication systems. This project is currently being developed at the three Greek ports of: Piraeus, Thessaloniki and the Municipal Port Fund Mykonos by a consortium of private companies and by the academic sector.

2.7.1 Results

The outcome of existing inspiring initiatives is currently still not optimized, and is it obvious that the increased efforts in sharing of different stakeholders' views could lead to more effective and/or efficient measures to manage maritime cyber risks.

---

[24] *More information on ISAC can be found at http://www.cpni.nl/informatieknooppunt/werkwijze-isacs*

[25] *http://s-port.unipi.gr/index.php/*

2.7.2 Recommendations

Information exchange platforms, as for instance the ones implemented by CPNI.NL, should be also considered and developed by Member States in order to foster and facilitate communication on cyber security for the relevant maritime actors, at the European level. Such trust-based networks can prove to be critical in helping to identify major and upcoming cyber threats. The **development of ISACs** requires the identification of relevant stakeholders from the public and the private sector and the establishment of a trust relationship with these identified stakeholders.

3 Conclusions & suggested next steps

The analysis of the ongoing initiatives and efforts taken within the Member States with regards to the topic of cyber security in the maritime sector, revealed several trends and commonalities.

A key characteristic identified is that a general insufficient focus on cyber security within the maritime sector exists. As a direct consequence, the overall sectorial capabilities to consistently assess and deal with cyber security challenges, are inherently reduced. One root cause of this situation is linked to insufficient awareness of the key stakeholders involved (e.g. governments, port authorities, shipping companies, telecommunication providers etc.) on the security challenges, vulnerabilities and threats specific to this sector.

The other issues that were identified are a direct consequence of the complexity of the maritime ICT environment and of the governance fragmentation at different levels (international, European and national/regional). Besides the common issues and challenges that are ahead of almost all involved stakeholders, the study highlights a few relevant inspirational cases that were observed in some Member States, such as the Port ISAC initiative in the Netherlands by CPNI.NL and the S-Port project in Greece.

This study highlighted the importance of considering and acting upon the key cyber security aspects in the maritime sector. It also highlighted the need to define appropriate measures in order to achieve the protection of this critical infrastructure sector against cyber threats and depicted the current lack of consideration and awareness towards this particular but raising type of menace.

As a logical conclusion to this study, a brief description is given on a suggested roadmap that could be taken forward by relevant stakeholders with the active engagement of COM and ENISA in order to improve cyber security in the maritime sector at the European level. These next steps are classified short-, mid-, and long-term priorities.

Short-term

1. Stimulate dialogue and information exchange between key stakeholders in the maritime sector and connected stakeholders;
2. Raise awareness about the criticality of this subject, as cyber security is currently not being sufficiently considered within this sector;
3. Develop strategies and good practices defining security requirements for ICT implementations in the maritime sector;

Mid-term

1. Develop appropriate cyber security trainings;
2. Define roles and responsibilities towards cyber security in this sector at European and national levels;

3. Define and implement a holistic, risk-based approach to address the subject of maritime cyber security.
4. Take appropriate measures in order to add considerations towards cyber in regulatory frameworks governing the maritime sector.

Long-term

1. Develop standards and enforce regulations ensuring the achievement of cyber security within the maritime sector;
2. Develop information sharing and analysis centres at national and European level based on the ISAC model;
3. Align and harmonize international and European policies on maritime cyber security requirements;
4. Take appropriate measures in order to add considerations towards cyber security in the existing regulatory frameworks applicable to the maritime sector.

4 APPENDIX A Workshop report

4.1 List of keynote speakers

	Organisation	Role and responsibilities	First Name, Last Name	Function
1.	CPNI (Centre for the Protection of National Information Infrastructure) www.cpni.nl	CPNI facilitates collaboration and provides advice which is targeted primarily at the critical national infrastructure - those key elements of the National Information Infrastructure which are crucial to the continued delivery of essential services to The Netherlands.	Allard Kernkamp	Secretary
2.	European Commission's Directorate General for Mobility and Transport (MOVE) http://ec.europa.eu/transport/index_en.htm	The Directorate General for Mobility and Transport works towards ensuring that the European transport infrastructure meets the needs of European citizens and economy, whilst minimising damage to the environment.	Jean-Bernard Erhardt Jukka Savo	Seconded National Expert Policy Officer
3.	European Commission's Directorate General for Information Society and Media (INFSO) http://ec.europa.eu/dgs/information_society/index_en.htm	The Directorate General for the Information Society and Media supports the use and development of ICT for all European citizens.	Andrea Servida	Deputy Head of Unit
4.	University of Piraeus http://www.unipi.gr	Academic research in maritime cyber security.	Nineta Polemi	Assistant Professor

4.2 Keynote summaries

4.2.1 EU Policy on network and information security and CIIP

The workshop started with a presentation by Andrea Servida, Deputy Head of Unit at the European Commission - Unit on Internet, Network and Information Security. This presentation introduced the EU Policy on network and information security and CIIP, and gave a clear description of its purposes while also describing the required future efforts. It was explained that this policy aims at mitigating IT security risks for Europe, looking at Cyber disruption in a holistic approach, ranging from national security to law enforcement.

It was indicated that an adequate policy should:

- Focus on prevention, resilience and preparedness;
- Take into account the civilian and economic stakeholders' role and capability;
- Make security and resilience the frontline of defence;
- Adopt an all-hazards approach;
- Develop a risk management culture in the EU;
- Focus on the role of socio-economic incentives;
- Promote openness, diversity, interoperability, usability and competition.

This presentation also highlighted the Communication to the Commission of March 31st, 2011 – "CIIP COM 163 (2011), Achievements and next steps: towards global cyber-security", which takes stock of the results achieved since the 2009 CIIP Action Plan and builds on existing policy initiatives.

4.2.2 SafeSeaNet

Mr. Jukka Savo and Mr. Jean-Bernard Erhardt from DG MOVE introduced the SafeSeaNet initiative currently being implemented under the supervision of the European Maritime Safety Agency (EMSA). This initiative consists in a centralised European platform for maritime data exchange, aimed at linking maritime authorities across Europe. It enables Member States, Norway and Iceland to provide and receive information on ships, ship movements, and hazardous freight.

As such, it puts in practice the Directive 2010/65/EU of the European Parliament on Reporting Formalities, which states that the information on cargo and crew/passengers transmitted when ships arrive to European ports must be communicated using electronic forms (e-messages).

The SafeSeaNet platform aims at offering data exchange services to clients, but must do so in a secure way as the information it provides can be considered critical. National single windows are put in place in order to exchange the required data from one country to another, while an interconnection of single windows with e-Customs is also foreseen. The importance of cyber security regarding such systems was clearly stressed by the speakers.

4.2.3 Management of public-private partnerships and information sharing for the protection of critical infrastructures

Mr. Allard Kernkamp from CPNI.NL (Dutch Centre for Protection of the National Infrastructure), provided insights on the Dutch public-private partnerships approach for critical infrastructures. This presentation highlighted the importance of building trust relationships with the private sector in order to have an effective information exchange regarding cyber security incidents, as well as the importance of building awareness towards information and cyber security. It also introduced the newly created Harbour ISAC (Information Sharing and Analysis Centre) and its chairman, Mr. Ruud Jongejan.

4.2.4 Open issues and proposals in the security management of PIT systems – The S-Port national case

As a final presentation, Dr. Nineta Polemi, assistant professor at the University of Piraeus, introduced the audience to a set of identified open issues and recommendations in the context of Ports Information and Telecommunication (PIT) systems. The presentation focused on ports being considered as transport critical infrastructures and being at the centre of the maritime environment.

Two main issues were described:

- The existing maritime security standards, methodologies and tools are monolithic and concentrate solely on physical security;
- Commercial ports are not considered as critical infrastructures and the security of their information and telecommunication systems is not organised.

A set of propositions on how to address these issues was then presented to the audience. An effective protection of all layers of PIT systems may be organised through a combination of IT and CIIP standards, while targeted maritime security management methodologies implementing these standards should be defined. Furthermore, maritime interoperable security management tools should also be developed.

As an illustration to this presentation, an introduction to the S-Port initiative[26] was also given. This initiative is a pilot project currently being developed by a consortium grouping the University of Piraeus, Intracom, the Information Security and Critical Infrastructure Protection Research Group (AUEB/CIS) and mVision. It aims at offering an open-source secure and collaborative environment for the security management of Port Information Systems.

[26] *See also* http://s-port.unipi.gr

4.3 Group discussions

Following the keynotes summarized in the previous section, the workshop proceeded into a number of open discussions on the following topics:

- Recommendations on legal initiatives;
- Recommendations for the Member States;
- Identification of the relevant stakeholders in this particular context;
- Identification of the appropriate means needed to address these recommendations.

The conclusions of these discussions were integrated in this study, in the Key Findings chapter.

5 APPENDIX B Summary of key findings and recommendations

Finding	Recommendations	Time line
Low awareness and focus on maritime cyber security	• Design and launch awareness raising campaigns • Develop appropriate trainings	Short term Mid term
Complexity of the maritime ICT environment	Build strategies and good practices defining security requirements for ICT implementations in the maritime sector.	Short term
Fragmented maritime governance context	• International level: align and harmonize international and European policies on maritime cyber security requirements; • European level: define clear roles and responsibilities for addressing cyber security matters in the maritime sector; • National/regional level: enforce European standards (develop standards and enforce rules in the core text) for ports requirements on ICT systems.	Long term Mid term Long term
Inadequate consideration of cyber security in maritime regulation	Take appropriate measures in order to add considerations towards cyber security in the regulatory frameworks governing the maritime sector.	Mid term
Absence of a holistic approach to maritime cyber risks	Define and implement a holistic, risk-based approach to address the subject of maritime cyber security.	Mid term
Overall lack of direct economic incentives to implement good cyber security in the maritime sector	Stimulate dialogue and information exchange between key stakeholders in the maritime sector and connected stakeholders (e.g. insurance brokers).	Short term
Inspiring initiatives	Establish information exchange platforms based on the ISAC model (trust-based public-private partnerships).	Long term

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu