DIWA Report

Sub-Activity 4.3: Cybersecurity & Privacy

Version: V 0.9 (Final draft report), 22.06.2023

Main author: Project team Masterplan DIWA

Contributing: Generaldirektion Wasserstraßen und Schifffahrt, De Vlaamse Waterweg, via donau – Österreichische Wasserstraßen-Gesellschaft mbH, Voies navigables de France, Rijkswaterstaat

Co-funded by the European Union

Main authors: Mathias Wijffels, ALSIC, BE
Tony Daems, ALSIC, BE

Contributing: Daniel Meerwald, Bundesministerium für Verkehr und digitale Infrastruktur, DE
Jeroen Van Acker, ALSIC, BE
Marie-Claire Schug, Viadonau, AT
Martijn van Hengstum, Rijkswaterstaat, NL
Piet Creemers, De Vlaamse Waterweg, BE
Robert Schwarz, Viadonau, AT
Therry van der Burgt, Rijkswaterstaat, NL
Tony Durinck, De Vlaamse Waterweg, BE

Co-funded by the European Union

Table of content

1 Executive Summary

1.1 Introduction

The transport and logistics sector depends more and more on information for the day-to-day running of business. Information systems are a fundamental part of transport and logistics, and therefore also the inherent cybersecurity threats

The current study provides a **cyber risk and vulnerability assessment** based on the business developments and technological developments as specified in activities 2 and 3, taking into account the requirements of the NIS(2) and GDPR directives. The study defines the effects on the digital transition in the period 2022-2032.
It is the objective to provide **advice on measures for prevention, detection and reaction** to secure the information and measures to be taken to avoid or limit the consequences of cyberattacks on the processes in the transport and logistic chain.

The information and knowledge required for this study was primarily gathered through an extensive desk research and through collection of the input from other DIWA Sub-Activities. Subsequently, a stepwise approach was used to establish an inventory of cyber risks in IWT and to define recommendations and a roadmap on how to address those risks.

The study concludes that the negative side effect of digitalisation is an increased probability and impact of cyber incidents and hence it is important that **organisations need to be prepared to address cyber risks**. Also there are vulnerabilities in certain systems, such as AIS that relies on VHF radio transmissions which can easily be falsified. However, **there are some measures that can be taken** to improve the cybersecurity of these IWT systems. Finally, although there is clearly a growing awareness of cyber risks and their potential business impact, it is key to **keep awareness at a high level and organisations must continuously adapt** their security measures to evolving cyber threats and vulnerabilities.

This study was conducted over a period of 10 months from may 2022 to march 2023. Five fairway authorities participated in the project: via donau (Austria), De Vlaamse Waterweg (Belgium), Voies navigables de France (France), Bundesministerium für Verkehr und digitale Infrastruktur (Germany) and Rijkswaterstaat (The Netherlands).

1.2 Frameworks for cybersecurity

There is an extensive body of existing standards, guidelines and studies available regarding cybersecurity in general, but also more specifically on cybersecurity in the maritime sector. A lot of this well documented knowledge is also largely applicable within IWT. These frameworks provide a structured approach to identifying, assessing, and mitigating cyber risks. They can help the IWT sector develop and implement a comprehensive cybersecurity strategy.

The main standards and regulations that provide guidance in this matter are:

- the EU cybersecurity strategy, a comprehensive cybersecurity strategy that aims to improve the protection of citizens, businesses and critical infrastructure from cyber threats.
- the NIS (Network and Information Systems) Directive, a EU legislation that aims to improve the security of network and information systems across the EU for operators of essential services and for digital service providers.
- the Cyber Resilience Act, a proposed EU legislation which will implement minimum requirements regarding cybersecurity on all devices sold in the EU.

There are multiple organisations (listed in section 6.2 of this report) that play a key role in the definition and implementation of the frameworks aimed at improving cybersecurity at the national and international level.

Finally, there are several frameworks and guidelines related to risk management, business continuity management, and information security management that provide organisations with a comprehensive approach to managing their cybersecurity and allow them to assess, control and monitor the effectiveness of their security controls:

- Risk management frameworks provide a structured approach to identifying, assessing, and mitigating cyber risks. They can help organisations to understand the threats they face and the measures they need to take to protect themselves.
- Business continuity management (BCM) frameworks provide a structured approach to planning, preparing, responding and recovering from disruptive incidents, including cyber incidents.
- Information security management (ISM) frameworks provide a comprehensive approach for protecting information assets and include guidelines for incident management, access controls, cryptography, and physical security.

1.3 Generic measures for cyber resilience

Cyber resilience is the ability of organisations to protect themselves against cyberattacks and to recover from them (quickly) in the event of an attack, Thus resuming normal business operations.

Organisations can achieve or improve their cyber resilience by

- Identifying vulnerabilities and risks
- Protecting the infrastructure, systems, applications, data, etc.
- Detecting cyber threats and attacks
- Responding to cyberattacks
- Recovering from cyberattacks

The security measures organisations can put in place consist of administrative, technical and physical controls. Often a simultaneous application of several security measures is applied in what is called a layered defence approach.

1.4 Cyber risks in IWT

Identification of Cyber Risks in IWT was mainly realised through the reports mentioned in paragraph 1.2 and through the input of other DIWA activities.

Summarised conclusions from other DIWA sub activities show:

- Cybersecurity is valued as a very important element of digitalisation but few specific cybersecurity risks are recognised. This limited and mainly technical coverage of cybersecurity is cause for concern.
- It is recommended to raise awareness of the broader scope (beyond pure technical) of cybersecurity and provide actionable advice to reduce cyber vulnerability of IWT across this broader scope.
- Fairway authority mandate might need to be extended beyond the technical equipment requirements of a vessel to the cyber resilience of the vessel and the vessel operator.

It is noted that within the RIS COMEX project a lot of work was done by privacy related and legal experts to draft the core agreements 1 and 2 (CA1 and CA2) regulating the information exchange between COMEX Partners and the users.
Also, in order to mitigate several cyber risks within EuRIS a lot of actions were taken including the use of scanning functionality (i.e. functionality that scans for the application of recommendations from different security related standards), a high-performance firewall to improve network security, components with a high availability (SLA 99.9% or higher), a modern anti-malware and a best practice central authentication platform.

The cyber risks within IWT that were identified can be grouped in 4 categories (Vessel related risks, infrastructure related risks, information/data platform related risks and RIS technology related) where the key risks are:

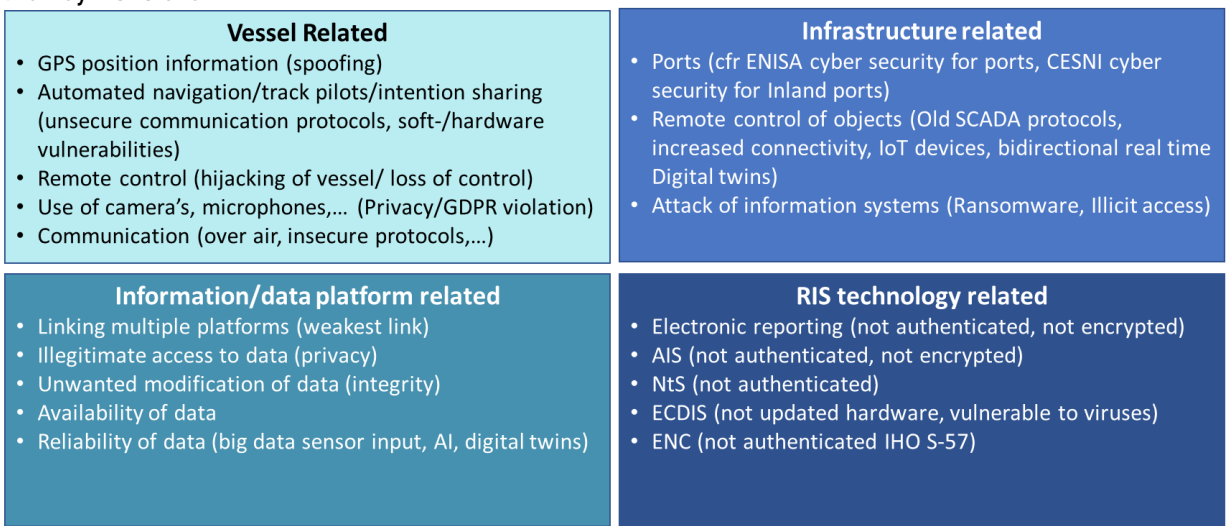


Figure 1: Cyber risks in IWT

1.5 Countermeasures & Recommendations

By applying the known frameworks for cybersecurity and generic measures for cyber resilience on the specific cyber risks in IWT, a set of countermeasures and recommendations is identified. for the in depth discussion of the conclusions, we refer to the recommendations (chapter 11) that provide specific and actionable steps that can be taken to address the issues outlined in the study. They are the tangible outcome of the analysis and research conducted, and serve as a guide for future decision making and implementation.
However, in order to highlight the key findings of this study, the main conclusions for this report can be summarised as follows:

- As digitalisation and the use of more connected systems increase, the surface of attack for cybersecurity risks also increases. On top of that, as the reliance on digital solutions to actively intervene in the system (e.g. in smart shipping) increases, the probability and potential impact of cyber incidents also increases. Hence it is increasingly important that **organisations need to be prepared to address cyber risks**.

- It is noted that IWT is not currently the most cyber resilient transport mode, through vulnerabilities in certain systems, such as AIS. While AIS has been implemented as a safety measure to improve vessel navigation and reduce the risk of collisions, it relies heavily on VHF radio transmissions which are prone to spoofing, which is the act of transmitting false AIS data to deceive other vessels or systems. However, **there are some measures that can be taken** to improve the cybersecurity of these IWT systems.

- Developments such as initiatives by organisations like PIANC and CESNI demonstrate a growing awareness of cybersecurity risks in the transport industry. This is a positive development, but efforts should continue to be made to keep **awareness** at a high level, as it is difficult to maintain this level of awareness over time. Also, cybersecurity is not a goal that can be achieved, but rather an ongoing process. Cyber threats and vulnerabilities are constantly evolving, and **organisations must continuously adapt** their security measures to keep pace.

1.6 Roadmap

In a last step, all recommendations were categorised using a high-level assessment of legal, technical, financial and organisational impact and assigned to a basic, intermediate or advanced scenario. They are grouped according to the risk categories defined above (+ one category covering the common and organisational recommendations), and represented in the roadmap below (Figure 2).

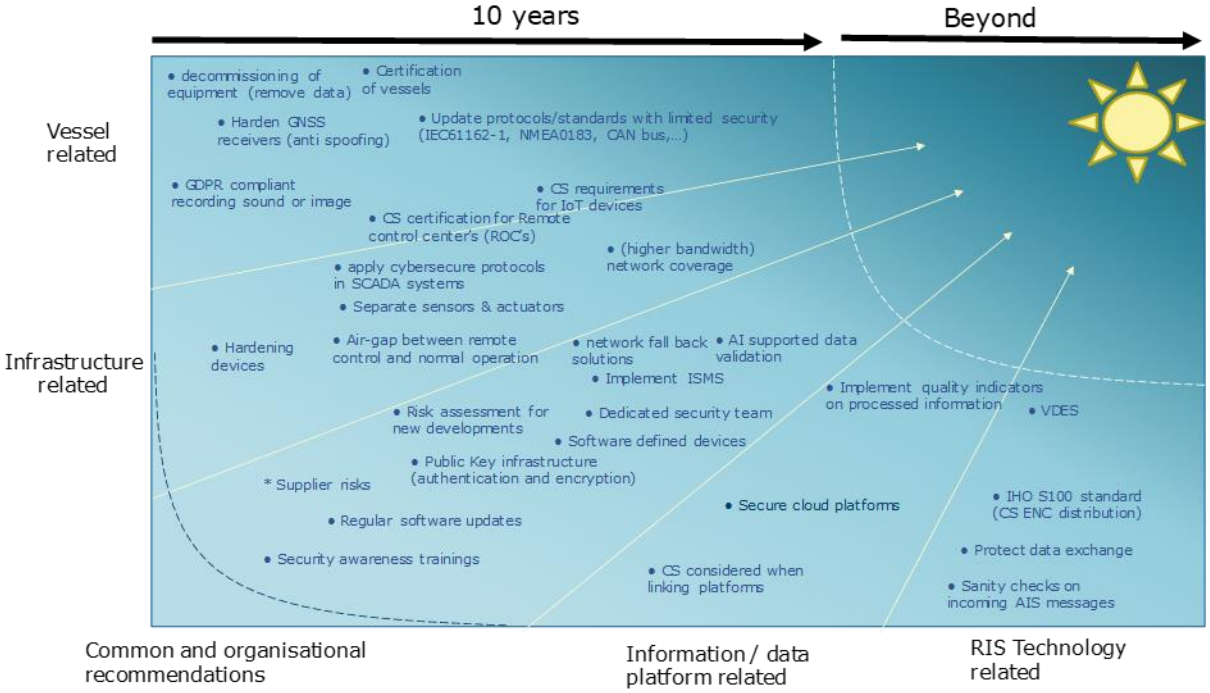


Figure 2: Roadmap for cybersecurity

2 Technical Terms

First, some terms that are often used in connection with cybersecurity will be explained in this chapter.
Abbreviations used in the report, are listed in section 13.1 Glossary.

Cybersecurity

Cybersecurity is a collection of solutions or strategies that are used to avert cyber risks. Various technologies, processes and controls are used to protect networks, programmes, devices and data from cyberattacks.

Cyberattack

Cyberattacks are carried out with malicious intent when a threat actor (individual or organisation) attempts to exploit a vulnerability or weakness in a system or individuals of an organisation.
By gaining unauthorised access to and interfering with systems, networks, programmes or data, the attackers manage to steal, alter or destroy them and thereby gain an advantage/benefit.

Further details on cyberattacks and the different types are discussed in section 7.1

Figure 3: Cybersecurity cycle

Cyber defence

Cybersecurity and cyber defence are often used as synonyms. Yet cyber defence is a component of cybersecurity strategies. Cyber defence refers to actions in the cyber domain that serve to support the goals set in relation to cybersecurity. The focus of cyber defence is therefore on identifying, detecting, targeting and defending against attackers/cyberattacks.

Cyber resilience

Cyber resilience is the ability of an organisation to withstand or recover quickly from cyber events that disrupt normal business operations.
Further details on cyber resilience can be found in chapter 7.2.

3 Introduction

3.1 Position of Cybersecurity and Privacy in IWT

The transport and logistics sector depends more and more on information for the day-to-day running of their businesses. Information systems are a fundamental part of transport and logistics. Digital vulnerability and rapid technological advancement are more and more the top concerns in the transport chain. Preparedness and planning of measures for a potential threat are essential.
The EU Directive on the Security of Network and Information Systems (NIS) was implemented in 2018 and it places obligations on organisations to secure the technology, data, systems and networks used to provide essential services and report incidents that affect them. NIS aims to ensure that operators in e.g. the transport domain are prepared to deal with the increasing numbers of cyber threats, as it requires them to take steps to protect against threats affecting IT systems such as power outages, hardware failures and environmental hazards as well as cyber breaches which create chaos when systems stop working regardless of whether there is a personal data element to the attack.
There is a strong relation between the NIS directive and the EU General Data Protection Regulation (GDPR). The GDPR standardises the rules for the processing of personal data by private companies and public authorities throughout the European Union. The aim is not only to guarantee the protection of personal data within the European Union, but also to ensure the free movement of data within the European internal market. The GDPR replaces the Data Protection Directive 95/46/EC.

3.2 Objective of the report

The study in Sub-Activity 4.3 aims to make a **cyber risk and vulnerability assessment** based on the business developments and technological developments as specified in activities 2 and 3 and taking into account the NIS and GDPR directive and define the effects on the digital transition in the period 2022-2032.
The risk and vulnerability assessment will include data privacy.

The study, together with the risk and vulnerability assessment, has to lead to an **advice on measures for prevention, detection and reaction** to secure the information and technical measures to be taken to avoid or limit the consequences of cyberattacks on the processes in the transport and logistic chain. This includes:

- What measures should be taken to prevent cyber incidents?
- What measures should be taken in order to continue business in the event of loss of information or service functionality?
- What steps should be taken to detect/identify a security attack?
- What measures should be taken to recover information and vital systems immediately when the disastrous event has occurred?

Based on the cyber risk and vulnerability assessment developed in this Sub-Activity 4.3 aims to identify proposals for **measures to be taken in relation to the developments in the Masterplan Digitalisation of Inland Waterways**.

3.3 Scope of activities covered in the report

To achieve these goals Sub-Activity 4.3 looks at the different elements in the IWT ecosystem and their interactions as depicted in the IWT Fairway and navigation system interconnection architecture (Figure 4) from a cybersecurity and privacy perspective.

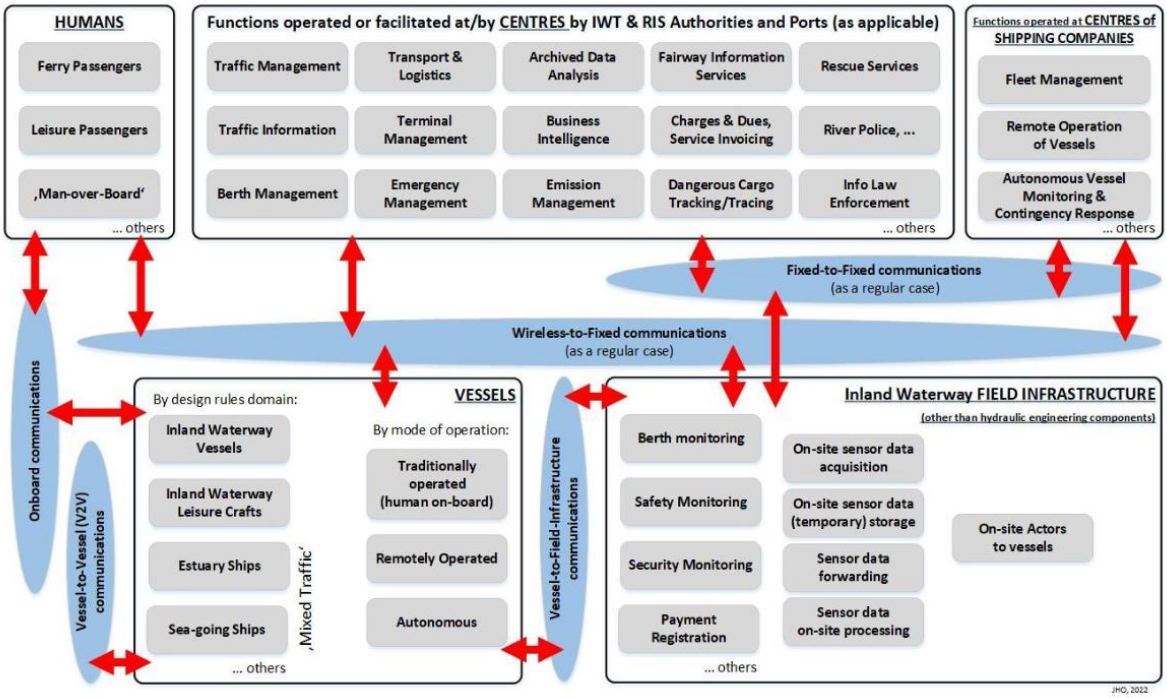


Figure 4: IWT Fairway & Navigation System Interconnection Architecture (DIWA Masterplan SuAc 3.5 – Technologies in other transport modes)

4 Work approach

4.1 Interdependencies with other (Sub-)Activities

DIWA activity 4 (Facilitators) as a whole, and Sub-Activity 4.3 (Cybersecurity) in particular cover transverse prerequisites that have a strong impact on the realisation of developments described in activity 2 (Business developments) and 3 (Technological developments). Cybersecurity can indeed act both as a possible stimulator and restriction for the development of specific business and technological developments related to navigation, traffic, transport and logistics. The defined services from activity 2, using the technological developments from activity 3, need to be designed taking into account privacy and cybersecurity. Sub-Activity 4.3 is hence an important input and condition for the development of the DIWA masterplan for Inland Waterways in 2022-2032 (activity 5).

The current report builds strongly on the output of activities 2 and 3, wherein multiple cybersecurity and privacy related items have been identified. These have been investigated in Sub-Activity 4.3. The aim of the current report is to provide the relevant insights and recommendations on cybersecurity and privacy.

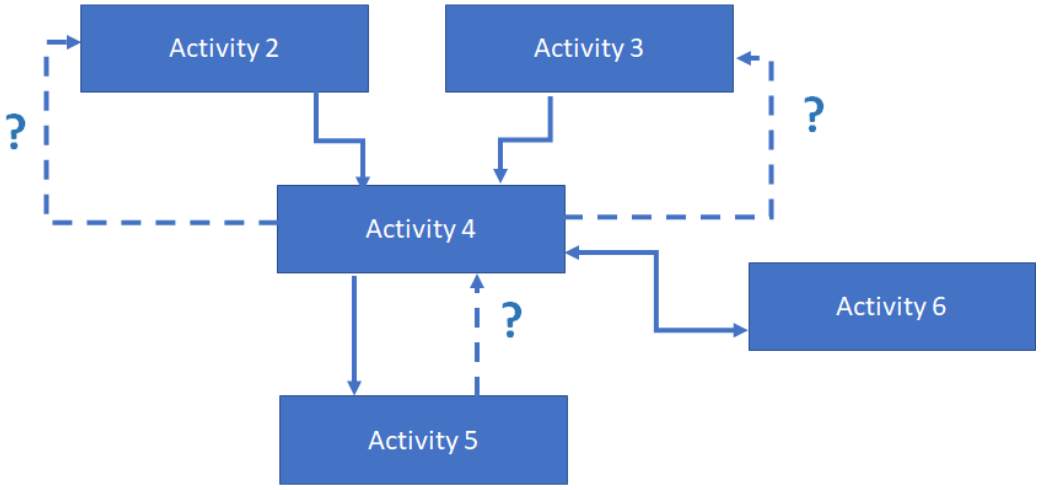


Figure 5: interdependencies of DIWA activities

Within activity 4 (Facilitators), a strong interdependency can be noted between Sub-Activities 4.3 and 4.2 (Rules and Regulations), as there are important regulatory initiatives impacting both cybersecurity and privacy, in particular the General Data Protection Regulation (GDPR) and the introduction of a European Cyber Resilience Directive.

4.2 Timeline

This study was conducted over a period of 10 months from May 2022 to March 2023. Five fairway authorities participated in the project: viadonau (Austria), De Vlaamse Waterweg (Belgium), Voies navigables de France (France), Bundesministerium für Verkehr und digitale Infrastruktur (Germany) and Rijkswaterstaat (The Netherlands).

This report was drafted during several meetings with the members of this Sub-Activity. In a Kick-off meeting the scope and expectations, the overall methodology and task division were discussed. Subsequently a phase of desk research was launched to investigate input from activities 2 and 3, from guidelines and standards, from industry reports and from the prior COMEX and EuRIS projects.
The results of this Desk Research were presented to and discussed in the workgroup. A mind map was developed identifying the most relevant topics for the Sub-Activity and resulting in a common view for a first table of content containing placeholders for topics that should be further elaborated or written down in a structured way. In several meetings the feedback of the desktop research was progressively integrated in the report.

Besides a description of general frameworks for cybersecurity, information security management and cyber resilience, the workgroup developed in a further stage an inventory of IWT specific cyber risks. In the subsequent stages a set of expedient countermeasures for the IWT cyber risks was defined and a gap analysis of the current performed. This eventually led to the definition of a set of substantiated recommendations for the DIWA Roadmap.

During the life cycle of this Sub-Activity there were also meetings with a limited audience, which allowed a deep-dive into several topics.

5 Methodology

This chapter describes the principles, procedures, and techniques that are used in the current study on cybersecurity. It includes the methods used to collect and analyse information, as well as the process used to establish a set of recommendations and a roadmap.

The information was primarily gathered through extensive desk research and through collection of the input from other DIWA Sub-Activities,

Subsequently a stepwise approach was used to establish an inventory of cyber risks in IWT and to define recommendations and a roadmap on how to address those risks.

5.1 Desk Research

In order to provide a basis for recommendations regarding cybersecurity in IWT, desktop research was carried out along several lines with the aim of establishing an overview of the cyber vulnerabilities, issues, best practices and activities in IWT.
There is an extensive body of existing standards, guidelines and studies available regarding cybersecurity in general, but also more specifically on cybersecurity in the maritime sector. A lot of this well documented knowledge is also largely applicable within IWT.

Chapter 6 (Frameworks for Cybersecurity) therefore not only intends to summarise the results of the desk research that was performed, but also to provide reference to the relevant reports and organisations where further information can be found that is relevant for cybersecurity in IWT. It comprises an overview of

- Applicable European directives & strategies on cybersecurity
- International organisations that provide relevant information on cybersecurity
- Risk management
- Business Continuity Management
- Privacy
- Information Security Management

5.2 Input from other DIWA activities

The second main source of information for the current study are the DIWA activity 2 (Business developments) and DIWA activity 3 (Technological developments) reports. In these activities, several references are made to cyber risks and the need for cybersecurity. These have been collected in section 8.2.1 (Input from other DIWA Activities) and indicate the (future) cyber threats that should be addressed within the DIWA masterplan.

5.3 From inventory to roadmap

A stepwise approach was used to obtain recommendations and a roadmap:

First a generic cyber resilience approach is described in chapter 7 (

Measures against cyberattacks/ for cyber resilience). This chapter introduces the types of cyberattacks, a general approach on cyber resilience and a description of recommended security measures.

This generic approach is then applied to the specific cyber risks in IWT: In chapter 8 an inventory of IWT specific cybersecurity risks is derived from input of the other DIWA activities, CESNI and PIANC reports and input from COMEX and EuRIS. In chapter 9 a set of specific desired countermeasures which can mitigate the cybersecurity risks in IWT is identified.
The conclusions (chapter 10) and recommendations (chapter 11) from this study were then identified as remedies to plug the gap between real and desired countermeasures. Finally, in chapter 0 a roadmap was defined based on priority and feasibility of the recommendations.

6 Frameworks for Cybersecurity

The current chapter collects and summarizes existing frameworks that are relevant for cybersecurity. It contains a set of standards & regulations, different risk management guidelines, and an introduction to business continuity management and information security management. The desktop research on these topics is used to gather background information on Cybersecurity and to identify relevant frameworks. It serves not only as a body of knowledge on cybersecurity but also provides reference to useful information which is published by other parties.

6.1 Standards & regulations

6.1.1 The EU Cybersecurity strategy for the digital decade

The EU cybersecurity strategy for the digital decade is a high level document which gives orientation, boundaries and the path that the EU parliament wants to follow concerning Cybersecurity

Quoting the official EU site[1]:

> *The new strategy aims to ensure a global and open Internet with strong safeguards where there are risks to security and the fundamental rights of people in Europe. Following the progress achieved under the previous strategies, it contains concrete proposals for deploying three principal instruments. These three instruments are regulatory, investment and policy initiatives. They will address three areas of EU action:*
> **Resilience, technological sovereignty and leadership;*
> **Operational capacity to prevent, deter and respond;*
> **Cooperation to advance a global and open cyberspace.*
> *The EU is committed to supporting this strategy through an unprecedented level of investment in the EU's digital transition over the next seven years. This would quadruple previous levels of investment. It demonstrates the EU's commitment to its new technological and industrial policy and the recovery agenda.*

The three cornerstones of the EU's cybersecurity strategy are:

1. Boosting Security: The EU's strategy for boosting security in cyberspace includes several key elements
   Resilient infrastructure and critical services: The EU has implemented the NIS (Network and Information Systems) and NIS2 (Network and Information Systems 2) directives to ensure that member states have in place appropriate measures to manage the risks posed to network and information systems that provide essential services, such as energy, transport, and healthcare.
   Building a European Cyber Shield: The EU is building a European Cyber Shield, which includes the establishment of Information Sharing and Analysis Centres (ISACs), Computer Security Incident Response Teams (CIRTs), and Security Operations Centres (SOCs) to share information and coordinate responses to cyber threats.
   Ultra-secure communication infrastructure: The EU is working to develop a secure Quantum communication infrastructure (QCI) and ultra-secure forms of encryption to enhance the security of its networks. It is also utilising existing fibre network and space satellites (GOVSATCOM) as well as emerging technologies such as Quantum, 5G, AI, and Edge computing to improve connectivity while maintaining cost-effectiveness.
   Internet of SECURE things: The EU is setting cybersecurity rules for manufacturers that include continuous security updates and general product safety rules.
   Greater global internet security: The EU is promoting the use of its DNS4EU (European DNS resolver service) and is encouraging the adoption of key internet standards and well-established internet security standards to improve internet security globally.

[1] European Commission (2022): https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

Invest in technology, research, and skilled people: The EU is investing in research and development, and in the development of the necessary skills and expertise to improve the security of its networks and infrastructure.

Figure 6: EU cybersecurity strategy for the digital decade[2]

[2] European Commission (2020), https://data.europa.eu/doi/10.2759/646087

2. Strengthening collective capabilities to respond to major cyberattacks: The EU aims to develop a Joint Cyber Crime unit, to tackle cybercrime and create an EU cyber diplomacy toolbox.

3. Advancing a global and open Cyberspace: The EU aims to step up on international standardisation, develop an EU position on the application of international law in cyberspace, and protect and promote human rights and fundamental freedoms in cyberspace.

6.1.2 NIS 1 & 2

The NIS Directive, which is an EU legislation, stands for Network and Information Systems Directive and its objective is to enhance the level of security of network and information systems across the EU by setting out measures to be taken by operators of essential services and digital service providers.

The NIS Directives are there for boosting cybersecurity which is the first cornerstone of the EU Cybersecurity strategy for the digital decade.

The main objectives of the NIS directives are:

- Security requirements will be strengthened with a list of focused measures,
- The cybersecurity of the supply chain of key information and communication technologies will be strengthened,
- Management responsibility for compliance with cybersecurity risk management measures,
- Streamlined incident reporting obligations with more precise provision.

Although NIS primarily concerns cybersecurity measures, it also covers physical and environmental factors.
NIS applies to two groups of organisations: 'operators of essential services' (OES) and 'relevant digital service providers' (RDSPs).

NIS 1 came in to force in 2016. For NIS2 the co-legislators reached a provisional agreement on the text on 13 May 2022. The text now needs to be adopted formally by both institutions, with the Parliament due to vote on it in plenary in the coming months. It is to be noted that NIS 1 and 2 are directives that have to be adapted into the legislation of the member states.

Difference between NIS 1 and NIS2: NIS 2 is a proposal to adapt NIS to the current needs and make it future-proof. The NIS 2 proposal expands the scope of the current NIS Directive by **adding** new sectors, **eliminating** the distinction between operators of essential services and digital service providers and by **imposing** a risk management approach.

Important note about NIS2:

- Includes waterway transport and other transport services in its objectives
- Gives instruction in incident notification for waterway and other transport services

6.1.3 Cyber Resilience Act

The Cyber Resilience Act (CRA)[3] is a proposal of a regulation for the European parliament and of the Council on horizontal cybersecurity requirements for products with digital elements. In short it requires manufacturers:

- to take cybersecurity into account in planning, design, development, production, delivery and maintenance phase;
- to document all cybersecurity risks;
- to report actively exploited vulnerabilities and incidents;

[3] European Commission (2022) https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

- Once sold, to ensure that for the expected product lifetime or for a period of five years (whichever is the shorter), vulnerabilities are handled effectively;
- to provide clear and understandable instructions for the use of products with digital elements;
- to make security updates available for at least five years;

In order to be able to sell or distribute products in the EU.

It also requires member states to designate notifying and market surveillance authorities.
CRA covers all products with digital elements whose intended and reasonably foreseeable use includes direct or indirect logical or physical data connection to a device or network. Products already covered by other EU regulations (e.g. civil aviation safety) are excluded. If a product conforms to harmonised standards published in the Official Journal of the European Union or a EU statement of conformity has been issued under a European cybersecurity certification scheme (as per regulation (EU) 2019/881) it shall be presumed to be in conformity with the essential requirements.
Products are divided in non-critical products (e.g. smart speakers) and critical products of class 1 (lower risk; e.g. Industrial Internet of Things not covered by class 2) and 2 (higher risk; e.g. Industrial Internet of Things intended for essential entities listed in NIS2 annex I). The critical products will be subject to conformity assessments, requiring class 2 products to undergo a third-party assessment.

Examples of security requirements that will be assessed[4]:
Products with digital elements shall:

- be delivered with a secure by default configuration, including the possibility to reset the product to its original state;
- ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;
- protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms;
- protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;
- protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;

Although the regulation will take some time to enter into force and exact implications are not clear yet, some preliminary conclusions can be drawn:

- Products will become safer to use (more cyber resilient);
- Products will become more expensive;
- (Semi-)Autonomous vessels will most likely need to use class 2 products (requiring third party assessment);
- Fairway authorities and ports will need to use class 2 products (because they are among the essential entities mentioned in the NIS 2 Annex I[5]);
- IWT companies will need to use class 2 products, however the NIS 2 annex containing the essential entities states that although "Inland, sea and coastal passenger and freight water transport companies, referred to for maritime transport in Annex I to Regulation (EC) No 725/2004 (11)" are essential entities, **"the individual vessels operated by those companies"** are not included.

The latter could lead to the situation that connected loading equipment putting dangerous goods onto a vessel needs to comply with class 2 requirements while (connected equipment on) the vessel itself at most needs to comply with (lesser) class 1 requirements.
Of special interest for IWT is AIS which, due to the nature of the technology, cannot comply with the encryption requirement for transmitted data in transit.
Exemptions for AIS (in addition to vessels operated by companies being exempted from class 2 requirements) may be needed to prevent incompatibilities between the installed base of products and

[4] Full list available in Annex 1 of the regulation.
[5] European commission (2023), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0823&from=EN

products on vessels from outside the EU but sailing on EU waters on the one hand and the new products which are subject to the CRA on the other hand.

It would however be prudent to exercise restraint when exempting products with digital elements on vessels from the CRA. Impeding the operation of a cooperative system (AIS) which is meant to improve navigation safety in favour of a stronger cyber resilience is clearly undesirable. However, care must be taken to avoid IWT becoming known as the least cyber resilient transport modality available.

6.2 Organisations

There are a lot of organisations in the private and public sector handling Cybersecurity.
In this chapter a selection of important organisations for our sector are mentioned

6.2.1 ENISA

ENISA (European Union Agency for Cybersecurity) is the agency responsible for the cybersecurity of the European Union. It was established in 2004 to promote the development of a secure and resilient information society by increasing the level of security of networks and services in the EU.

The EU Cybersecurity Act, which came into force in 2019, gave ENISA a new mandate and increased resources to help EU member states improve their cybersecurity.

Quoting ENISA[6]

> *This Act strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services.*
> *ENISA will have a key role in setting up and maintaining the European cybersecurity certification framework by preparing the technical ground for specific certification schemes. It will be in charge of informing the public on the certification schemes and the issued certificates through a dedicated website.*
> *ENISA is mandated to increase operational cooperation at EU level, helping EU Member States who wish to request it to handle their cybersecurity incidents, and supporting the coordination of the EU in case of large-scale crossborder cyberattacks and crises.*
> *This task builds on ENISA's role as secretariat of the national Computer Security Incidents Response Teams (CSIRTs) Network, established by the Directive on security of network and information systems (NIS Directive).*

ENISA's role in the maritime sector includes:

- Addressing key issues and recommendations: ENISA monitors the cyber threats facing the maritime sector, analyses the cybersecurity risks, and provides recommendations for addressing them.
- Supporting the development and implementation of the relevant policy and regulatory framework: ENISA provides support to the EU and member states in the development and implementation of the regulatory framework for maritime cybersecurity, such as the EU Cybersecurity Act and the EU Cybersecurity Strategy.
- Facilitating information sharing and the exchange of good practices between maritime stakeholders: ENISA facilitates the exchange of information and good practices among maritime stakeholders, including shipping companies, ports, shipbuilders, and maritime service providers, to improve the resilience of the sector to cyber threats.

[6] Enisa (2022), https://www.enisa.europa.eu/

- Conducting awareness raising activities and organising physical and virtual events: ENISA conducts awareness-raising activities and organises events, such as workshops and webinars, to increase awareness of cyber threats facing the maritime sector and to promote the sharing of best practices.

- Promoting discussions and validating activities through the maritime work stream in TRANSSEC: ENISA participates in the Transport Security Coordination Group (TRANSSEC) which promotes discussions among stakeholders, validates activities and supports the development and implementation of policies and regulatory framework for the transportation sector, including the maritime sector.

Overall, ENISA's goal is to contribute to the establishment of a secure and resilient digital environment for the EU maritime sector, enabling it to better resist, detect, respond to and recover from cyber-threats and incidents.

6.2.2 TRANSSEC Expert Group

The 'Transport Resilience and Security Expert Group' is **an information exchange platform** that brings together experts to ensure security and resilience of the Transport sector in Europe.

Transsec aims at gathering experts from the Transport sector to exchange viewpoints and ideas on cybersecurity threats, challenges and solutions. It is the intent of ENISA for this group to produce specialised work streams focusing on specific sub-sectors of transport, namely (air, rail &water)

The role of experts participating in TRANSSEC:

- To contribute to relevant position and policy papers on security topics in Transport;
- To exchange knowledge with other participants and ensure the convergence of current and future cybersecurity efforts;
- To participate with priority in related workshops organised by ENISA or other important stakeholders of the community;
- Discuss other on the approaches taken towards protecting Transport infrastructures and services (policy, good practices, standardisation …)

6.2.3 CSIRTs/CERT-EU

A Computer Security Incident Response Team (CSIRT) is a team charged with incident response, handling all security incidents affecting an organisation in a timely manner, as depicted in Figure 7.

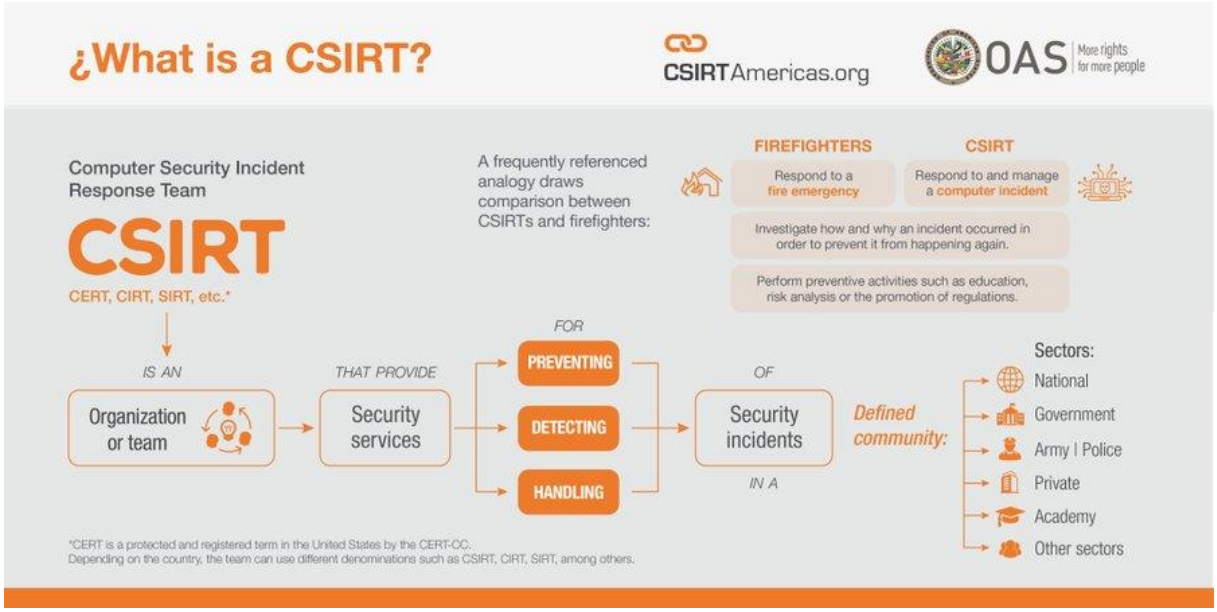


Figure 7 Definition of a Computer Security Incident Response Team (CSIRT)[7]

The Computer Response Team for the EU (CERT-EU) provides services spanning prevention, detection, response and cyber threat intelligence to EU institutions, bodies and agencies.

The NIS Directive in Article 12 establishes the CSIRTs Network[8]

Quoting NIS

> *"to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation".*

The CSIRTs Network is a network composed of EU Member States' appointed CSIRTs and CERT-EU ("CSIRTs Network members"). The European Commission participates in the network as an observer. ENISA is tasked to actively support the CSIRTs cooperation, provide the secretariat and active support for incident coordination upon request.
The CSIRTs Network provides a forum where members can cooperate, exchange information and build trust. Members will be able to improve the handling of crossborder incidents and even discuss how to respond in a coordinated manner to specific incidents.

6.2.4 ISACs

Information Sharing and Analysis Centres (ISACs) are organisations that serve as a central point for the collection, analysis, and dissemination of threat intelligence and incident response information to their respective industries or sectors. The goal of ISACs is to improve the cybersecurity of the industries they serve by providing actionable and relevant cybersecurity information to members, enabling them to better protect their networks and systems.

ISACs typically have members from different companies within the same sector, and they operate on a non-profit basis. They are typically operated by the industry or sector, but can also be operated by government or a third party and are coordinated by the EU through ENISA and the European Cybersecurity Certification Framework.

ISACs typically provide a range of services to their members, including:

- Sharing threat intelligence and information on cyber threats, vulnerabilities and incidents

[7] OEA_Cyber/OAS(2022), https://twitter.com/OEA_Cyber
[8] Enisa (2022), https://csirtsnetwork.eu/

- Providing guidance on best practices for incident response
- Coordinating incident response activities
- Conducting threat assessments
- Offering training and educational resources
- Promoting research and development in the area of cybersecurity

ISACs are an important tool for organisations to gain insights about cyber threats and improve their cyber resilience.

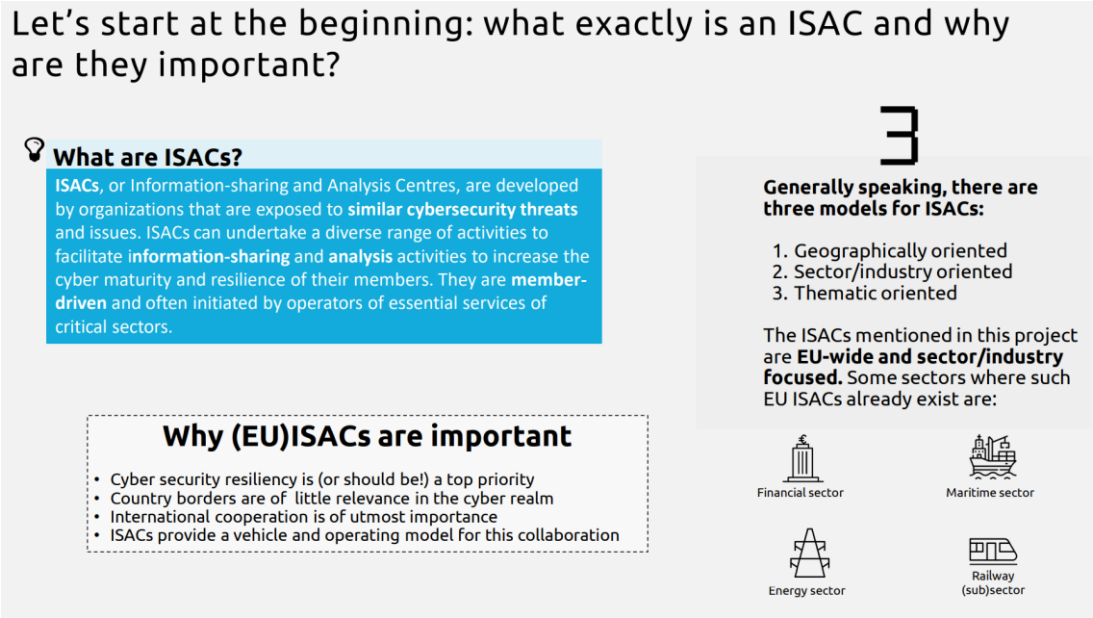


Figure 8: Description of Information Sharing and Analysis Centres[9]

6.2.5 IMO

The International Maritime Organization (IMO)[10] is a specialised agency of the United Nations that is responsible for the regulation of shipping. The IMO's main functions include setting international maritime standards, promoting cooperation among member states, and providing technical assistance to developing countries.

The IMO has issued **guidelines on maritime cyber risk management**[11], recognising the importance of cybersecurity in the maritime sector. These guidelines aim to provide a framework for the management of cybersecurity risks in ships and port facilities, and are intended to help ship owners and operators, port operators, and other stakeholders in the maritime sector to identify and manage cyber risks effectively. The guidelines focus on the management of cyber risks and the protection of maritime systems and assets against cyber threats, providing recommendations on cybersecurity best practices, such as incident management, security management and risk assessment.

6.2.6 EC3

[9] Empowering information Sharing Analysis Centres (2022): introduction to isacs www.isacs.eu
[10] International Maritime Organisation (2023), https://www.imo.org/
[11] International Maritime Organisation (2022), https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ANNEX%20Guidelines%20on%20Cyber%20Security%20Onboard%20Ships%20v.4.pdf

EC3 (European Cybercrime Centre)[12] is a centre within Europol, the European Union's law enforcement agency, that focuses on **fighting cybercrime** in the EU. The EC3 was established in 2013 to strengthen the law enforcement response to cybercrime and to help member states effectively investigate and prosecute cybercriminals.

Whereas EC3 is an important actor in the field of Cybersecurity, they have no actions that are specifically geared toward IWT. EC3 is therefore added here primarily to complete the overview of organisations.

6.2.7 CCNR

The Central Commission for the Navigation of the Rhine (CCNR) is an international organization that manages and regulates navigation and shipping on the Rhine river, which flows through several European countries.

In 2019 an international workshop with presentation and round tables on cybersecurity in inland navigation[13] was held in Bonn, under the auspices of the CCNR and in partnership with the German Federal Ministry of Transport and Digital Infrastructure (BMVI) and the World Association for Waterborne Transport Infrastructure (PIANC). This demonstrated to over 100 participants, from both public and private organisations, the need for all players in the waterway sector to address the complexity of challenges on the topic of cybersecurity to succeed in the digital transition of inland navigation.

As a follow-up of this workshop, the CCNR has organised regular meetings of cybersecurity specialists and non-specialists to exchange information on cyber attacks, their detection, prevention, and response. The objective of this initiative is to improve cyber resilience of the Rhine corridor, with better coordination and better flow of information between IWT authorities and their IT services.

6.2.8 CYBER-MAR (Project)

CYBER-MAR[14] (full title "Cyber preparedness actions for a holistic approach and awareness raising in the Maritime logistics supply chain") is a project aimed at promoting **cyber preparedness in the maritime logistics** supply chain. The project is being undertaken by a consortium of 13 partners from 8 European countries, comprising of members from the research, academic, and industry sectors. The project was conducted from September 1, 2019 to August 31, 2022.

The project is developing a Cyber-MAR platform that utilises data from CSIRTs (Computer Emergency Response Teams) and CERTs (Computer Emergency Readiness Teams) to provide a knowledge-based decision support tool and risk analysis capabilities.

6.2.9 National organisations

The previous sections describe international European organisations (and one project) that are important for IWT cybersecurity.
Within each country there also different public and private organisations for cybersecurity which should be looked at. They coexist and ideally should all work together to protect against cyber threats. For example think about the NIS directive which has to be adapted into the national legislation,.

[12] Europol (2022), https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[13] CCNR (2019), https://www.ccr-zkr.org/13020152-en.html
[14] Cyber-MAR (2022), https://www.cyber-mar.eu/

6.3 Risk Management guidelines

This section describes a set of guidelines developed to set up risk management whereby some are sector agnostic whereas others are specifically tailored towards shipping or ports. In addition a detailed description on the risk management process can be found in section 6.6.3

6.3.1 Guidelines for Cyber Risk management for Ports[15] (ENISA)

6.3.1.1 Content:

This report aims to provide port operators with good practices for cyber risk assessment that they can adapt to whatever risk assessment methodology they follow. In order to achieve this, this report introduces a four-phase approach to cyber risk management for port operators, which follows common risk management principles and is mapped to the steps of the risk assessment methodology that is laid out in the ISPS Code and relevant EU legislation for Port and Port Facility Security Identify cyber-related assets and services in a systematic way that includes maintaining an asset inventory, identifying dependencies and deploying automation.

The four-phases introduced are:

- Adopt a comprehensive approach for identifying and evaluating cyber risks that includes CTI, risk indicators and business impact analysis, involves all relevant stakeholders and is integrated at an organizational level;
- Prioritize the implementation of security measures following a risk-based approach that considers security measure effectiveness and pertinence to the identified risks, and is founded in a security-by-design approach;
- Implement organisation-wide cybersecurity awareness and technical training programs;
- Develop a comprehensive cybersecurity program that involves a commitment by senior management;
- Conduct a cybersecurity maturity self-assessment to identify priorities for improvement, and budget and resource allocation.

For each of these phases, this report provides actionable guidelines to assist port operators in their efforts, lists common challenges associated with the performance of the relevant activities, good practices that can be readily adopted and customised by individual organisations and a mapping of the listed good practices for each phase with the respective challenges they address. The proposed guidelines and good practices may be adapted to any common cyber risk management methodology and can be tailored to the unique characteristics of port operators of different sizes, cybersecurity maturity, information security budgets and operational scope. Phase four of this approach also introduces a model for port operators to perform cybersecurity maturity self-assessment founded on the selected security measures and to identify priorities for investing resources for either improving on or building an organisational cybersecurity maturity program.

6.3.1.2 Method:

The ENISA Guideline for Cyber Risk management for Ports uses a 4 phase approach to cyber risk management depicted in Figure 9:

[15] Enisa (2022), https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports

Figure 9: 4 phased approach to Cyber Risk Management (source: ENISA guidelines on cyber risk management for ports)

For each phase the guideline has 3 main parts:

- Actionable guidelines to assist port operators in their efforts to perform each phase. These include specific guidance in how to effectively apply the various taxonomies presented in ENISA's Port Cybersecurity report of 201912 .
- Related challenges associated with the performance of activities as reported by port stakeholders who were interviewed/surveyed for this report.
- Good practices that can be readily adopted and customised by individual organisations and easily tailored and integrated into any risk assessment methodology utilised by port operators

For each phase an overview is created in a map or table, as a example the used representation of the identified topics of phase 1:

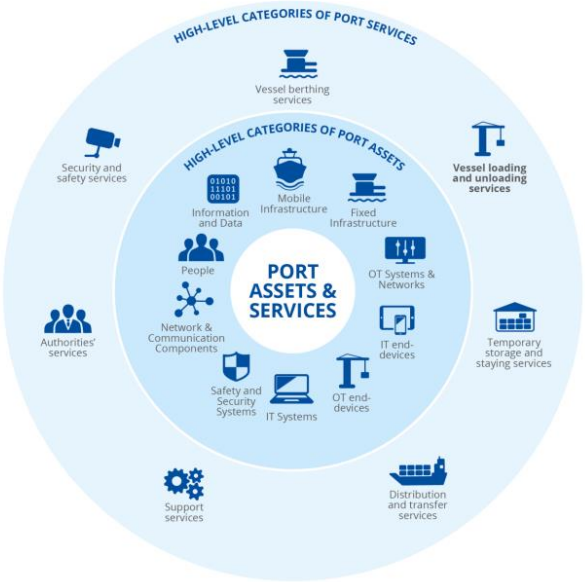


Figure 10: High-level categories of port assets and services (source: ENISA guidelines on cyber risk management for ports)

A similar representation is used in cyber related risks.

For identifying security measures a simple table is used to represent the different domains, there security measures, assets and threats.

For mapping the organizational challenges against the good practices the following table is used in phase 1:

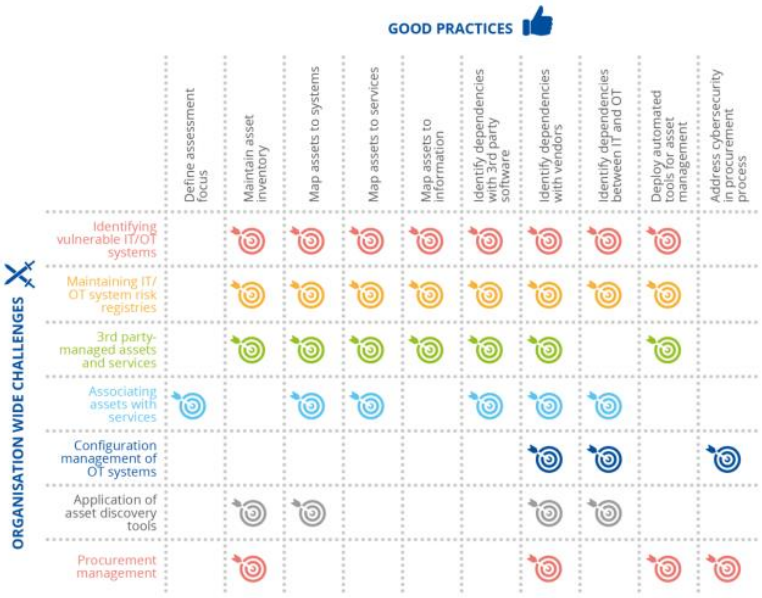


Figure 11: Mapping of good practices against challenges in identifying and evaluating cyber related assets and services (source: ENISA guidelines on cyber risk management for ports)

The same method is used in all four phases.

In phase 4 after mapping the organizational challenges against the good practices in addressing cybersecurity maturity, 3 maturity levels are defined: basic, intermediate and optimal.

A table is drafted with all the cybersecurity measures that needs to be implemented. Per measure states are defined which conclude if in the current situation the measure is implemented in a basic, intermediate of optimal level.

This last table allows to identify priorities for investing resources for improvement and/or building the programmatic foundations for organisational cybersecurity maturity.

6.3.2 Msc-fal.1/Cir.3 Guidelines on maritime cyber risk management (IMO)

The IMO MSC-FAL.1/Circ.3 guidelines on maritime cyber risk management[16] provide high-level recommendations for addressing cyber risks in the maritime industry. These recommendations include:

- Foundation: The guideline emphasises the importance of establishing a strong foundation for understanding and managing cyber risks. This includes developing a cyber risk management strategy and policy, identifying and protecting critical assets, and implementing risk management processes and procedures.

[16] International Maritime Organisation (2022), https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf

- Detailed guidance: The guideline provides detailed guidance on cyber risk management for the maritime industry. This includes guidance on identifying cyber risks and vulnerabilities, implementing security controls and risk mitigation measures, incident response and recovery, and monitoring and reviewing the effectiveness of cyber risk management activities. Additionally, it suggests that the Ship Owners and ship management companies can also refer to the International Ship and Port Facility Security Code (ISPS) which also include security measures to address cyber risks.

It's worth noting that these guidelines are not specific to technical guidance, but rather functional guidance that helps maritime organisations to understand the importance and scope of cyber risks in their operations, and to implement the appropriate cyber risk management measures to address them.

6.3.3 D8.1. Guidelines for Cybersecurity Training Programme across EU[17] (CYBER-MAR)

6.3.3.1 Content

- Includes challenges and gaps to which the cybersecurity and maritime domains are exposed
- Includes guidelines and recommendations obtained out of the executed environmental analysis
- List of domain stakeholders
- Focused on Political, Economic, Social, Technological, Environmental, and Legal factors
- Focused on different European countries and the differences between them
- Provides a global picture of challenges, gaps for maritime cybersecurity in the EU and presents preliminary recommendations.

6.3.3.2 Interesting conclusions

Several interesting conclusions can be drawn from this report.

- The legal foundations of cybersecurity within the EU are noted to have discrepancies between member states, and that national security strategies need updates and reinforcement with relevant legislative and policy instruments.
- In terms of education, it is noted that some EU members need to implement national education strategies to reinforce competence and awareness.
- Additionally, operational capabilities, specifically in regards to CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams), are established in member states but their mission and experience vary greatly among EU countries.
- Finally, it is noted that there is a lack of systematic cooperation with non-governmental entities and public-private partnerships, and that the practical implementation of sector-specific plans remains limited.

6.3.4 ISO Standards

The International Organization for Standardization (ISO)[18] is an independent, non-governmental international organisation that develops and publishes standards. These standards provide a common set of guidelines, specifications, and best practices for various industries and sectors, including information technology, manufacturing, transportation, and healthcare.

ISO 27001 and ISO 27005 are two of the most widely known and used standards dedicated to information security. They are specifically focused on providing a framework for managing information security risks, with ISO 27001 providing requirements for an information security management system (ISMS) and ISO 27005 providing guidelines for information security risk management.

[17] Cyber_MAR (2022), https://www.cyber-mar.eu/wp-content/uploads/2021/02/D8.1-Guidelines_Cybersecurity_Training_Programme_v1.00.pdf
[18] International Organization for Standardization (2022), https://www.iso.org/

ISO 27001 sets out a formal process for identifying, assessing, and managing risks to the confidentiality, integrity, and availability of information. Annex A to this standard lists the implementation of security controls to mitigate those risks. ISO27001 can help organisations to **demonstrate** to customers and other stakeholders **that they have a robust information security management system in place** and sets general requirements on the implementation of risk management measures.

ISO 27005, on the other hand, provides guidelines for managing information security risks. It is a subset of a broader set of best practices for data breach prevention in an organisation. This standard gives more information on **how, what and why** to implement a robust information security management system. ISO 27005 contains a description of standard risk process (cfr Figure 12 below), with description of typical activities, prerequisites and outcomes, a number of decision points and a Plan-Do-check-Act cycle.

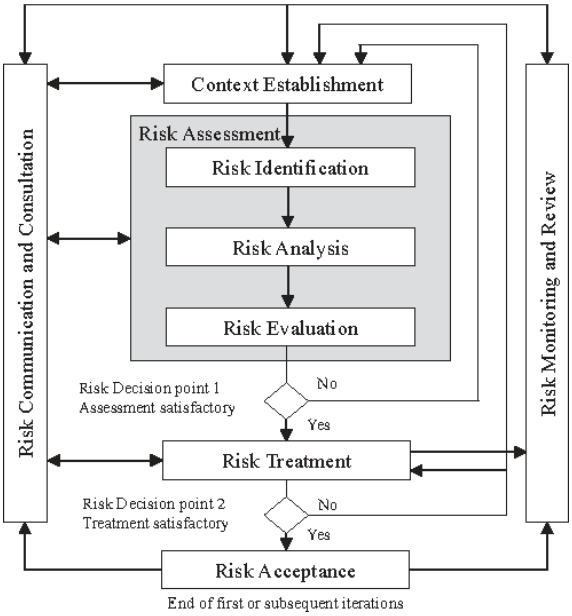


Figure 12: ISO27005 process flow diagram (Source: ISO27005)

ISO 31000 and **ISO 31010** are more general standards that aim to bring different existing standards together in one framework. They provide a risk management process, including the description of standard risk process, typical activities, prerequisites, and outcomes. They give example methods for identifying, assessing, treating and monitoring the risk, for organisations that want to implement a risk management process in general and not only in Information security.

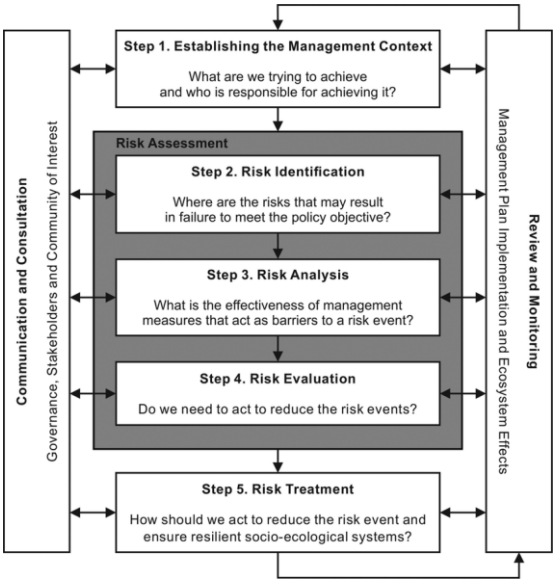


Figure 13: ISO 31000 process flow diagram (Source ISO 31000)

There are other interesting standards for the maritime domain, such as **ISO/DIS 23806**, which is a standard for cybersecurity on a ship.
Some standards, although meant for autonomous road vehicles, can have relevant points of comparison for smart shipping, in particular **ISO 26262** (for safety), **SAE ISO 21434** (for security) and **PAS 11281** (for safety & security),

6.3.5 Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity[19] (ENISA)

In a vast majority of cybersecurity breaches, a human element is involved. For instance, social engineering (see also section 7.1.2.1), the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes, is a very frequently used tool for cyberattacks.

This stresses the importance of people and behaviour in ensuring a robust and effective cybersecurity strategy. There is a growing recognition that technical cybersecurity measures do not exist in a vacuum, and need to operate in harmony with people. This has led to a plethora of academic research that seeks to address the role of the human in cybersecurity.

In this context, ENISA presents, as a first part of the report, four evidence based reviews of human aspects of cybersecurity based on different methodologies. The main conclusions drawn from these reviews are:

- It is required to shift from a technology and process centric view to a human centric view when evaluating the human aspects of cybersecurity. On top of the traditional quantifiable metrics, it is important to recognise that deeper insights can be gained by combining these with qualitative research and organisational studies.
- many of the models currently used to study human aspects of cybersecurity are a poor or moderate fit to actual behaviour
- There is increasing evidence that increasing users' understanding of the threat posed by cybersecurity breaches, or fear of the consequences, is not an effective tool for changing behaviour. Organisations should strive for adherence (active participation) rather than

[19] Enisa (2018), https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/at_download/fullReport

compliance - rapidly emerging threats require employees who are engaged and willing to step up.
- There is a moderately reliable link between people's ability to cope in the face of threats and their cybersecurity behaviour. The more people are convinced that a response works and that they are able to carry out this response, the more likely they will be motivated to contribute.

ENISA summarises that by systematically approaching and analysing the current cybersecurity stance of the organisation, and carrying out an in-depth analysis of the causes of any problem(s). Practitioners can take significant steps towards helping employees to act in a more secure way.
Security must therefore support and work with staff and business leaders to develop workable and effective security solutions, not fight them; Blaming people or their inability to comply with security policies (e.g. by referring to them as the 'Weakest Link') is counterproductive. We should stop trying to 'fix the human' and fix the security instead. Insecure behaviour is largely driven by security being too complex and/or effortful. Security needs to accept that human effort and attention is a precious resource primarily dedicated to productivity.
Thus, security needs to fit into work processes and tasks rather than disrupt them; policies and tools need to be targeted and easy to follow. If it were possible to make coping with cybersecurity threats a simple, obvious action, we would massively increase the likelihood that people will behave in a secure way and thus reduce the likelihood of threats ever materialising.

In a second part of the report ENISA proposes a circular model of awareness, analysis and intervention for organisations to systematically plan and implement changes to address human aspects of cybersecurity (as depicted in Figure 14).

Figure 14: framework for designing interventions for human aspects of cybersecurity (ENISA)

- **Awareness:** The starting point for any organisation is to gain understanding of its current cybersecurity status, and the ways in which human factors might support or detract from that defensive stance. This can best be achieved by combining methods that probe multiple levels in an organisation. The main pain points most often are not in awareness and training per se, but in supporting domains that strongly influence the work environment of the users, like work and technology design, organisational structure, leadership and problem management. These domains strongly influence the perception and the motivation, which in fact finally have a strong impact on the behaviour. It is also important to recognise that many 'problems' that seem 'human' in cause may be due to a variety of causes, some of which are not within the control of the individual.
- **Analyse:** This can be divided into two core elements: analysis of the problem (and root causes), and choice of appropriate method to study the problem (and to measure success). Practitioners should consider conducting a detailed analysis of the causes or barriers to conducting the desired behaviour. In this respect ENISA identifies two models:
    - The COM-B model (Michie et al., 2011) to identify why a desired behaviour may or may not be carried out based on the factors capability, opportunity and motivation.

  - The B=MAT model (Fogg, 2009) whereby Behaviour = Motivation x Ability x Trigger, to guide thinking about possible interventions.
- **Plan:** Once awareness and analysis has been completed, the next stage is to plan based around that. The exact nature of that planning will be determined by the diagnosis of the problem in the previous two stages.
- **Implementation:** It is important to note that changing behaviour (or indeed organisational culture) is likely to be a long-term project.
- **Evaluate and iterate:** Both the process and the outcome should be evaluated and evaluation is to be used as a starting point for a new cycle.

In a last part of the guideline, recommendations are developed towards specific groups:

- Policy makers
- Management and organisational leadership
- CISO and security specialists
- CSIRT's /CERT's & SOC's
- Software Developers - and those who manage and educate them
- Awareness raising among managers

6.3.6 Reducing the Cyber-Attack Surface in the Maritime Sector via Individual Behaviour Change[20]

This research paper was published in the context of cyber 2022 - The Seventh International Conference on Cyber-Technologies and Cyber-Systems. It describes how humans play a significant role in cybersecurity in a dual fashion; on the one hand, human error allows for the majority of attacks to be successful, as in the case of ransomware attacks via phishing, and on the other hand, appropriate security behaviours can serve as a strong line of defence.

The paper advocates that **security needs to transcend awareness and materialise as behaviour of individuals**. If this is achieved the vulnerability and susceptibility of the maritime sector can be significantly minimised via investing in the human factors of cybersecurity. Humans can become a significant 'line of defence' in the sector, if equipped and trained appropriately.
In order to change security behaviour, the authors propose an AI-based individualised assistant which

a) is customised to the particular environment of implementation, e.g., by analysing and codifying the existing – and being updated with new – guidelines on maritime cyber risk management, security policies and standards, and

b) learns the individual's personal characteristics, behaviours, and knowledge gaps, and directs them to relevant information in a focused fashion. For example, the tool will know which policies and procedures are required for the person's role and rank and will learn which knowledge gaps the person has;

it can then prompt the individual with targeted information.

6.3.7 EMSA online course on awareness in maritime cybersecurity

The European Maritime Safety Agency (EMSA)[21] is a part of the Directorate-General for Mobility and Transport of the European Commission (DG-MOVE). EMSA offers an online course on Awareness in Maritime Cybersecurity[22] which can be watched for free. The course provides an overview of cybersecurity in the maritime domain and covers several important topics including:

[20] Royal Holloway University of London (2022) https://pure.royalholloway.ac.uk/ws/files/47210933/K_Mersinas_CD_Chana_2022_Reducing_the_Cyber_Attack_Surface_in_the_Maritime_Sector_via_Individual_Behaviour_Change_CYMAR22_.pdf
[21] European Maritime Safety Agency (2022), https://emsa.europa.eu/
[22] European Maritime Safety Agency (2022), https://www.emsa.europa.eu/contact/advanced-search/item/3477-cybersec.html

- Module 1: Welcome and Introduction
- Module 2: Basic concepts in maritime cybersecurity
- Module 3: International legal framework applicable to the maritime domain
- Module 4: European legal framework applicable to the maritime domain
- Module 5: Challenges

The course is interesting to watch as it will give an overview of maritime cybersecurity and legal framework that are applicable to the maritime domain globally.
It is well suitable for those who are seeking to understand the complexities and challenges of ensuring the safety of the marine sector in terms of cyber threats.

6.3.8 Non-European guidelines

There are many non-European cybersecurity guidelines, among which we name only two that have a particular relevance for IWT:

United states department of transportation (USDOT):
The United States department of transportation has a program that specifically handles cybersecurity in transportation[23] and covers several domains:

- Vehicle cybersecurity
- Infrastructure cybersecurity
- Dedicated short-range communications security
- ITS Architecture and Standards security

United States National Institute of Standards and Technology's[24] (NIST)
The United States National Institute of Standards and Technology (NIST) was tasked by the US Cybersecurity Enhancement Act of 2014 to identify and develop cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. NIST published in 2014 and updated in 2018 a "Framework for Improving Critical Infrastructure Cybersecurity". The goal of this framework is to help organisations to better understand and improve their management of cybersecurity risk.

6.4 Business Continuity Management (BCM)

BCM describes a managed process to overcome emergencies and make an organisation more resilient against emergencies and crises. Like the ISM needs the ISMS as a system to function. The BCM needs the Business-Continuity-Management-System (BCMS) to work in an organisation. Core elements of the BCMS are the BCM-Organisation, the BCM-Techniques, the BCM-Process, the BCM-Resources, and the BCM-Documentation.

BCM-Organisation
The BCM-Organisation is a particular form of organisational structure that only takes over in the case of an emergency. It consists of three levels. the strategic-, tactic-, and operative levels.

BCM-Techniques
The typical techniques of the BCMS are the business impact analysis, the BCM-Risk Analysis, Business-Continuity-Strategies, and Business-Continuity-Plans which are often named emergency plans.

To better understand how the BCM benefits in making an organisation more resilient, the BCM-Techniques will be shortly explained.

[23] U.S. Department of Transportation (2023), https://www.its.dot.gov/research_areas/cybersecurity/index.htm
[24] U.S. NIST (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

- **Business-Impact-Analysis (BIA):** The BIA examines which business processes are time-critical and at which point outages are not tolerable anymore. This is important for the Business-Continuity-Plans to define if and when the workflows of an organisation have to be put in emergency mode and which resources are needed in that situation.

- **BCM-Risk-Analysis:** Like any Risk-Analysis the BCM-Risk-Analysis consist of risk assessment, risk evaluation, and risk response to examine potential causes for the outage of critical workflows.

- **Business-Continuity-Strategies:** The BCM-Risk-Analysis identifies the risks against which strategies have to be identified or developed, evaluated, and established. The worked-out strategies for specific scenarios can then be put together in Business-Continuity-Plans.

- **Business-Continuity-Plan:** The Business-Continuity-Plan has the objective to prevent the outage of time-critical resources with the help of alternative activities until the normal workflow is established again.

BCM-Process
The BCM-Process is a continuous process following the Plan-Do-Check-Act model (PDCA-Cycle) to establish, operate and improve the BCM.

BCM-Resources
BCM needs enough staff and financial resources to be operated. The effort that needs to be put into the BCM to make an organisation resilient against emergencies of all kinds should not be underestimated.

BCM-Documentation
Documentation is an essential component of any organisation's overall BCM program. The purpose of the BCM documentation is to provide clear guidance and direction to the organisation's management and employees on how to respond to and recover from disruptive incidents.

Effective BCM documentation should be regularly reviewed and updated to reflect changes in the organisation's operations, risk profile, and technology landscape. It should be easily accessible to relevant stakeholders and communicated to all employees to ensure that everyone understands their role and responsibilities in maintaining business continuity.

6.5 Privacy

The General Data Protection Regulation (GDPR) is the comprehensive privacy regulation that applies to all organisations operating within the European Union (EU). The GDPR establishes strict standards for data protection and privacy and gives individuals greater control over their personal data, including the right to access, rectify, and delete their information.

The GDPR requires organisations to implement appropriate technical and organisational measures to protect personal data against unauthorised access, alteration, and destruction. This includes implementing robust cybersecurity measures.

Fairway authorities play a critical role in ensuring the privacy and security of sensitive data and systems. It is important for them to be aware that the introduction of new technologies can have a potential impact on privacy and that a Data Protection Impact Assessment (DPIA) is required any time a new project is started that is likely to involve “a high risk” to other people’s personal information.

In this regard, special reference is made to SuAc 3.3 where the use of sensors and PNT is described. New sensors create a potential privacy impact and the implementation of adequate cybersecurity measures is needed to keep the data safe.

An Information Security Management System (ISMS), as described in next section, can be an effective tool for safeguarding privacy by providing a structured and systematic approach to data protection and security. In addition, it can help organisations to comply with the General Data Protection Regulation (GDPR) by providing a framework for managing personal data in accordance with the regulation's requirements. It is therefore recommended that fairway authorities and operators handling privacy sensitive information introduce an ISMS

It is important for an organisation to define and classify the different types of information and data it processes and stores. Based on these classifications it should be possible to distinguish between regular (public) data, sensitive data, classified data, proprietary data and data through which people can be personally identified. Concerning the privacy aspect of data all measures should be taken to protect all classified data according to the strict security controls, especially for Personally Identifiable Information (PII). More information on Data classification can be found in the FIPS-199 and NIST 800-122 guidelines.

6.6 Information Security Management (ISM)

ISM means the planning and controlling tasks needed to build a functioning Information Security Management System (ISMS). The scope of ISM should be broad enough to cover all topics within the organisation and should at least contain controls on the level of people, processes, systems, applications, and facilities.

The scope of ISM should be broad enough to cover all topics within the organisation and should at least contain controls on the level of people, processes, systems, applications and facilities. Furthermore, the organisation should always ensure that any processes they implement are appropriate and tailored for their own environment.

To apply ISM in a structured and proven manner it should be noted that the key is to choose an Information Security Management standard to implement. Various standards exist which provide generic guidelines on how to implement controls within an organisation. These general guidelines will lead to the practical implementation of controls.

ISM should provide a high-level strategy that can be applied through a "plan" on the various structures within the organisation. A strategic plan consisting of a high-level strategy to be reached within a fixed set of time (e.g. the next few years). This strategic plan should contain a (yearly) tactical plan which then contains operational plans. This allows for a smooth transition phase over time as can be seen in Figure 15 below.

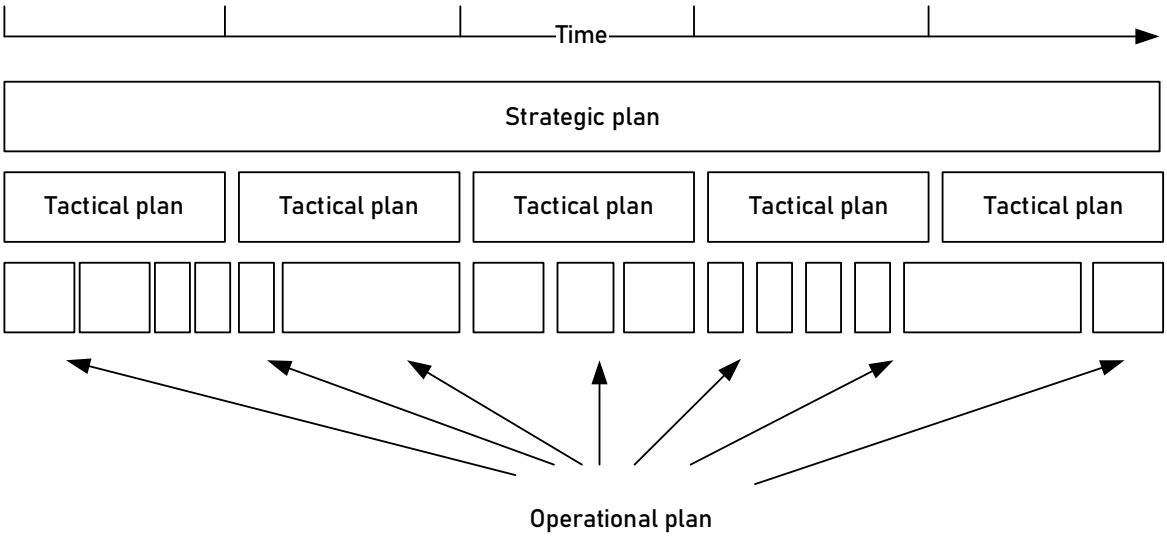


Figure 15: ISM planning phases

6.6.1 Information Security and Cybersecurity

Classical IT-Security means to do anything to defend a classical IT-System.

Cybersecurity takes this approach further and not only takes the IT-System but also the networks it is placed on (also the internet) and other connected IT-Systems into account.

Information Security takes this approach even a step further and focuses on the data that is to be protected. It tries to protect data not only digitally and therefore includes Cybersecurity, but also data that is stored on paper or otherwise like e.g. in the minds of people. Next to that Information Security can also be related to physical protection like protecting buildings, rooms, data centres, vehicles, vessels, specific equipment, etc. Furthermore, controls could be set on various levels of the organisation, for instance for hiring staff, working with contractors or hardware/software vendors, etc. Information Security, therefore, is the most holistic approach to protecting data, human resources, and IT-Systems. Since scoped so broadly, ISM should be considered a task of upper management, at the organisational level.

6.6.2 Basic values of information security

There are three basic values of information security. If one of these values can be broken the system is not secure so there have to be actions taken to prevent these values from being broken. These values are also referred to as the CIA triad, as can be seen in Figure 16.

Confidentiality means protection against the unauthorised disclosure of information. Confidential data and information should only be accessible to those authorised using the methods permitted.

Integrity refers to ensuring the correctness (intactness) of data and the correct functioning of systems. When the term "integrity" is used in connection with the term “data”, it means that the data in question is complete and unchanged.

Availability: Services, information, and the functions of IT-Systems, IT-Applications, and IT-Networks are considered available when users are able to access them as intended at all times.

Figure 16: CIA triad

6.6.3 Information-security-management-system (ISMS)

An ISMS is a System that combines management principles, resources (including human resources), and a working security process to get to the state of administrated information security. An ISMS is a necessary part of Information Security Management and gives an organisation the tools it needs to follow up its Information Security Management implementation and enables them to keep the oversight.

An ISMS is a systematic approach to establish, implement, operate, monitor, review, maintain, and improve an organisation's information security.

It should be noted that in addition to an ISMS it is highly recommended to define a "specialists taskforce" to follow up on the ISMS content and accuracy of the various controls that will be put in place. The constant evolution within Information Security Management requires specific practical and theoretical knowledge to be able to adequately create and define policies and controls. For instance, a CISO (Chief Information Security Officer) can fulfil this role together with an InfoSec team of specialists.

Management principles
There are six management principles that have to be taken care of. Assumption of overall responsibility for information security, Initiating, managing, and supervising information security, Integration of information security, setting objectives that can be achieved, Considering security costs against benefits, and the Role model function.

Security process
To organise the security process the framework of conditions has to be determined. The security objectives and an information security policy have to be formulated and the appropriate level of safety of the business processes has to be determined. Then a security organisation can be established and the information security policy can be implemented. After this, the security process is started. It is crucial to maintain the information security process through continuous improvements and revisions.

Security concept
The Security concept consists of a risk analysis to develop a strategy for dealing with the risks. Then the security safeguards have to be selected and implemented. This is further described in section 6.6.4

Documentation
Documentation is crucial for an ISMS to work. Every step of the development must be documented for the next review cycle to find potential gaps and to improve on what has been done before. Guidelines and concepts have to be written out, verified, and implemented. Also, the Risk analysis and the selection of the security safeguards have to be documented as well as the check on every system whether the safeguards are implemented or not.

6.6.4 Security concept

6.6.4.1 Risk-Management

In order to select security safeguards that work effectively a risk analysis has to be done. The Risk-Management identifies, analyses, and classifies risks to help to develop security safeguards for the organisation.

Risk refers to the potential for an event or set of events to negatively impact an organisation's ability to achieve its objectives. It is generally understood as the product of the likelihood or frequency of an event occurring and the potential impact of that event.

Risk = Likelihood X Potential impact

Risk can come from various sources, including financial, operational, strategic, and compliance-related issues, among others.
Cyber risk is the risk of damage to an organisation that arises from its information systems.

6.6.4.2 Risk Framework

There are many different frameworks on how exactly a risk analysis can be done. The important steps that are generally proven best-practice will be presented in the next paragraph.

6.6.4.3 Risk-Analysis

Most organisations are too big to do just one Risk-Analysis. Therefore, the range of the analysis has to be defined. Which systems, organisations, etc. shall be in the scope of the analysis? Then the threats can be identified. Elemental threats (weather, natural disasters, infrastructure problems, etc.) have to be taken into account as well as specific ones like cybercrime or supply chain problems, etc. The threats have to be rated in different classes depending on their probability of occurrence and their potential for damage to the organisation. After that, the risks can be evaluated via a Risk-Matrix.
As a preparatory measure, it is worthwhile for organisations to carry out a risk assessment. Figure 17 shows that pre-assessment activities, such as

- Threat identification: understand external and internal cybersecurity threats (to a ship or other assets), e.g. caused by inappropriate use and poor cybersecurity practices. By means of a threat model, potential threat patterns are uncovered, which are then analysed further within the framework of the risk assessment. Furthermore, an attack graph, in which cyberattacks are modelled and thus a visual representation of attack paths that an attacker could take to reach his target, can also help.
- Vulnerability assessment: This involves identifying vulnerabilities in computer networks, systems, hardware, applications and other parts of the IT environment (e.g. onboard systems). Vulnerability scanners, for example, are a useful tool for identifying the vulnerabilities of systems. Penetration testing (of critical IT and OT infrastructure) is also suitable for identifying vulnerabilities and assessing them. This is a method to identify web applications, networks, computers or systems and thus possible vulnerabilities that could be exploited by attackers later on. De facto, penetration testing attempts to perform the same operations as potential future attackers. On the one hand, these tests help to fill vulnerability gaps by applying measures and, on the other hand, personnel thereby learn about potential attacks through malicious entries. Based on the vulnerabilities, a comprehensive security plan for, for instance, the ship's network should be developed.
- Likelihood assessment analyses the likelihood of a cybersecurity event as a product of the threat and the vulnerability
- Impact assessment: e.g. through
  a) CIA models (see chapter 6.6.2),
  b) quantification of the impact (e.g. in low - moderate -high or more specifically: safety of personnel, safety of environment, cargo safety, asset safety, business continuity, financial impact, and company's reputation)
  c) the assessment of the impact on critical equipment and technical systems which are necessary to properly assess the risk to an organisation from cyber threats.

An important aspect of risk assessment is the involvement of the entire organisation at all levels (e.g. staff) to raise awareness of potential risks throughout the organisation.

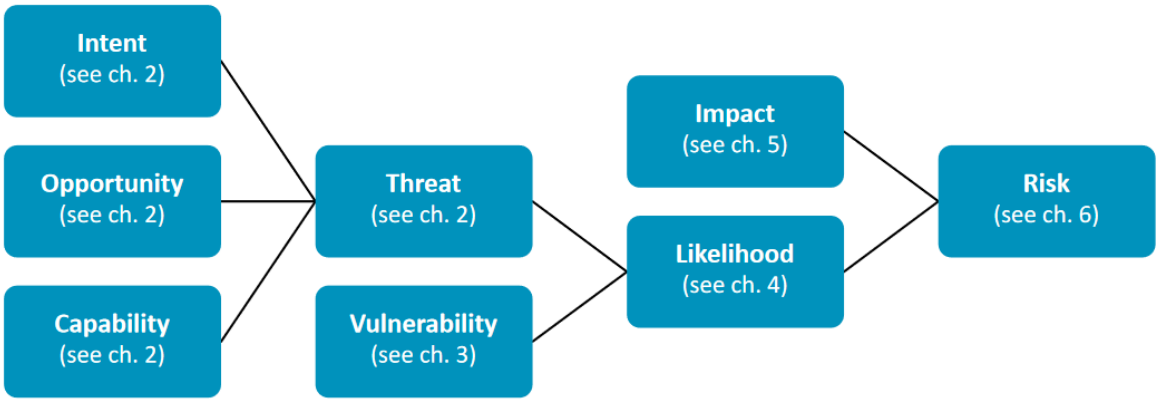


Figure 17: The relationship between different factors influencing the risk. The lines represent multiplication, ie "Likelihood" is (see [25])

Based on this risk assessment, organisations can then prioritise the identified risks in order to determine which potential threats could cause the greatest damage within the organisation and where

[25] BIMCO (2021): The Guidelines on Cybersecurity Onboard Ships - Version 4.

(to which assets or areas). Defence mechanisms should be put in place/adapted according to the prioritisation.
Furthermore, other subsequent tasks should not be forgotten, such as

- debriefing the results and reporting. As with the risk assessment, this should be an iterative document that should be updated based on the continuous re-evaluation of the risk assessment.
- Debriefing with manufacturers to jointly identify the right solution to address the vulnerabilities.

Furthermore, contingency plans should be established based on the risk assessment.

An example of a risk assessment and the identification of appropriate mitigation measures to reduce the impact of the potential hazard with regard to ECDIS can be seen in Figure 18.

System	Impact	Likelihood	Initial risk	Mitigation	Residual risk
ECDIS	**Score 5** due to risk of catastrophic events like grounding and collision	**Score 4** due to active USB ports, computer used for other purposes, connection to admin network for access to shared printer, connection to automatic chart updates via satellite via trusted vendor	Risk = 5 x 4 = 20	Password protect and restrict PC use to ECDIS only	Risk = 5 x 3 = 15
				Disconnect from admin network	Risk = 5 x 2 = 10
				Blind off USB ports	Risk = 5 x 1 = 5

Figure 18: Example of risk assessment and identification of mitigation measures (see 25)

6.6.4.4 Risk-Matrix

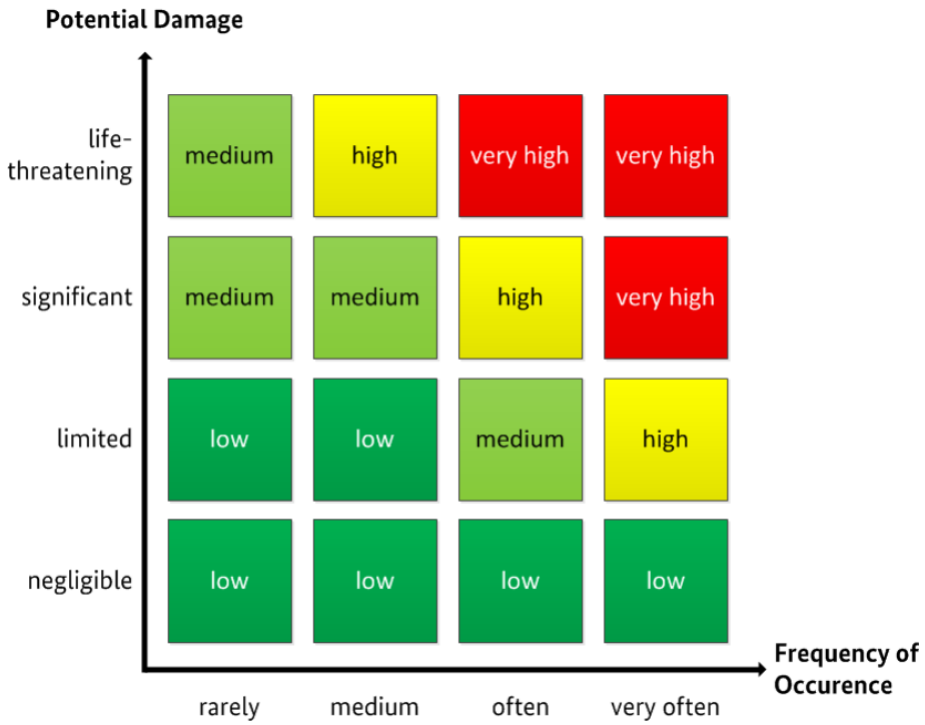


Figure 19: Risk Matrix (Source: BSI Standard 200-3 Figure 3)

Every organisation has then to determine its risk appetite as shown in the next figure.

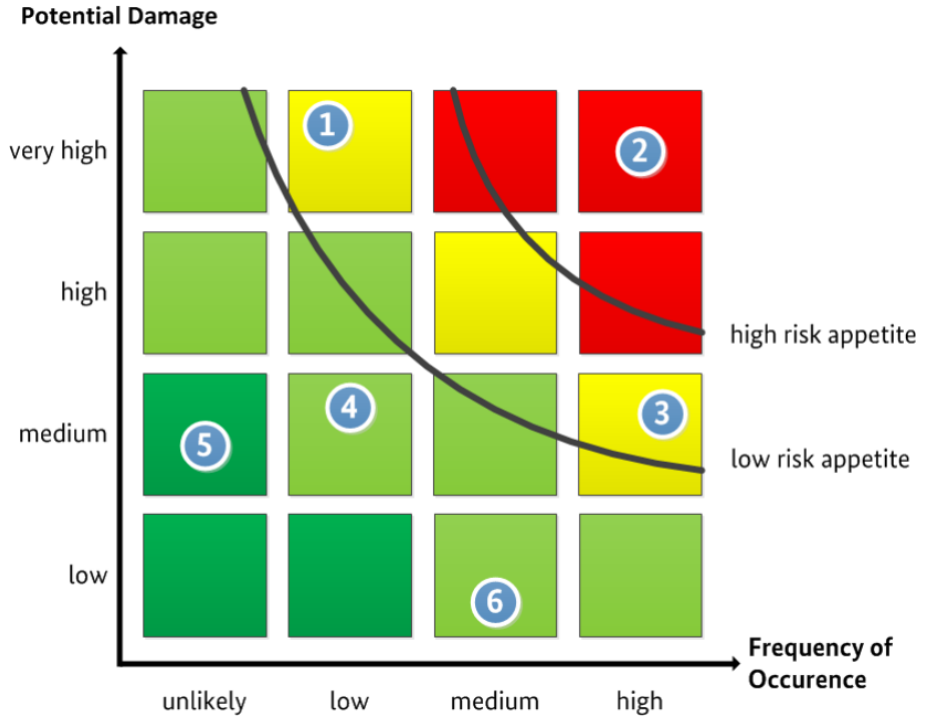


Figure 20: Risk appetite (source: BSI standard 200-3 Figure 5)

Risks that are determined and are to the left of the risk appetite line are negligible and will be accepted. Risks that are on the other side cannot be ignored and have to be treated.

Co-funded by the European Union

6.6.4.5 Risk-Treatment

Risk-Treatment, for the most part, can be done in four ways: Avoidance, reduction, transfer, or acceptance.

Risk-Avoidance
This means restructuring processes so that the risk is no longer existing.

Risk-Reduction
This means implementing special safeguards and measures to reduce the probability of the risk occurring so that it is on the left side of the risk appetite line and can be accepted.

Risk-Transfer
This means transferring the risk to a third party. Examples would be to take out insurance or to outsource specific risky processes to third parties that are specialised in dealing with those processes.

Risk-Acceptance
This means accepting a risk, which should normally be addressed, for a specific time. This is normally done, when a risk is just temporary and/or the cost to lower its risk potential is not justified by the measures that have to be taken.

6.6.4.6 Risk-Monitoring

As most security-based processes, Risk-Management also is a continuous process that follows the PDCA- Cycle. Risks have to be re-evaluated after an appropriate time to check if their risk potential has changed. These re-evaluations can be different for each risk and have to be documented when the risk is addressed.

7 Measures against cyberattacks/ for cyber resilience

7.1 Types of Cyberattacks

7.1.1 The objective of Cyberattacks

Attackers want one of three things or deny these, Money or Data or computer resources (mostly computation power). To achieve this, they use different strategies that we identify as attacks. The malware itself is not an attack; it's a tool an attacker uses to achieve his objective. Only when we use this tool for a harmful purpose are we talking about an attack. Most, but not all attacks these days consist of two things; Social Engineering and Malware.

The result of a cyberattack is that one or more key values of the CIA triad are violated, see Figure 16 in chapter 6.6.1. Cyberattacks will try to alter one or more of these key values of Information Security.

Attacks or breaches of these key values of Information Security cannot be attributed solely to cyberattacks. Different attack vectors exist where a breach of these value is possible by not using a single digital or analog device or any other type of tool. For example physical theft of documents breaches „Availability" and possibly „Confidentiality" of the CIA triad of Information Security.

This topic discusses types of cyberattacks which are more related to the digital world and digital information, but not exclusively. An organisation needs to be aware that other attack vectors exist, hence the advised broad scoping of Information Security Management in general, as mentioned in chapter 6.6.

7.1.2 Tools

Attackers use all kinds of different tools to gather information, attack or infect systems like: network sniffers, research, pen testing frameworks, vulnerability scanners, brute force and cracking, self-written, malware of any kind, bot-networks, and Social Engineering. The next chapter will talk about these different tools and how attacks come together.

7.1.2.1 Social Engineering

To get Malware onto the computer of a target the attacker needs to trick his target. For this he often uses social engineering (click on this link, download this document, etc.). But social engineering is also used to gather information, get physical access, or even the data itself. The most holistic definition of social engineering would be "The deliberate influencing of human interaction to do something that would not have been done without the influence." Therefore, social engineering comes in very different forms.

Social engineering has been proven to be so effective that nearly any common attack these days uses social engineering to some extent. Therefore, it is crucial to sensitise every employee of an organisation to strengthen their security awareness and spot social engineering attempts.

Attacks involving primarily social engineering:
Phishing Attacks, Vishing (via phone), Smishing (via SMS), Pretexting (offering a deal that is too good to pass or pretending to be a superior), Whaling Attacks (pretending to be someone you know), Tailgating (following an authorised employee and gaining access that way)

7.1.2.2 Persistent Threats also called Malware

Malware comes in all different kinds, the most popular and known are Viruses, Worms, and Trojans. These can be differentiated by their behaviour like Rootkits[26], Keylogger[27], Chimera[28], Network Malware, and Ransomware.

7.1.2.3 Exploits

Exploits are pre-coded or self-coded ways to exploit a vulnerability of a protocol, software, or a specific system. These can be found in frameworks or can be self-written by attackers to implement them into their malware or to use them to get access to systems via a network. An exploit itself is not malware. Conversely, malware does not need to include exploits to be identified as malware. However, most malware uses some kind of exploit, e.g. to get administrative rights on a system in user mode.

7.1.3 Attack Types

There are too many attack types to name them all, but most of them can be clustered together into bigger categories. The most commonly known will be discussed in this chapter.

7.1.3.1 Passive Attacks

Brute Force
The attacker uses sheer calculation power to get access to a system by trying out all different possible combinations of characters.

Countermeasures:
Longer and more complex passwords, login suspension after failed attempts

Viruses, Trojans, and Worms
These three are very similar in terms that they are classical malware. They are differentiated by their biology. A Virus infects data and writes itself into its code to get executed. A Trojan disguises itself as a not-harmful program to get executed. A Worm is itself a program that uses different techniques to get executed but replicates itself over the network and infects other devices.

Countermeasures:
Security Awareness online, Antivirus Software, Intrusion Detection or Intrusion Prevention Systems

Sniffing
Means getting information about the target network by listening to the traffic. Usually used before an active attack. An attacker needs access to the network or the front end of the software he is sniffing on.

Countermeasures:
Encryption of the data traffic for example by using VPNs when accessing from the outside, Intrusion Detection or Intrusion Prevention Systems for intra networks

Dictionary attack
The Attacker uses not brute force to crack a password but gathered information. Lists of standard passwords or password lists of the most used passwords but also self-made lists. The more the attacker knows about the target the more likely he will succeed.

Countermeasures:
More complex and longer passwords, no trivial passwords, usage of cryptographic passwords via a password safe, always change standard passwords

[26] Malicious software designed to enable unauthorized access: https://en.wikipedia.org/wiki/Rootkit
[27] Soft or hardware designed to capture keystrokes (passwords): https://en.wikipedia.org/wiki/Keystroke_logging
[28] Type of ransomware: https://www.knowbe4.com/chimera-ransomware

7.1.3.2 Active Attacks

Zero-Day-Exploit
The exploitation of a vulnerability that was previously unknown. The name comes from the reaction time the software developers have to fix the exploit -> zero days. This is the most dangerous form of cyberattack and there are no countermeasures that work right away. The only chance is to detach the systems that are vulnerable to the exploit from the network and wait for a security update.

Drive-by-Exploit
This means that malicious code gets embedded inside a website and infects the computer of a target via a vulnerability in the browser of the target. An example of such an attack is a Cross Site Scripting (XSS). An XSS attack is used to embed malicious scripts in (trusted) websites.

Countermeasures:
Up-to-date browser updates, script blocker, security awareness

Man-in-the-Middle Attack
The attacker places itself in between the connection of the target and its communication partner. Now the attacker can read out the whole communication or manipulate it, however he wants.

Countermeasures:
Extended-validation-SSL-certificates

Denial-of-Service Attack (DOS)
The DOS Attack can take different forms. What they all have in common is the denial of access to a resource like a website or a server. This can be achieved by mostly flooding a server with requests via protocol vulnerabilities or bot-networks but other forms of denying access to digital resources of any kind count as DOS too. A bot-network is a robot network of servers/computers infected by malware that are under the control of an attack party. This can be used to carry out so called distributed denial of service attacks (DDOS).

Countermeasures:
IP-Blocking, Hiding the own IP, Traffic analysis and redirection

Combination Attacks
By combining social engineering and other tools like fake websites or phishing mail with malware the attacker tricks the target into executing his malicious program to infect the target. Nearly all common attacks are Combination Attacks that involve some kind of social engineering and malware. Phishing is the most commonly known under them. When it comes to combination attacks the limit of what is possible is up to the imagination of the attacker and the resilience and security awareness of its target.

7.2 Cyber resilience

As already explained under the section Technical Terms at the start of this report, cyber resilience[29] is the ability of organisations to protect themselves against cyberattacks and to recover from them (quickly) in the event of an attack, thus resuming normal business operations.

Organisations can achieve or improve their cyber resilience by

- Identifying vulnerabilities and risks
- Protecting the infrastructure, systems, applications, data, etc.
- Detecting cyber threats and attacks
- responding to cyberattacks
- recovering from cyberattacks and
- adapting mitigation measures

[29] https://www.ibm.com/downloads/cas/MNEL3WVY, https://conscia.com/de/loesungen/security/

This strategy for achieving or increasing cyber resilience can be mapped in a cycle (see Figure 3), as the actions within the pillars recur depending on the temporal dependency on a potential cyber incident.

Figure 21: Cybersecurity cycle

7.2.1 Identify

Every organisation has points of attack through which attackers can gain unauthorised access to systems, applications or data. To counteract this, a first important preventive step against cyberattacks or to increase resilience is the development of an organisational understanding of the essential elements of business operations (= creation of a security roadmap). Only when the organisation has gained an understanding of the infrastructure, systems, applications, their data and the interrelationships of these, will they be able to identify and prioritise vulnerabilities and risks in the organisation and subsequently avoid / address them. In addition, the existing security measures that have already been taken to protect against cyberattacks should be continuously analysed in order to be able to make timely adjustments if necessary.

The identification of possible threats is only possible when all assets and information streams can be identified and classified. Knowing what to protect is handled by Asset management. Assets can be tangible (computers, facilities, supplies, personnel, …) and intangible (intellectual property, data, organisational reputation, …).

7.2.2 Protection

Once the vulnerabilities of the organisation or its infrastructure, systems, applications, data, etc. have been identified, appropriate protective measures can be developed, implemented or tightened to reduce the security exposure and thus harden the system. These include, for example, the development of cybersecurity policies, the implementation of security controls, the regular updating of systems, the implementation of security awareness training etc.
Furthermore, appropriate measures should be developed to enable the organisation to detect the occurrence of cyber incidents (see chapter 7.3).

7.2.3 Detection

By implementing the appropriate measures to detect cyber threats and attacks, organisations are able to detect threats or attacks at an early stage through implemented alerts. This includes, for example, the identification of behaviour patterns, i.e. understanding how "normal" users behave. This can minimise harmful effects on business operations and thereby reduce the time to recover from a cyber incident. This can be done, for example, by conducting routine penetration tests, implementing Security

Information and Event Management (SIEM) and/or Intrusion Detection & Prevention software (IDS and IPS), and Security Orchestration, Automation, and Response (SOAR) (see chapter 7.3).

7.2.4 Reaction

Once a cyberattack has been detected and reported, organisations must respond appropriately to the attack. Pre-analysis (identify, protect, detect) or cyber forensic analyses enable organisations to respond to the cyberattack in an appropriate manner and, most importantly, in a significantly shorter timeframe through pre-prepared response plans. This could include simple measures such as a contact list and step-by-step instructions. This ensures that the optimal set of measures to quickly counteract the attack is available and that the right actions are taken to clean the system and to make the work possible again.
One way of reacting to cyber attacks is, for example, the use of intrusion response systems (IRSs) (see chapter 7.3).

7.2.5 Recovery

After the organisation has responded appropriately to the cyberattack, it is important to recover from it and to return to the normal status. This includes taking measures for business continuity, as well as the subsequent evaluation of the effectiveness of the measures taken (evaluation of the cyber forensic analysis) and, if necessary, a corresponding adjustment of the measures taken so far in order to stay one step ahead of potential threats. Backups and system recoveries, for example, help organisations to recover quickly from cyberattacks with data loss.

7.3 Security Measures

From the 5 elements of cyber resilience (see chapter 6.2), different security measures or controls can be derived that are available to organisations in order to …

- prepare for a cyber incident/attack in advance,
- react appropriately during an attack and
- return to the original business continuity after a cyberattack / incident.

A proven means to ensure the cybersecurity of different systems is the risk assessment. This identifies and evaluates potential threats, vulnerabilities, likelihood and impact in order to assess and prioritise the potential risks and finally find suitable protective measures (see chapter 6.3 for further information on risk assessment).

This chapter provides an overview of general existing countermeasures to ensure cybersecurity / improve cyber resilience. It should be noted that the following list of countermeasures is neither exhaustive nor timeless. This means that, on the one hand, it only gives an overview of selected generic security measures. On the other hand, cyber threats and the corresponding security measures are subject to constant change. Consequently, the following overview is an excerpt from the currently available security measures.
Nevertheless, these generic security measures are/should be also applied in inland navigation. Countermeasures that specifically address vulnerabilities in IWT are listed and discussed in detail in chapter 9.

The currently available security measures listed below are divided into three different categories:

- Administrative controls
- Technical controls
- Physical controls

7.3.1 Administrative controls

Organisations should implement policies, procedures or guidelines that define personnel or business practices in accordance with the organisation's security goals. To be able to create such policies, procedures or guidelines an organisation must be able to determine the scope of applicability. A key

factor here is to rely on a thoroughly implemented asset management system to be able to identify (as mentioned in chapter 7.2.1) and classify all assets and information streams. Knowing what needs to be protected is the basis of determining the further necessary administrative controls since these need to be applied to a certain scope of assets.

The value of an asset is debatable and should therefore be considered with respect to the asset owner's view.

These six considerations can be used to determine an asset's value[30]:

- Value to owner
- Work required to develop or obtain the asset
- Costs to maintain the asset
- Damage that would result if the asset were lost
- Cost that competitors would pay for the asset
- Penalties that would result if the asset were lost

Once the asset's value has been determined it can be used in the risk assessment and the further definition of the administrative controls. Typical administrative controls can be implemented, such as

- **Precautionary plans and analyses**
  Within the framework of cybersecurity management, it is advisable to draw up certain precautionary plans and analyses, such as an incident response and recovery plan, contingency plan, business continuity plan.

- **Management**
  In principle, all applied technical measures used to ensure the cybersecurity of an organisation should be managed at a higher level. This includes, for example:
  - management of access rights and the associated rights
  - Antivirus and antimalware management
  - MFA and password management
  - patch management
  - …

  To clarify the contents of the management of technical measures, these are explained in more detail below.

- **Governance and organisation**
  - Define personnel roles (privileges) and responsibilities for cyber risk management [31]
  - Based on the administrative roles, users are only given appropriate rights, e.g. access to all system configurations and data should only be allowed to selected persons with administrative roles. [31]
  - Create contact lists and step-by-step instructions

- **Training and awareness**
  Staff in an organisation plays a relevant role in the implementation of cybersecurity, as careless behaviour can quickly lead to breaches of security measures. Appropriate training and the creation of awareness of staff regarding cyber risks can help to ensure that phishing mails or possibly infected removable media are handled more carefully, thus preventing a large number of cyberattacks from the outset.[32]

- **Access rights**
  Manage and review the access rights of all employees and persons who need access to the network.
  - Only limited access to computers or networks for visitors [32]

[30] CompTIA® Advanced Security Practitioner (CASP) CAS-003 Cert Guide
[31] IMO (2021): Guidelines on maritime cyber risk management
[32] BIMCO et al. (20XY): The guidelines on cybersecurity onboard ships

  - Appropriate policies and procedures should also be developed for remote access by staff to prevent potential cyberattacks. These include, for example, who, when and what can be accessed. In addition, all remote access should be recorded. [32]
  - Usage of unauthorised software should be limited to non-critical operations [36]
  - Review audit logs and unauthorised changes

- **Configuration management**
  Since misconfigurations represent an increase in the cyber vulnerability of organisations and their systems and networks, security configuration management is an essential general countermeasure to protect cybersecurity. It is a process that involves the adjustment of the default settings of an information system. [33]

- **Upgrades and software maintenance**
  To protect hardware and software, they should be kept up to date at all times (e.g. by updating). [32]
  - Requiring software updates, including security patches, to be applied and tested in a timely manner, by a competent person. [32]
  - Keeping unauthorised software away from the organisations' systems [32]

- **Anti-virus and anti-malware tool management**
  Appropriate anti-virus and anti-malware tools that scan organisations' systems, detect cyber incidents and defend against them, must also be kept up to date to maintain the desired protection. [32]

- **Multi/factor authentication (MFA) and password management:**
  To protect data and systems, an appropriate password policy is necessary. Depending on the degree of confidentiality or relevance of the data and systems, MFA (explained in 7.3.2) should be applied. [32]
  - Ensuring that default passwords are changed after initial log-in [32]
  - Ensuring that common/shared usernames and passwords are not used [32]
  - Requiring minimum length (at least 8 characters) and complexity (e.g. uppercase characters, lowercase characters, numbers or symbols) [32]
  - Deleting the user accounts of colleagues and crew who have left [32]

- **Backup Management**
  In order to ensure data recovery capability, the creation of (manual or automatic) backup copy procedures and the performance of system updates are appropriate and should be applied. Backups can be made either manually by a portable storage device, remote or by automatic updates via a direct internet links. [32]
  Backups should also be regularly restored to check the validity of the backup and the procedures.

- **Data management**
  Ensure adequate protection e.g. by using encryption and retention of data based on the sensitivity of the information. [32]

- **Communication and media management** [32]
  - Setting protocols and channels for communication (e.g. between the ship and the shore side)
  - Segregating official and operational systems from personal and recreational use computers
  - Ensuring that critical work-related information is not shared on social media or personal email

- **Management of removable media** (e.g. USB keys, external hard drives, CDs, etc.) [32]

[33] Tanium (2022): What is Security Configuration Management? https://www.tanium.com/blog/what-is-security-configuration-management/

  - Usage of IT devices: Procedures should be established regarding the private use of the organisation's devices. [32]
  - Physical and removable media controls:
    - To prevent the transmission of malware through removable media, a clear policy on the use of such devices should be established to ensure that media devices are not used to transfer information between uncontrolled and controlled systems. If this cannot be prevented, additional requirements such as scanning removable media devices before or during use should be added to the policies and procedures. [32]
      - Restricting/limiting the types of media that can be used and types of information that can be transferred [32]
      - Improving the protection and ensuring the integrity/security of the device [32]

- **Equipment disposal including data destruction**
  Before disposing of equipment that is no longer needed, organisations should implement procedures to ensure that data, especially sensitive and confidential data, has been properly destroyed and cannot be recovered before the equipment is disposed of. [32]

- **Security Audits**
  Security audits are also a measure for analysing the risks and vulnerabilities of an IT system or computer programme. It usually takes place within the framework of quality management and serves to reduce security gaps and introduce best practices in organisations. Usually it is conducted by trained 3rd party entities, or by internal resources in preparation for an external audit. Based on the assessment of the protection needs of the IT structure, a selection of protective measures is made from the proposed catalogue of measures, which are then implemented within the organisation - i.e. to the exclusion of external auditors. [34]

- **Monitoring/testing**
  The applied barriers to secure cybersecurity should be monitored and reviewed to ensure the effectiveness and robustness of the barriers. Suitable tools for this purpose are e.g. functional testing, vulnerability assessments, penetration testing, red teaming, testing recovery plans, drills and audits. [36]

7.3.2 Technical controls

Organisations have a wide range of technical protection measures at their disposal to ensure cybersecurity. It is important to note that the implementation of these security measures alone is not sufficient. As already mentioned in subchapter 7.3.1, it is very important that the technical measures are kept up to date by the management.

- **Vulnerability scanning and testing:**
  - With the help of e.g. penetration testing, which should be carried out regularly, the vulnerability of the organisation with regard to cyber risks can be assessed.
  - The vulnerability patching is a short-term implementation of patches, i.e. pieces of code added to existing software to improve functionality or fix vulnerabilities that have been discovered [35]

- **Secure configuration of hardware and software**
  - It should be ensured that computers, servers etc. are only used for the purpose for which they were originally intended. [32]
  - Usage of unauthorised software should be limited to non-critical operations [32]

- **Password**

[34] Wikipedia (2022): IT-Sicherheitsaudit. https://de.wikipedia.org/wiki/IT-Sicherheitsaudit
[35] Rezilion (2022) : Vulnerability Patching: A Recourse Guide. https://www.rezilion.com/blog/vulnerability-patching-a-resource-guide-or-everything-you-need-to-know/

Introduce high requirements in complexity of a password (e.g. at least 8 characters, uppercase and lower-case characters, numbers and characters etc.) [36] It is even necessary to use longer passwords in combination with strong and modern Hash algorithms in combination with salts ("salting hash algorithms" is a specific method to strengthen passwords) in order to withstand brute force techniques. Passwords are often combined with further authentication methods and are thus usually part of a Multifactor Authentication.

- **Multifactor Authentication (MFA)**
  This is an electronic authentication method by which users are only granted access to an application or similar after the successful presentation of at least two pieces of evidence (factors). [37]

- **Antivirus & antimalware software**
  The software protects computers and IT systems from being infected by a variety of malware, such as viruses, worms, trojans etc. Should an infection nevertheless occur, the software recognises the malware and attempts to quarantine and destroy it.

- **Encryption**
  It "is the process through which data is encoded so that it remains hidden from or inaccessible to unauthorised users. It helps protect private information, sensitive data, and can enhance the security of communication between client apps and servers. In essence, when your data is encrypted, even if an unauthorised person or entity gains access to it, they will not be able to read it." [38]

- **Code Signing Certificate & Digital Signature**
  - Signing certificates verify the identity of the developers to digitally sign applications, drivers, executables and software programs as a way for end-users to verify that the code they receive has not been altered or compromised by a third party. That way these certificates prevent attackers from injecting malware into legitimate software without being detected.[39] [40]
  - This approach is also useful for handling official documents. By having an official signature, users can be sure on the one hand that the document comes from an official body and on the other hand that it has not been manipulated.

- **Extended-validation-SSL-certificates (EV SSL)**
  These certificates are mostly used to encrypt and secure web applications via https. This is to protect website users from phishing attacks. Extended validation SSL certificates are better than organisation and domain validated certificates. During the verification of an EV SSL Certificate, the owner of the website passes a thorough and globally standardised identity verification process.

- **Protection of networks**
  - *Network segregation:*
    Is the process that separates critical network elements from external networks such as the internet and other less sensitive networks. By tailoring network segregation to limit network usage to the strict minimum, and placing applications / servers in different network zones dedicated for their specific use only, it becomes more difficult for threat

[36] Standard Club (2020): Maritime Cyber Risk Management Guidelines
[37] Wikipedia (2022): Multi-factor authentication. https://en.wikipedia.org/wiki/Multi-factor_authentication
[38] Gentec (2022): What is encryption and how important is it? https://www.genetec.com/blog/cybersecurity/what-is-encryption-and-how-important-is-it
[39] Code Signing Store (2022): Code Signing Helps Get Rid of Hidden Cybersecurity Threats. https://codesigningstore.com/code-signing-to-stay-away-from-cybersecurity-threats
[40] Digicert (2022): Code Signing certificate. https://www.digicert.com/signing/code-signing-certificates

actors to work their way laterally through the network, even if they have penetrated the system.[41]

- *Network segmentation:*
  splits a larger network in to smaller segments—also called subnets—usually through switches, routers, firewalls and VLAN's.

- **Patching**
  Software update for an existing application or operating system to resolve bugs (errors) or vulnerabilities [42]

- **Virtual Private Network (VPN)**
  VPN connections allow organisations encrypted virtual access to the internal network from outside. It is a network service that is secured by two factor authentication (2FA) and data encryption.

- **IP address**
  - IP banning/blocking is a configuration of a network service that blocks requests from hosts with certain IP addresses. Applying this countermeasure enables organisations to restrict access to or from certain geographical areas, for example. [43]
  - By hiding (translating) the IP address, search engine traffic remains anonymous, increasing an organisations privacy and security.

- **Software Whitelisting**
  This is the practice of specifying an index of approved software applications or executable files that are permitted to be present and active on a computer system. The goal of whitelisting is to protect computers and networks from potentially harmful software.

- **Access and user control lists**
  - Access Control Lists (ACL) "is a list of rules that specifies which users or systems are granted or denied access to a particular object or system resource. ACLs are also installed in routers or switches, where they act as filters, managing which traffic can access the network." [44]
  - Hardened critical equipment can limit the escalade of privileges.

- **Wireless access control**
  It should be ensured that only approved devices have access to the networks. In addition, wireless access should be secured by a strong encryption key, that is changed regularly. [32]

- **Email and web browser protection**
  The aim is to ensure, among other things, that (a) staff are protected from potential social engineering attacks, (b) that email clients and web browsers prevent sensitive information from being accessed, (c) that the exchange of sensitive information via email is sufficiently protected (e.g. by encryption protection) and (d) that web browsers and email clients prevent malicious scripts from being executed.

- **Honeypots**
  Simulated computer systems are placed like a dummy as worthwhile targets for cyberattacks. As soon as hackers try to penetrate the systems, the honeypot collects information on the

[41] Parallels (2022): A Complete Overview of Network Segregation and Why It's Crucial for Your Organization. https://www.parallels.com/blogs/ras/network-segregation/
[42] Myra (2022): What is a patch? https://www.myrasecurity.com/en/what-is-a-patch/
[43] Wikipedia (2022): IP address blocking. https://en.wikipedia.org/wiki/IP_address_blocking
[44] TechTarget (2022): access control list (ACL). https://www.techtarget.com/searchnetworking/definition/access-control-list-ACL

cyber criminals and their methods by analysing the penetration attempts or tries to distract them from other targets. [45]

- **Intrusion Detection System (IDS)**
  IDS detects cyberattacks, and documents them in log files that are reported to the administrator. They can either supplement the firewall or run directly on the computer system to be monitored. [46]

- **Intrusion Prevention System (IPS)**
  Compared to an IDS, the IPS not only detects cyberattacks, but also provides functions that can automatically and actively defend against detected attacks. [47] For example, IPS monitor network traffic to detect anomalies in traffic flow, intercept deviant network traffic and can quickly prevent malicious activity by dropping packets or resetting connections.

- **Intrusion Response System (IRS)**
  "The purpose of an IRS is to automatically identify the proper response to an ongoing attack, usually exploiting additional knowledge of the behaviour of the attacker and of the protected system." [48]

- **Security Orchestration, Automation and Response (SOAR)**
  Several combined software programs enable an organisation to collect data on security threats and respond to security events without human assistance. Thereby, SOAR enables organisations to improve the efficiency of physical and digital security operations.
  The name of SOAR platforms is derived from the 3 main components: security orchestration, security automation and security response. This allows cyber incidents to be detected more quickly and response times to be shortened accordingly, as well as providing a better threat context as a wider range of data is analysed. [49]

- **Security Information and Event Management (SIEM)**
  - It is a security solution that helps organisations detect potential security threats and vulnerabilities by collecting and analysing log events - both near real time and historical. [50] [51]

7.3.3 Physical controls

Physical controls are probably the most obvious and - depending on the execution - also the simplest and cheapest form of cyber defence. In particular, areas with sensitive control systems and/or data should be securely locked and protected from unauthorised access[32], e.g. by

- Fences
- Gates
- Locks
- Locked and dead-bolted steel doors

[45] Kaspersky (2022): Was ist ein Honeypot? https://www.kaspersky.de/resource-center/threats/what-is-a-honeypot
[46] Wikipedia (2022): Intrusion Detection System. https://de.wikipedia.org/wiki/Intrusion_Detection_System
[47] Wikipedia (2022): Intrusion Prevention System. https://de.wikipedia.org/wiki/Intrusion_Prevention_System
[48] Cardellini V. et al. (2022): An Intrusion Response System utilizing Deep Q-Networks and System Partitions. https://arxiv.org/pdf/2202.08182.pdf
[49] TechTarget (2022): SOAR (security orchestration, automation and response). https://www.techtarget.com/searchsecurity/definition/SOAR
[50] Gartner Glossary (2022): Security Information And Event Management (SIEM). https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem
[51] IBM (2022): What is SIEM? https://www.ibm.com/topics/siem

- Biometrics
- Picture IDs
- Security Guards (a person employed protecting an organisation's assets)
- Closed Circuit Television Cameras (CCTV) / closed-circuit surveillance Cameras
- Motion or thermal alarm systems

7.3.4 Layered defence approach

Layering is another protection mechanism. This involves the simultaneous application of several security measures - i.e. several layers of protection - in order to increase the security of the IT/OT systems etc. to be protected. This layering ensures that even if one layer of protection fails to prevent a threat, the other layers are still in place to help prevent a breach in the system. In doing so, each layer of protection protects the system from a specific threat. Using this layering approach, a so-called defence-in-depth strategy is developed.
For example, endpoint detection and response solutions are great at preventing viruses and malware from infecting computers and servers. However, endpoint detection is not equipped to log and monitor traffic on a network like a SIEM, or detect and prevent an attack in real-time like an IPS. Consequently, it is worthwhile to apply several protective mechanisms simultaneously and in a superimposed manner.

"The defence in depth approach encourages a combination of:

- physical security in accordance with the organisation's security plan
- protection of networks, including effective segmentation
- intrusion detection
- use of firewall
- periodic vulnerability scanning and testing
- software whitelisting
- access and user controls
- configuration and change management controls
- appropriate procedures regarding the use of removable media and password policies
- personnel's cybersecurity awareness and understanding of the risk to themselves and the industry
- understanding and familiarity with appropriate procedures, including incident response." [32]

A complementary approach to the defence-in-depth strategy is the defence-in-breadth strategy. This approach is intended to ensure the cybersecurity of an organisation at the application level, i.e. within a layer. The above-mentioned protective measures are thus applied layer by layer to all vulnerable and integrated systems. [32]

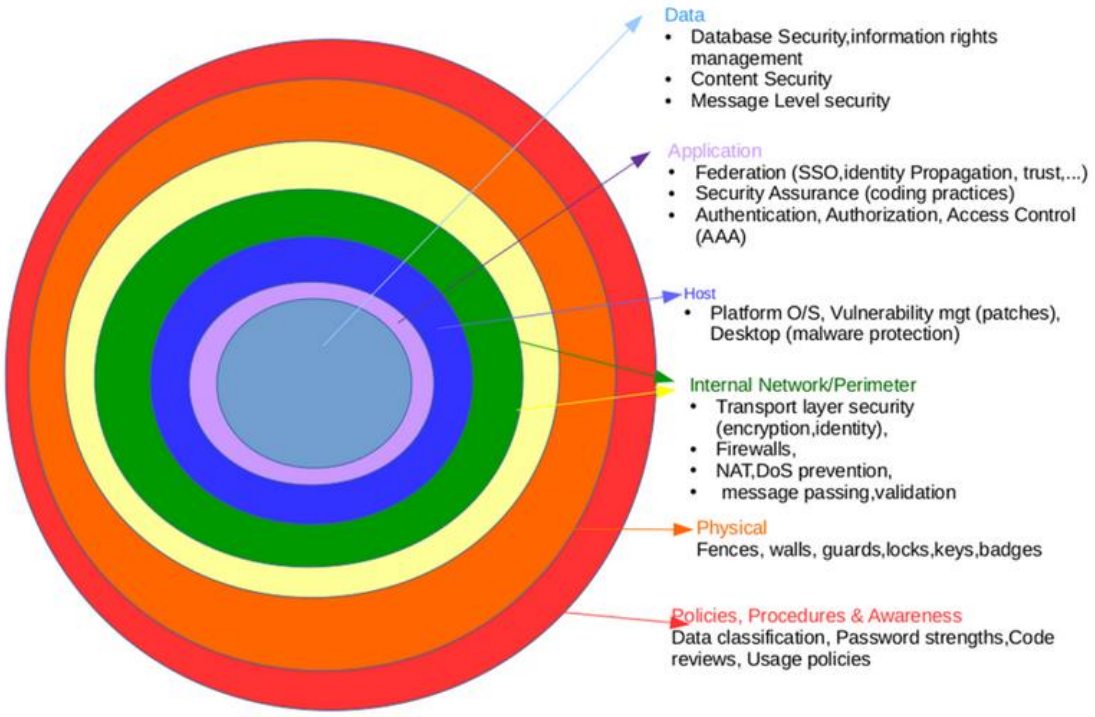


Figure 22: Graphic representation of the defence-in-depth strategy [52]

7.3.5 System administrator dilemma

The system administrator dilemma is the conflict between the implementation costs of certain countermeasures and the desired level of security and the corresponding search for the optimal trade-off. The better and more numerous the protective measures, the higher the costs that have to be incurred. In order to find an appropriate level of protection mechanisms for the identified cyber threats, the risk assessment that was carried out, in which priorities of the threats to be defended were also established, serves as a basis. Based on this, the system administrators or cybersecurity management team must find the optimal trade-off between the implementation cost of a specific countermeasure and the overall security level of the system.

[52] Purplebytes (2017): Defence in Depth and Breadth – The new approach. https://www.purplebytes.co.uk/blog/2017/11/21/defence-in-depth-and-breadth-the-new-approach

8 Inventory on cyber risks in IWT

8.1 Introduction

During the study of the different sub activity's within DIWA we compiled a list of possible cyber risks. This list is extended with possible cyber risks found in other related projects. This list mainly focuses on the cyber risks clearly related to IWT. The "classic" or already commonly known cyber risks such as "weak passwords", "default admin passwords", issues related with cloud technology, … are not mentioned here as we believe that these risks are already handled/described in quite some detail in other projects and studies. Furthermore the implementation of an ISMS, as discussed in chapter 6.6, covers these topics extensively.

We also want to stress the fact that the provided list of cyber risks is certainly not complete. Beside the known risks, other risks can indeed materialise that are not within the awareness of an organisation, so called unknown unknowns. In order to respond effectively to these unknown unknowns, organisations should remain curious about new evolutions and continuously monitor their situation, plan for uncertainty and remain flexible and open to change to respond to unexpected events. Also, information about risk can be asymmetric, e.g. in closed software/hardware implementations where only the supplier has the inside knowledge. These risks can't always be identified by outsiders.

8.2 Used sources

This sub chapter contains input from other DIWA Activities concerning cybersecurity. During the previous Sub Activities questions were raised related to cybersecurity. A summary of this is given in the next paragraph.
Also input from two specific IWT cyber security related reports are given here. These are drafted by CESNI and PIANC.
Some lessons learned from the RIS COMEX Project and the realisation of the EuRIS portal are included in the last paragraph of this sub chapter.

8.2.1 Input from other DIWA Activities

8.2.1.1 Smart shipping (SuAc 2.1)

Sub-Activity 2.1 identifies the increased cyber vulnerability due to increasing connectivity between (vessel)systems and infrastructure. For the upcoming years (semi)autonomous vessel operation is envisioned to require secure communication and cybersecurity protection ingrained in all related soft and hardware systems.

A set of questions specifically for Sub-Activity 4.3 to address consists of:

- What can authorities do to reduce vulnerability?
- What kind of conditions related towards cybersecurity should be taken into account when giving permission automating on board of a ship?
- What kind of responsibility does an authority have regarding cybersecurity of (autonomous) vessels?

8.2.1.2 Synchromodality (SuAc 2.2)

No mentioning of cybersecurity except the statement of France: "The ambition of the government is to implement a new security system, based on blockchain technology."

8.2.1.3 Port & terminal information service (SuAc 2.3)

The need for state-of-the-art cybersecurity measures and safeguards is recognised for digitalisation to be successful.

8.2.1.4 RIS enabled corridor management (SuAc 2.4)

Sub-Activity 2.4 states that data security is of utmost importance for RIS as many data is exchanged internationally. Data security has high priority in order to maintain the trust in RIS by the users.

8.2.1.5 Intelligent Transport Systems (ITS), European Rail Traffic Management System (ERTMS), E-navigation (SuAc 2.5)

It is stated that the future concept of RIS not only depends on the revision of the RIS Directive but also on transversal topics such as automation of inland navigation and cybersecurity.

While activity 3 Sub-Activities are still under way at the time of writing, several preliminary results are already available for Sub-Activity 4.3 to take into account.

8.2.1.6 New technologies (SuAc 3.1)

The report urges to ensure: "Compliance with data security policies (like e.g., GDPR)" in public-private partnerships and mentions security in relation to blockchain.
Big Data is listed as a promising new technology. There is no cybersecurity use case in the report regarding Big Data, however identifying patterns is one of the functionalities associated with Big Data technologies.
This provides new opportunities for cybersecurity in IWT, e.g.: Collecting IT-network traffic from locks and bridges to establish a baseline "normal". Perform real time monitoring of IT-network traffic against this baseline to detect hacking attempts.
A similar approach could be taken for AIS to detect spoofing.

Questions/statements specifically for SuAc 4.3:

- Compliance with data security policies (eg GDPR) in public-private partnerships are of importance
- Big data: potential solution in identifying patterns in IT networks/real time monitoring (e.g. AIS network, lock/bridge facilities)?

8.2.1.7 IWT connectivity platform (SuAc 3.2)

When discussing platforms such as EuRIS and eFTI, cybersecurity is seen as an important characteristic of connectivity platforms.

Questions/statements towards SuAc 4.3:

- Privacy by design as principle for connectivity platforms like EuRIS or eFTI.

8.2.1.8 Smart sensoring & PNT (SuAc 3.3)

Possible privacy issues related to a variety of smart sensors are listed by Sub-Activity 3.3, recognising the need to secure captured data. In addition, cybersecurity vulnerabilities and associated risks concerning the use of AIS for PNT and smart sensors in general are briefly described. Sub-Activity 4.3 is expected to delve deeper into these topics and integrate them in the larger IWT cybersecurity subject.

Several recommendations regarding cybersecurity are put forward:

- REC 4: Cybersecurity measures should not merely be applied to the smart sensor. Applications connected to the Smart Sensors or applications using the data of these sensors must also comply with appropriate cybersecurity measures. (It's proposed to consider this in SuAc 4.3) (cfr. 7.3 - Cybersecurity)

- REC 5: When introducing a new sensor on a vessel, it becomes part of a larger network of sensors and applications. The security aspect should be revised to ensure the safety of the

complete network. (cfr. 7.3.3 - Awareness and risk mitigation)

- REC 11: Investigate the need of a security policy for vessel operators (dos and don'ts regarding IT and Data). This could also be demanded by authorities.

Questions/statements specifically for SuAc 4.3:
Cybersecurity should not merely be applied to the smart sensor. Applications connected to the Smart Sensors or applications using the data of these sensors must also comply with appropriate cybersecurity. How can a proper use of the data be ensured?

8.2.1.9 Information model & data registry (SuAc 3.4)

The report did not raise any questions related to cybersecurity nor did it contain any recommendations in this regard.

8.2.1.10 Technology in other transport domains (SuAc 3.5)

Sub-Activity 3.5 identifies adoption of the Maritime standard for secure communications (EN IEC 63173-2 SECOM) as an opportunity for an IWT connectivity platform to provide services via secured data link.

Recommendations/questions specifically for investigation by 4.3:

- Study-REC-SECOM-Impact-1: Study potential impact on IWT Fairway & Navigation in general, and on the ICT infrastructure of authorities in particular of the large-scale introduction of EN-IEC63173-2 (SECOM) as a correlate development with S-100 framework. --- to Sub-Activity 4.3 regarding Cybersecurity issues

- Study-REC-Application-of-SECOM-For-ROV: As motivated in Study-REC-SECOM-Impact-1 and as additionally motivated by pending ISO considerations to use SECOM standard for Remotely Operated Vessels. --- to Activity 4.3 regarding Cybersecurity Issues.

8.2.1.11 Conclusions Summary on input from other activities

Summarised conclusions from other DIWA Sub-Activities:

- Cybersecurity is valued as a very important element of digitalisation.
- Few specific cybersecurity risks are recognised (only by Smart Shipping and Smart sensors & PNT)
- This limited and mainly technical coverage of cybersecurity is cause for concern.
- Content and recommendations of activity 4.3 should strive to raise awareness of the broader scope (beyond pure technical) of cybersecurity and provide actionable advice to reduce cyber vulnerability of IWT across this broader scope
- Fairway authority mandate might need to be extended beyond the technical equipment requirements of a vessel to the cyber resilience of the vessel and the vessel operator.

8.2.2 CESNI & PIANC reports

For the compilation of the inventory, among others, two relevant reports from PIANC and CESNI were consulted, the contents of which are summarised below. For further information, we recommend consulting the reports themselves:

1) CESNI (2023): Good practice Guide on Cybersecurity in Inland Navigation – Especially for ports
2) PIANC (2019): Awareness paper on cybersecurity in inland navigation

8.2.2.1 CESNI – Good practice Guide on Cybersecurity in Inland Navigation[53]

Although the CESNI report focuses on the cybersecurity of Inland Water Ports, many of the topics mentioned in it can also be applied to inland navigation in general.

Cybersecurity threat landscape of inland ports

The report begins with an asset assessment of inland ports and points out that even before identifying threats, organisations should first be aware of which assets need to be protected. It also points out that the assets to be protected or their prioritisation may vary from organisation to organisation.

Inland port assets	Vessel assets
• Vessel reception and docking • Container storage and staying • Security and safety • Support service • Distribution service • Authorities and customs • Vessel berthing • Energy service • Lock Bridge Management (LBM) systems • IT systems involved in traffic planning, such as a Vessel Traffic Service (VTS) • Passenger and tourist barge system	• River Information Services (RIS) • Machinery • Cargo • Business assets • Communication and crew technology

Considering the cybersecurity attributes that inland ports have to fulfil according to CESNI *(Confidentiality, Integrity, Availability, Possession)*, a taxonomy for cyber threats as well as the analysis of potential impacts for inland ports was finally created. According to CESNI, threats can be identified by correlating vulnerability and malicious actor motivation. Consequently, potential threat actors and their motivations for a cyberattack are listed.

Threat taxonomy	Potential impacts
• Failures, malfunctions • Physical attacks • Eavesdropping, interception, hijacking • Information spoofing or jamming • Disaster • Outages • Unintentional damage	• Reputational impact • Financial loss • Regulatory sanctions • Destruction of property • Human loss or injury • Criminal activities: fraud, illegal trafficking • Theft of property • Environmental disaster

Furthermore, the report lists three selected scenarios of threats related to cybersecurity and Inland water ports that have occurred in recent years. In addition, the report lists the key steps of a wide variety of cyberattacks.

a) **Infiltration of control systems to operate machinery**: In 2013, two hackers infiltrated the control systems of a small dam in New York state [54]
b) **Compromising data to facilitate illicit drugs smuggling**: Hackers gained access to, and thus control of, the container terminal computer, allowing them to tag and track containers of their illicit drugs.
c) **Jamming of AIS equipment**: In 2017, at least 20 vessels in the Black Sea reported that their AIS showed their position at a location 30 kilometres inland [55]

Mitigating cybersecurity risks for inland ports

[53] CESNI (2023): https://www.cesni.eu/wp-content/uploads/2023/05/Guide_cybersecurite_en.pdf#search=%22good%20practice%20guide%20on%20cybersecurity%20in%20inland%20navigation%22

[54] U.S. Department of Justice: https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.

[55] https://www.ship-technology.com/features/ship-navigation-risks/

In the chapter on mitigating cybersecurity risks for inland ports, an overview of legislation and policies relevant to the inland port context is first provided.
Subsequently, possible mitigation measures are listed, which have been divided into three sections:

1) Organisation Policies and Procedures
2) Information Technology / Operational Technology Policies for Inland Ports
3) Technical Security Measures for Inland Ports

In the context of this summary, only the generic terms are listed, under which detailed measures are listed in the CESNI Report. Please consult the CESNI Report to get an insight into the detailed measures.

Organisation Policies and Procedures	**Information Technology / Operational Technology Policies**	**Technical Security Measures**
• Roles and responsibilities • Organisational processes • Physical security • Incident response and crisis management • Training and awareness	• IT/OT general responsibilities • Identity and access management (IAM) • Maintenance and operations of IT/OT systems • Technical security measures for IT/OT systems • Monitoring IT/OT systems • Incident response and crisis management for IT/OT systems • Securing navigation systems	• Identity and access management (IAM) • Operations security • Network security • Data protection • Vulnerability management and systems monitoring

The measures listed in the report are classified into three different categories of security posture (low, medium, high target maturity posture) in a clear matrix at the end of the report.

Furthermore, 3 additional case studies have been included in this chapter, one on "Employee awareness programs", as well as "building a cybersecurity risk assessment" and "protection of container terminals".

Finally, a maturity evaluation framework is proposed.

8.2.2.2 PIANC (2019): Awareness paper on cybersecurity in inland navigation

This paper focuses on specific risks in the inland navigation transport sector and thus covers the areas of ships, waterways, ports, shipping companies and cargo, linked by ICT services (such as RIS). Compared to the CESNI report, this paper aims to build an appreciation of the salient issues being discussed in the industry, rather than an inventory of technologies, threats and mitigation measures.

In a first step, the paper shows that the basic cyber preparedness across industry is very low and emphasises that there is no global standard for cybersecurity. As a result, many organisations and governments do not have a cybersecurity strategy. In particular, the shipping industry is clearly behind the others in terms of cybersecurity - awareness regarding cybersecurity is rated as low.
It was found that especially (a) the high complexity of information & communication technologies (ICT), which are very often used in the shipping sector, as well as (b) the use of industry-specific technologies, (c) the long life in service of vessels and the associated constant replacement of only parts of the onboard systems and (d) the complexity of multiple, interconnected systems on board ships represent a challenge for cybersecurity.
Furthermore, the complexity of shipboard systems (d) makes risk patterns difficult to identify. In addition, the dispersed governance / regulation on different levels (i.e. international, European, national) makes a common approach to cybersecurity difficult.
The paper highlights that rising concerns about data protection continue to increase the necessity and urgency of implementing measures against cyber risks.

Before discussing systems that are currently used in shipping and their issues and specific countermeasures to address potential cyber risk, the paper lists general aspects of risk mitigation, such as (a) adequate procedures for assessing systems, system risks and establishing mitigation procedures (incl. staff training), (b) establishing IT industry-standard security countermeasures, (c) segregating safety-critical equipment from other on-board systems and communications, (d) monitoring data activity, (e) cyber hygiene and reporting and sharing of cyber incidents are further mentioned.
As mentioned before, the report then lists systems that are currently used in shipping such as:

- vessel control systems (e.g. SCADA)
- navigation (GNSS, AIS, ECDIS, Radar, ERI & NtS, Web/Database Servers)
- infrastructure control systems (River Infrastructure Systems, e.g. Lock and Bridge Management (LBM), Traffic Planning)
- information reporting/exchange
- network infrastructure/communication systems (On-Board LAN / other networks, bespoke industry web portals, distributed devices)

Problems regarding their use and cybersecurity and possible mitigation measures are identified and discussed. In addition, various case studies are also included in this paper.

Finally, the report gives an insight into possible future technologies and risks. Under the topic of automated / autonomous vessels, an insight into the NOVIMAR Platoons[56] is given. Furthermore, Digital Inland Waterway Area and Digital Multimodal Nodes are explained.
As future risks, the report mentions that an increase in attacks on SCADA networks is to be expected in the future. However, with adequate training of personnel, the risk can be significantly mitigated.
The increase in the use of automated systems also exposes the sector more and more to cyberattacks. Experiences from the road sector show that the establishment of comprehensive cybersecurity principles is necessary.

8.2.3 Input from COMEX (CA1, CA2, …..) and EuRIS (cybersecurity)

Within the RIS COMEX project a lot of work was done by privacy related and legal experts to draft the core agreements 1 and 2 (CA1 and CA2) regulating the information exchange between COMEX Partners and the users.

[56] https://novimar.eu

These agreements stress the need for privacy. The solution is built with the principle "Privacy by Design". The data needed to be classified within several classes:

- Not privacy sensitive
- Normal sensitive: position of inland vessels, travel destinations and ETA, personal accounts, …
- High sensitive (medical, religion, sexual preference, ….) -> no high sensitive data is handled or stored within EuRIS.

The provided solution also had to be GDPR compliant. The related recommendations were applied. During the realisation of RIS COMEX a Data Protection Impact Assessment (DPIA) was executed. This contained a risk assessment, an inventory of involved data and assets and an overview of planned or existing measures.

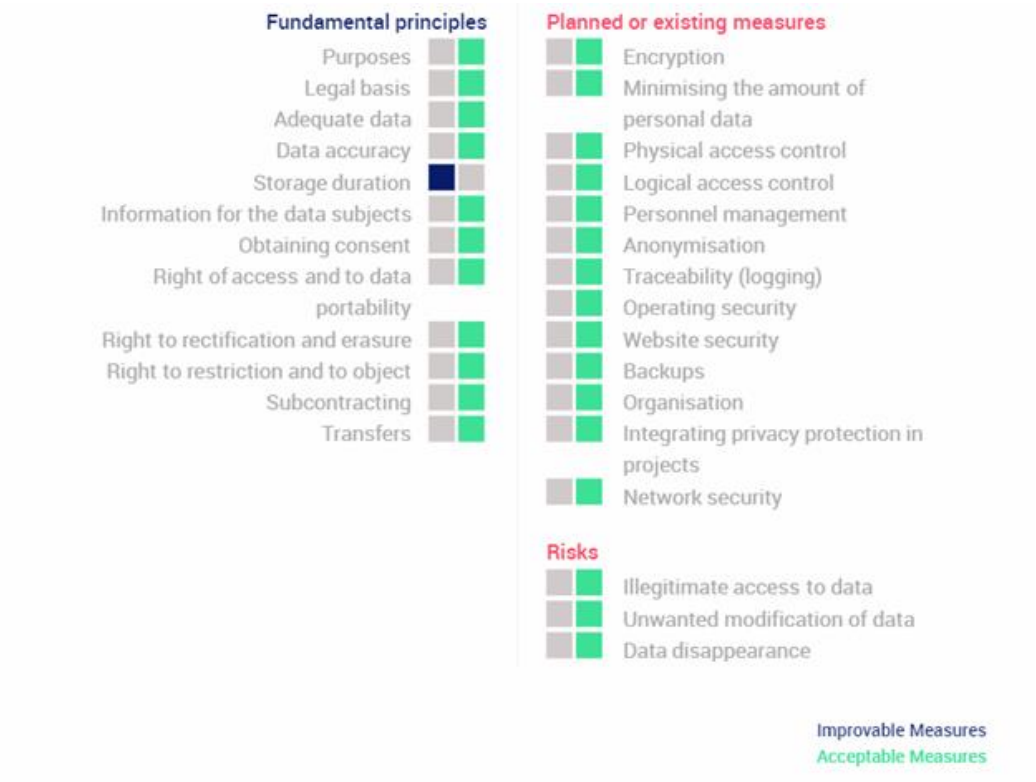


Figure 23: Planned and existing measures RIS COMEX

Several technical and organisational measurements had to be taken:

- Confidentiality
  - Entry and access control
  - Data classification scheme
  - Data anonymisation
- Data integrity
  - Control of data transfer
  - Data entry control
- Availability and resilience
  - Availability control
  - Rapid recoverability
  - Deletion of person-related data
- Procedures for regular testing, assessing and evaluating
  - Data protection management including regular employee training
  - Incident-response management
  - Data protection by design
  - Data processing control

Two limited risks related to 'Illegitimate access to data' were detected, and measures to reduce them were drafted. These measures were brought into practice in 2021. One limited risk related to 'Unwanted modification of data' was detected. This risk is, however, inherent to the use of AIS in Inland Waterway Transportation, and sufficient measures (encryption, minimizing the amount of personal data collected, traceability, security by design, data validation checks) are already in place to reduce its risk and impact to a minimum.
The life cycle of data and processes is documented in the DPIA. In EuRIS there is a strong ownership of data implemented. Individuals owning data can decide with whom and for how long to share the data. They have the tools to see who has access and to revoke this access. There is a concept called privacy classes with determines how much data can be seen by another person. AIS related information is not permanently stored. Derived information from AIS for statistics is pseudo-anonymised. Voyage related information is stored for a short time period and purged automatically.

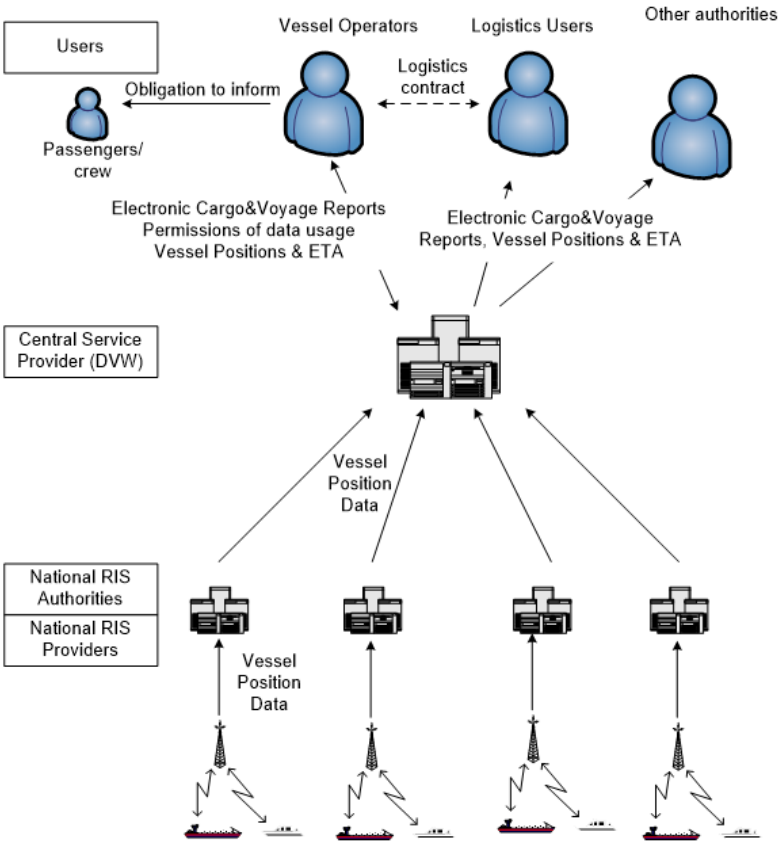


Figure 24: Schematic representation of EuRIS data exchange

Functionality to delete a user account and to retrieve data is foreseen and available in EuRIS. The data subjects are given insight in the information that is processed by means of the Privacy Policy and Terms & Conditions on the website.

In order to mitigate several cyber risks within EuRIS a lot of actions were taken: Scanning functionality provided by the hosting partner was activated. This is a scanning tool which scans for the application of recommendations from different security related standards such as ISO 27001 (version from 2013).

A strong focus on network security was foreseen. A Layer 3 firewall[57] with Intrusion Detection capabilities is used to screen incoming and outgoing traffic. Several malware use an outgoing connection to receive remote control commands or download additional payload. These connections can thus be blocked if they use uncommon ports or unknown IP addresses. A Layer 7 web application firewall is used to clean incoming web related traffic. Several commonly used attacks can be blocked

[57] Layer 3 firewalls are also commonly referred to as network layer firewalls. They operate at the third layer of the Open Systems Interconnection (OSI) model, which is the network layer. This layer is responsible for routing and forwarding of data packets between different networks.

such as SQL injection attacks, cross site script attempts, usage of known exploits (log4j), …. All resources are deployed in different network zones. There are boundaries between environments: production, acceptance and test. There are also boundaries between resource roles (layers) like web, app, storage, … related services. A hub and spoke model is applied where all incoming and outgoing traffic is routed through a central hub. The different environments but also the connected partners via a VPN tunnel are considered as the spokes.

In order to maintain a high availability of the environment the supplier has chosen for components with a high SLA (99,9% or higher). On back-up level there is a differentiation made between data and infrastructure (virtual machines, applications, …). These datasets are backed up with a different interval where the data has the highest interval. Regular data snapshots are taken allowing point in time recovery. Redundancy is also foreseen. The deployment of the virtual machines and applications has been automated through the usage of DevOps principles. The infrastructure configuration is treated as code and the related configuration/deployment scripts are stored in a GIT repository (infrastructure as code principle). This allows for an easy upgrade and redeployment of machines making sure that the latest versions of operating systems and middleware are used. The time needed to deploy a machine from scratch is quite short this way.

A modern anti malware product has been deployed on all related virtual machines. This also contains intrusion detection and vulnerability scanning. These scan results are used to further harden the provided operation system configurations (although software vendors should really consider to make sure that a basis fresh install is already hardened). A vulnerability scanning tool is also foreseen on database level. Possible exploits are identified. In order to provide a highly patched environment the supplier has automated the patching of several resources. The virtual machines are daily (working days) patched using the combination of an orchestration tool and monitoring. If alerts are detected then the patches won't be deployed to the next environment (test -> acceptance -> production).
Used certificates are centrally managed in a key vault. There is an auto renewal process in place with a high frequency (certificates are renewed each 3 months). Sensitive data is encrypted in transit and at rest where feasible.

A central modern authentication platform is used to provide standardised authentication methods such as OAuth V2. Multi factor authentication is required for all persons with administration privileges. The platform uses policies to determine access to the environment. These policies also use conditional access and risk detection. Example: A user logging in simultaneously from two different countries is deemed as a high risk user. The least access privilege principle is applied and a regular screening of the membership of high privileged roles is executed.
Single sign on for application access is foreseen in order to strengthen the security management. Access to the test and acceptance environment is regulated by an additional login using a proxy in front of these environments.

8.3 Vessel related

8.3.1 Position information

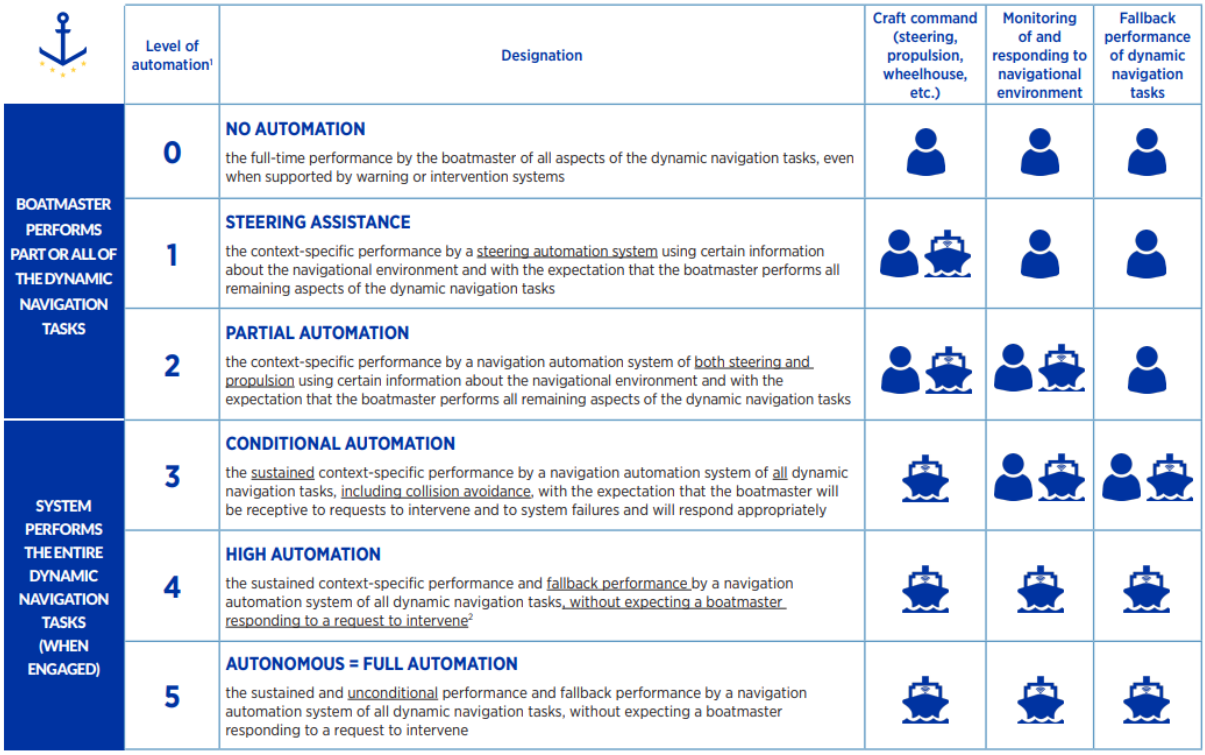
GPS information can be spoofed or manipulated to give wrong location information. This was already done in the Black Sea incident where the position of vessels was shifted[58].

Falsified position information can lead to interruptions in vessel transport and maybe even causing a vessel collision or grounding, especially in the case of automated navigation. Waterway related authorities can also be hindered in their operations: sending inspection crews to wrong locations, making bad decisions about voyage intentions and object scheduling, …

[58] See scenario 3 – Jamming of AIS equipment described in the report „Good Practice Guide – Cybersecurity for Inland navigation – Especially for ports"

8.3.2 Automated navigation

The Central Commission for the Navigation on the Rhine (CCNR) has defined several levels of automation in inland navigation. Currently, there are a lot of initiatives on regarding all levels to provide autonomous navigation. With the level of increasing automation, the number of cyber risks and their potential impact also increases.



	Level of automation[1]	Designation	Craft command (steering, propulsion, wheelhouse, etc.)	Monitoring of and responding to navigational environment	Fallback performance of dynamic navigation tasks
BOATMASTER PERFORMS PART OR ALL OF THE DYNAMIC NAVIGATION TASKS	0	**NO AUTOMATION** the full-time performance by the boatmaster of all aspects of the dynamic navigation tasks, even when supported by warning or intervention systems			
	1	**STEERING ASSISTANCE** the context-specific performance by a steering automation system using certain information about the navigational environment and with the expectation that the boatmaster performs all remaining aspects of the dynamic navigation tasks			
	2	**PARTIAL AUTOMATION** the context-specific performance by a navigation automation system of both steering and propulsion using certain information about the navigational environment and with the expectation that the boatmaster performs all remaining aspects of the dynamic navigation tasks			
SYSTEM PERFORMS THE ENTIRE DYNAMIC NAVIGATION TASKS (WHEN ENGAGED)	3	**CONDITIONAL AUTOMATION** the sustained context-specific performance by a navigation automation system of all dynamic navigation tasks, including collision avoidance, with the expectation that the boatmaster will be receptive to requests to intervene and to system failures and will respond appropriately			
	4	**HIGH AUTOMATION** the sustained context-specific performance and fallback performance by a navigation automation system of all dynamic navigation tasks, without expecting a boatmaster responding to a request to intervene[2]			
	5	**AUTONOMOUS = FULL AUTOMATION** the sustained and unconditional performance and fallback performance by a navigation automation system of all dynamic navigation tasks, without expecting a boatmaster responding to a request to intervene			

[1] Different levels of automation may make use of remote control but different conditions to be defined by competent authorities might apply in order to ensure an equivalent level of safety.
[2] This level introduces two different functionalities: the ability of "normal" operation without expecting human intervention and the exhaustive fallback performance. Two sub-levels could be envisaged.

Figure 25: Levels of automation in inland navigation

To provide some support for automated navigation track pilot devices or TGAINs (Track guidance assistants in Inland Navigation) were introduced. A track pilot or TGAIN is an automated course system which can steer a vessel on a beforehand configured track line (level 1 of automation) or steer the vessel and control the propulsion (level2 of automation).. The automatic steering of the vessel is controlled by the software of the track pilot. It makes the navigation less intensive and fewer steering commands are needed. The responsibility still lies fully with the skipper. These devices rely on a hardware/software combination. If the system is inadequately protected these systems can be vulnerable to attacks. Some suppliers even requests to disable automatic updates of the computer. This can lead to missing security updates further increasing the risk.
A track pilot or TGAIN could also give a false sense of security because the track pilot doesn't know the intentions of other skippers, doesn't take in account the objects, depth restrictions, water flows, vessel height, …. Indeed, track pilot or TGAIN may be equipped with a collision warning but a TGAIN has no function to avoid a collision.
Track pilots depend on the correctness of inland AIS position information to steer the vessel. Some track pilots also use AIS information to provide AIS-based collision warnings along the guiding line. This dependency makes them susceptible to attacks using spoofed AIS position information

All these connections between the different devices are most of the time using serial or TCP/IP communication in combination with the NMEA 0183 protocol. This protocol uses plain text commands and is easy to manipulate. These kinds of connections are not protected and could be manipulated by a man in the middle attacks or falsified connections could be set up. These systems could be used to ground vessels or to setup collisions.

In the next paragraphs we discuss some examples of the risks associated with automated navigation. Recently, experiments have been conducted regarding intention sharing between vessels via the exchange of track pilot tracks[59]. When providing intended short term course and route towards and between nearby vessels, skippers are expected to gain a better situational awareness without having to resort to coordination via VHF communication. Especially when navigating in busy areas with limited or obstructed line-of-sight, having an indication of the intended course of vessels in the vicinity is expected to improve safety. Since this entails digital information exchange which, when manipulated, could cause serious damage (tricking skippers into thinking that their vessels can pass each other safely while in actuality they are on a collision course) it is important to protect this exchange against (cyber) interference. Care should be taken to protect the communication data link from manipulation of the data in transfer and guarantee the validity of the originator and recipient.
The technology is still in development and therefore offers the opportunity to be engineered (cyber)secure-by-design. This should be encouraged by authorities and possibly required to be demonstrated by suppliers before being allowed to be used operationally on inland waters.

Within the project NOVIMAR[60] between 2017 and 2021 several studies and pilots were executed on the concept of vessel trains. In the NOVIMAR vision, waterborne transport operations on short-sea, sea-river and inland waterways can be performed by Vessel Trains. Such a Vessel Train consists of a Lead Vessel and a number of Follower Vessels, remotely controlled from the Lead Vessel and having a reduced crew. See Figure 26 for the concept.

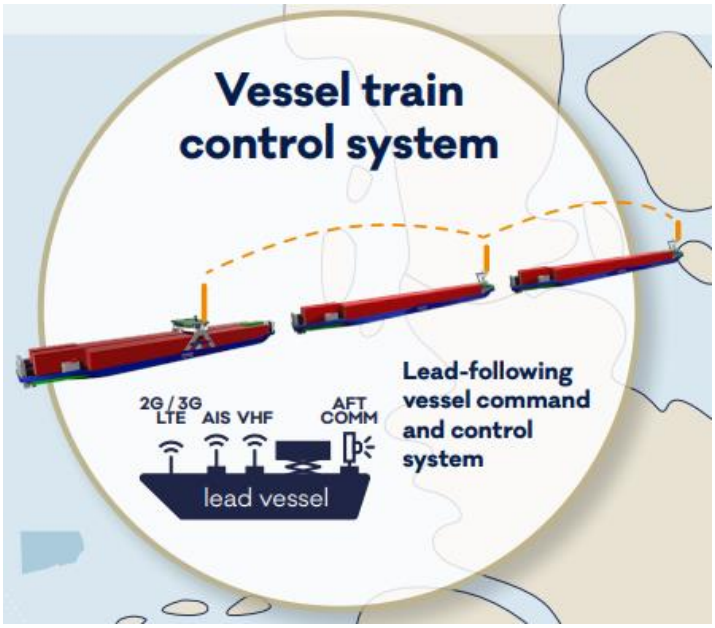


Figure 26: Vessel train control system (source NOVIMAR)

Within this concept of Vessel Trains several communication systems like mobile data (2G/3G LTE, AIS, direct WIFI and VHF are used. If the communication protocols aren't sufficiently protected this could also lead to cyber risks in which vessel controls can be hijacked.
The NOVIMAR project made a safety and cybersecurity assessment in work package 5 – Safety Issues and human skills. A summary of this has been proved in the deliverable 5.3 – Safety and Cybersecurity Assessment[61]. The research showed that the vessel train control system can be exposed to external and internal attacks. Some vulnerabilities were identified like spoofing GNSS, AIS, Radar and the direct wireless communication system. This latter system is deemed as the most critical one because of the possible impact. The source of the internal attack would be a human having physical access to the systems.

[59] RWS (2022): https://open.rws.nl/publish/pages/8711/intention_sharing_simulator_study_final_4.pdf
[60] Novimar.eu
[61] Novimar (2022): https://novimar.eu/wp-content/uploads/2021/09/Deliverable-5.3.-public-summary.pdf

The assessment was performed using the Cyber Risk Analysis Flow Methodology steps 1 and 2 of the role note NR 642 – Cybersecurity Requirements for Products to be Installed On-Board Naval Ships provided by Bureau Veritas[62]. In the assessment recommendations are made for the architecture and installation of a vessel train control system.

8.3.3 Privacy

To support automated navigation additional devices like cameras and microphones (active sound monitoring) are used (and recorded). Microphones and speakers are used to communicate with persons around the vessel and for monitoring the sound of the vessel itself. If the data is wrongly accessed this can lead to several privacy related issues.

Another privacy risk is when the information of AIS transponders is combined with other data sources. With this combination of data, one is able to determine where identifiable persons are. The use of personal identifiable information (PII) necessitates adherence to the GDPR. This is also mentioned in the DIWA report SuAc 3.3 – chapter 7.2.

Special consideration should be given also to the decommissioning of vessels and systems on board of them. There is often still data on board which could be recovered (e.g. voyage logs).

8.3.4 Vessel takeover

In case of automated navigation, the remote control of a vessel can be hijacked leading to the takeover of the vessel. This vessel can then be used to perform criminal or terrorist activities having potentially huge impacts such as:

- Collision with other vessels or objects
- Destabilisation or sinking of vessels
- Explosions, fires, leaks and damage to cargo or vessels
- Loss of lives
- Pollution

In this context the cyber resiliency of remote control centres (ROCs) is also important. These ROCs need to be digitally and physically secured to ensure that the risk of vessel hijacking is reduced.

8.3.5 Loss of control

Carefully planted malware can lead to the loss of control of a vessel navigation, propulsion or steering system with potentially the same impact as described in the previous paragraph 8.3.4.

The same applies to the loss of control of safety systems, cargo management systems and other similar systems.

8.3.6 Communication

To enable the communication flows between two or more vessels as well as vessels and shore, several communication systems are in place:

- Satellite communication
- Very High Frequency (VHF)
- Digital Selective Calling (DSC)
- Automatic Identification System (AIS)
- Mobile communication (2G, 3G, ….)
- WIFI

[62] https://erules.veristar.com/dy/data/bv/pdf/642-NR_2018-07.pdf

Several of these communications systems are going over the air and are not secured making them vulnerable to all kinds of attacks. They are also broadcast based systems which makes it very easy to eavesdrop.
VHF communication could also be a target of a social engineering supported attack. There is no way of knowing who the communication partner is.

A lot of vessels carry several devices which can be very old and vulnerable (legacy). These are often prone to cybersecurity related attacks. The protocol IEC 61162-1 is considered as the NMEA 0183 protocol and is commonly used as a communication protocol between onboard devices (AIS, GPS, …). It is a partly human readable protocol since the messages consists of printable ASCII format with commands. The messages can be easily intercepted and manipulated. Authorisation scheme is not used.
The Controller Area Network (CAN) bus standard is often used within vessels to connect various devices and provide communication in combination with the NMEA 2000 standard. This type of communication also has some cyber risks which can be manipulated. These risks are documented in the report "The CAN Bus in the Maritime Environment – Technical Overview and Cybersecurity Vulnerabilities"[63].

8.4 Risks related to the Infrastructure

8.4.1 Ports

The Cybersecurity risks concerning Ports are already well documented in the document "Good Practice Guide – Cybersecurity for Inland Navigation - Especially for ports. A short summary of this report is given in chapter 8.2.2.

The European Union Agency for Cybersecurity (ENISA) also wrote a report about Cyber Risks Management for Ports, containing guidelines for cybersecurity in the maritime sector[64]. Although written for the maritime sector there is a very large common ground with the IWT sector (especially since many large ports cover both maritime and IWT). This report aims to provide port operators with a set of guidelines and good practices to effectively manage commonly referenced cyber risk management challenges. The report gives guidance on the high-level categories of threats and possible impact of cybersecurity incidents.

[63] https://www.transnav.eu/Article_The_CAN_Bus_in_the_Maritime_Environment_Kessler,59,1145.html
[64] https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports

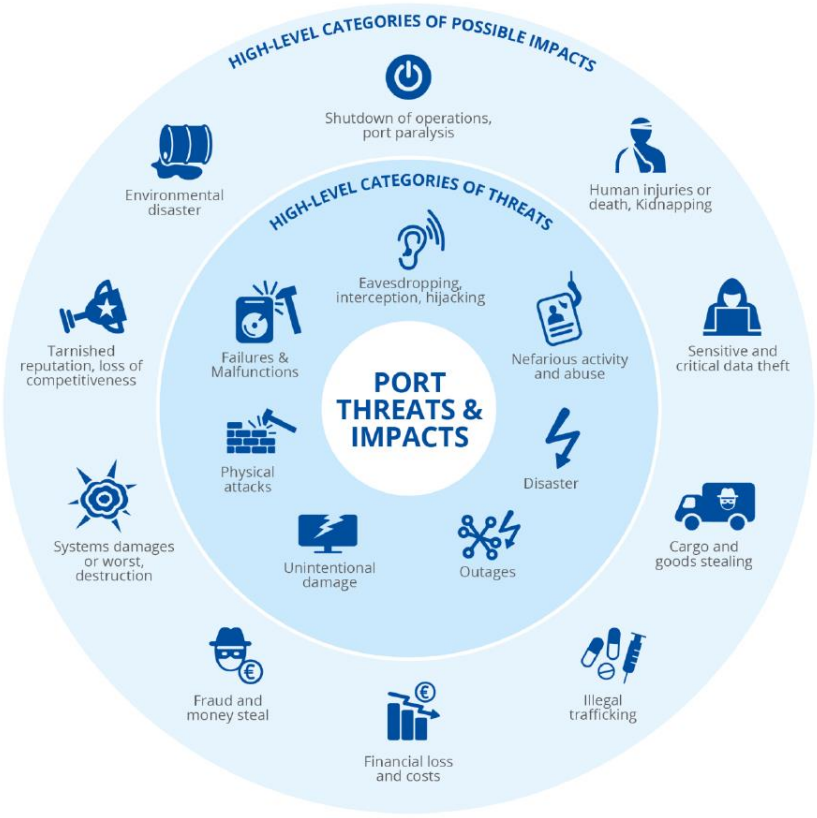


Figure 27: High-level categories of threats and possible impacts of cybersecurity incidents

The report also describes challenges for detecting potential cyber threats and risks. For example: lack of information/intelligence regarding Information Technology (IT) and Operation Technology (OT) systems' vulnerabilities or the lack of available resources (people, budget) to carry out an effective risk assessment, ….

The report "Port cybersecurity – Good practices for cybersecurity in the maritime sector" published by ENISA in November 2019 also deals with this subject. Chapter 4.2 Cybersecurity challenges gives a good overview of challenges which also can be considered as risks.

8.4.2 Remote control of objects

Industrial Control systems including Supervisory Control and Data Acquisition (SCADA) are often used for the remote control of several infrastructure assets such as bridges and locks, sluice gate systems for flood protection and water level management, crane operation, etc. These systems often rely on older protocols when Cybersecurity was not deemed as important or the manufacturers were not aware of the risks.
The infiltration of such controls systems can lead to many risks such as:

- Unwanted operation of locks leading to transport blockage or flooding.
- Unwanted operation of bridges leading to transport blockage on water, road and train related transports. It is also possible to damage passing vessels by lowering the bridge too early.
- Unwanted operation of sluice gate systems causing flooding or low water situations.
- Blockage of power and water supplies towards berthed vessels.
- Loss of control of ports including their infrastructure (terminals, cranes, …) can lead to damage of cargo and infrastructure.
- Unwanted manipulation of light signals causing collisions or traffic jams.
- …

These systems can be considered as vulnerable and need to be protected by several measures.

The increase in (network) connectivity between many control and information systems and the areas where they are used, make them also more interesting for attackers. The attack area and the associated risks are getting increasingly bigger.

Internet of Things sensors also are increasingly used within remote control and provision of information. Sensors are used for detecting when a bridge is open/closed, the operating mode of a lock, …. Information from these sensors are also used for predictive maintenance.
These types of devices are often poorly engineered on the field of Cybersecurity. Special care has to be taken when interpreting the results of those values. Since they can be considered as vulnerable (spoofing, hijacking, default passwords, …) the reported values need to be checked on validity and plausibility. The communication between all elements and the received values in the remote-control network need to be checked.
Internet of Things are often embedded devices with a very short life span. There are often supported for only a few years meaning that they will lack further security updates. Often, they don't receive security updates. There is no chance to detect if malware is installed. It not easy to check the security of those devices. You need some deep inspection to do this.
The European Union is taking initiative with the proposal of a regulation on horizontal cybersecurity requirements for products with digital elements and amending regulation (EU) 2019/1020[65] to increase the cyber resiliency of these products.

The networks for the normal operation and remote control are sometimes separated in organisations to increase the security of the remote-control network (air-gapped). This is already a good measure to increase the security but still other security measures have to be taken. The systems can be still be vulnerable to attacks. This was proven with the Stuxnet attack[66] where specific devices were targeted which were only connected to an internal network.

In the sector of water level management (inland shipping and flood protection) remote control of pumps, sluices, etc. in combination with Internet of Things (IoT) sensors is gaining popularity. Authorities are using or investigating the usage of artificial intelligence (machine learning) to automate the water level management. These solutions should also be checked on the level of cyber resilience. Attacks here can lead to serious damage (floods) or blocked transport.

The usage of digital twins could also pose some cyber risks in the case where the level of interaction between the physical and digital objects is automated, bi-directional and in real-time. If the digital twin is breached, the digital twin could be used to do malicious manipulations in the real world. If there is a direct synchronous command exchange with the physical objects this could lead to serious issues like a wrong manipulation of locks. Thus, if the digital twin is compromised by a cyberattack, the effect on the physical twin may be catastrophic. By introducing digital twins, the attack surface may be even further enlarged by including an additional failure point in a system that can be exploited by cyberattacks.

8.4.3 Information related systems

Information related systems (port community systems, berth management, terminal control, …) in use by ports or terminal operators can often be the target of malware attacks. In the past few years there were some serious attacks which led to the disruption of cargo/transport handling. The systems were often the victim of a ransomware attack encrypting the involved systems (encryption of disk). This leads to denial of service and blackmailing.

Another risk is that illegally gained access to the information related systems is used for criminal purposes to track transports of illegal goods and to open the related containers. Recently such an attack[67] was discovered where a criminal organisation used these kinds of attacks to transfer illicit drugs.

[65] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[66] https://en.wikipedia.org/wiki/Stuxnet
[67] Scenario 2 – Compromising data to facility illicit drugs smuggling described in the report „Good Practice Guide – Cybersecurity for Inland navigation – Espcecially for ports

8.5 Information/data platforms

8.5.1 Introduction

The focus of this chapter is on information and data platforms which have a larger scope or covers more area than the information related systems used within infrastructure like ports. Examples of such platforms are www.vaarweginformatie.nl, www.eurisportal.eu, www.visuris.be, www.ceeris.eu, ….

The value of these systems will increase in the future when more data will be exchanged. Especially when looking at synchro modality and when transport will become more managed by those platforms, then the value for (cyber) attackers will increase.

Sufficient consideration is necessary when linking multiple platforms together. All chains need to be cyber protected at the same level. With the increasing level of interconnection and automation the dependencies will also increase.

8.5.2 Illegitimate access to data (privacy)

RIS related systems used for vessel tracking, transport management, object scheduling, voyage permits, … use a lot of privacy related information. A breach can lead to several unwanted information disclosures.

The actual position of the vessel, skipper, crew and passenger could be either misused for illegitimate purposes or become visible to unauthorised third parties.

The data subject's username, first name, last name, address, mobile telephone, … could be visible to unauthorised 3rd parties and be used in phishing campaigns to gain further access in other systems.

Unauthorised 3rd parties could grant access to the personal data of the data subject to other users by using a data sharing platform.
The main threats for these kinds of risks are zero-day exploits, hacking, API leaks and lacking security measurements.

Digital twins and the usage of Big Data (cloud technologies) can further enlarge the risk of a privacy breach. The data will probably be stored in more than one place and the attack surface of an environment will be further extended making it more interesting and vulnerable for attackers. It will also become easier to interrogate the data because of the digital twin and big data tools. This could be used to identify possible security vulnerabilities in the underlying or shadowed physical components.

8.5.3 Unwanted modification of data (integrity)

Data stored within RIS related systems used for vessel tracking, transport management, object scheduling and voyage permits can become the subject of unwanted data modification.
The data of their vessel could be exposed to other users (change of (default) Privacy Class).
An account can be modified to gain access to other systems.

- If AIS messages are modified or spoofed, the vessel could be in another location than the location that is reported, or its dimensions, name, ENI/IMO number, … could be different.
- If a flood of fake AIS messages is fed to the system, this could result in a delay in the processing of AIS messages and the display of non-existent vessels on the maps.
- If ERI messages are modified, voyage information could become incorrect, resulting in bad ETA information, incorrect itinerary display, incorrect cargo information, …

Data could also be removed thus hiding the presence or movement of certain cargo.

Falsified water related information (distributed via NtS/AIS/…) can lead to the grounding of vessels resulting in a possible loss of lives, pollution and blockage of ports/waterways.

The main threats for these kinds of risks are unauthorised access to databases, zero-day exploits, hacking, API leaks, (D)DOS attacks by spoofing AIS messages and lacking security measures.

8.5.4 Availability

The availability of the information and data platforms will become more important when they are more interconnected and used for the planning of transport and as message/data hubs for other systems in the context of synchro modality. These systems could become the target of denial of service attacks and lead to an availability disruption thus hampering the transport sector.

8.5.5 Reliability

Another type of risk is that users can have issues trusting the data or that they are not able to detect that the data is compromised or unreliable. This could have huge ramifications like taking the wrong decisions.

With the rise of big data where large quantities of sensor input, Internet of Things data, process data, … is gathered in cloud like environments and processed using machine learning algorithms it becomes more difficult for the normal users to comprehend the outcomes. There is sometimes not a clear or direct link between the raw data and the results. Sufficient consideration has to be taken that the processed results are trustworthy and that there are some quality indicators to give feedback on the reliability of the results.

This also applies to the usage of digital twins and shadows. The users look at a representation of a (digital) reality but are often unable to question the representation because they often don't understand how it works. If it's compromised they won't know it and make the wrong assumptions.

8.6 RIS technologies related

8.6.1 Electronic reporting

Different messages are used in the context of Electronic reporting such as ERINOT, ERIVOY, PAXLST and BERMAN. These messages however can easily be drafted and distributed towards various systems. The authenticity of the messages is not checked. The electronic reports are also not encrypted which can lead to possible privacy related issues by disclosing professional and personal related information.

Information about the location and transfer of dangerous goods can be misused by persons to organise the theft of dangerous goods or to organise terrorist like attacks such as causing explosions, fires, leaks, damage to cargo/vessel, …

By using spoofed messages, the working of various waterway authorities can be hindered.

8.6.2 AIS

Automatic Identification System (AIS) plays an important role within IWT. It is used for avoiding vessel collisions (ship-to-ship) and information sharing with authorities (ship-to-authority). In the near future AIS will also be more and more used to transfer information from authorities towards the ship (virtual AtoNs, water level reports, signal status, weather related information, dangerous zones, recommend time of arrivals (RTA), …. Also, AIS is being increasingly used to provide position derived services (e.g. berth occupation, passage notifications, average speed calculation, passage statistics,…).

AIS is an old but proven technology using VHF communication with low bandwidth. The main issues with AIS is that there is no encryption of transmitted data. Everybody can eavesdrop and spoof data with low cost hardware. AIS has no features for verifying authenticity, integrity and validity of data.
The vulnerability of AIS lies in the fact that all data transmitted by AIS is considered to be true.

Receiving software can be augmented with some sanity checks using standard controls like valid MMSI/ENI/IMO format control, plausibility checks like distance calculation between two subsequent positions, duplicate number checks (e.g. two ENI numbers with the same MMSI number), …

Several websites rely on the fact that AIS data can be captured and provide additional business on that, even if the data is deemed as personal position related information (in the case of persons living on vessels where a relation can be made between the person and the vessel).
These kind of data leaks can also be used in a more nefarious manner.

The spoofing/displacement of AIS positions information can lead to vessel/object collisions potentially leading to loss of lives, disrupting transport and or port/waterway access.

Within the maritime world there is an interesting development called the VHF Data Exchange System (VDES). The International Telecommunications Union (ITU) has produced technical standards[68] and has revised the VHF marine band to designate channels for data transmission. These bands could be used for both analogue voice communications and digital communication. VDES addresses the identified need to protect AIS along with essential digital communications contributions for e-Navigation and Global Maritime Distress and Safety System (GMDSS) Modernisation. IALA has provided guidelines and the technical specifications concerning VDES[69]. The VDES related applications addresses cybersecurity (e.g.: authentication, key management and, if required, encryption).
VDES VHF consists of three technologies: AIS, Application Specific Messages (ASM) and VHF data exchange (VDE) each operating on its own VHF channels. The data bandwidth is increased, see Figure 28.

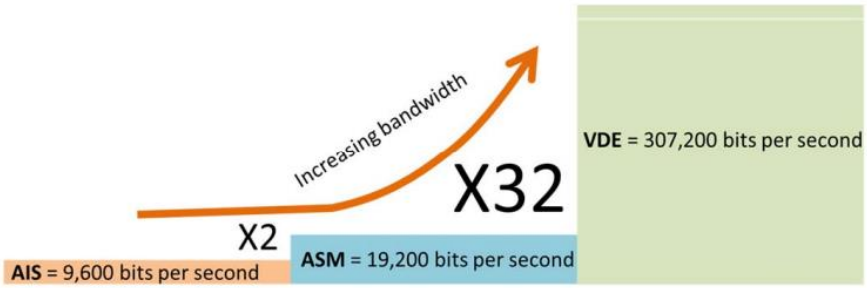


Figure 28: Increasing (raw) data bandwidth in VDES

The VDES technology uses a Terrestrial Bulletin Board (TBB) consisting of 108 bytes to assign the primary operating environment parameters to the Control Station Service Area. This includes which frequencies are being used and the service area dimensions amongst a range of other technical detail. Here an authentication mechanism (digital signature and public key infrastructure) is used to check if the TBB is transmitted by a trusted source. This is an improvement compared with AIS where it is possible to influence the behaviour of AIS transponder by providing different AIS control messages (assigned mode, group assignment mode, channel management, …) from unauthorised sources.
Several types of attacks are also applicable to this new technology such as position spoofing and jamming since it relies on the same used components as AIS. With the authorised messages it is possible to warn users of certain events.

8.6.3 Notices to skippers

Notices to skippers (NtS) are used to inform the vessel operators/skippers about general and specific limitations. Vessel operators and skippers should be wary as to use only notices to skippers from trusted sources.
Notices to skippers are not digitally signed which means that they can be the subject of modification or spoofing. NtS messages are often distributed by ECDIS suppliers or other systems which can make them additionally susceptible to modification.

[68] ITU-R m.2092-1 recommendation (02/2022)
[69] IALA Guideline G1117 – VHF Data Exchange System (VDES) Overview – Edition 2.0 – December 2017 & IALA Guideline G1139 – The Technical Specification of VDES – Edition 3 – June 2019

Spoofed/modified messages can potentially lead to dangerous situations such as vessel groundings by providing falsified depth information leading to loss of lives, disrupting transport and or port/waterway access.
Other situations that can arise is that unaware operators/skippers can think that a certain waterway is blocked due to a limitation causing transport delays/disruptions.

8.6.4 ECDIS

Current ECDIS related systems are often placed on old dedicated hardware and are not often updated. The lack of patches can lead to cyber risks.

These systems are not often protected by anti-malware products making them vulnerable to malware and viruses. Malware and viruses can be brought on board during an ENC cell download or by USB transfer. ENC cells can contain attachments such as XML, TXT and TIFF files. A possible attack vector is by injecting special instructions in the EXIF (metadata) information of pictures.

Malware installed on board can be put in to a sleeping mode while waiting for commands. These commands can be given by providing specially crafted AIS messages which will trigger the malware. Possible consequences are false or nefarious commands sent towards other connected devices via NMEA commands, shutdown of the ECDIS system or presentation of wrong navigation information. This kind of attack was described in the paper "A Triggering Mechanism for Cyberattacks in Naval Sensors and Systems"[70].

In the current implementation of ENC cells based on the IHO S-57 standard there is no way of knowing that the ENC cell is produced by an authorised provider. As such false information (e.g. wrong depth contours) could be provided possibly leading vessels to ground. These files should be protected by signing the files with a certificate. The related systems should check the validity of these certificates.

The cybersecurity risks addressed while discussing the IHO S-57 standard and the distribution of IENC cells are partly addressed In the IHO S-63 standard (IHO Data Protection Scheme) and fully in the IHO S-100 standard (Universal Hydrographic Data Model). The S-100 standard is the overarching standard under which umbrella the S-401 and S-402 is defined. The S-401 standard deals with the Inland Electronic Charts (IENC).

The S-63 has support for the encryption and digitally signing of the IENC base cell and updates. The attachments like pictures and files are not encrypted. It is unclear if a signature of the attachments is used so they could be vulnerable for tampering.

The S-100 standard has a part 15 called "The Data Protection Scheme". This part describes the recommended standard for the protection of hydrographic or spatial information. It provides security constructs and operating procedures that must be followed to ensure that the data is distributed in a secure and commercially viable way. The main purposes of the data protection are:

- Piracy protection: to prevent unauthorised use of data by encrypting the product information.
- Selective access: to restrict access to only the products that a customer has acquired a license for.
- Authentication: to provide assurance that the products have come from approved sources.

These goals are reached by encrypting data, providing permits to use the data and by digitally signing the data. The International Hydrographic Organisation on behalf of the IHO Member States and other organisations is responsible for maintaining and coordinating the Protection Scheme. In this context the IHO will maintain a top-level digital root certificate. They will also certify the producers of the data. Thus, a data client can verify if the information comes from a trusted source.

The S-401 "IEHG Inland Electronic Navigational Chart Product Specification" version 1.0.0 Draft published on November 2019 was checked upon the usage of the S-100 protection scheme methods.

[70] Citation: Junior, Walmor & Coreixas de Moraes, Claudio & Albuquerque, Carlos & Machado, Raphael & Sá, Alan. (2021). A Triggering Mechanism for Cyberattacks in Naval Sensors and Systems. Sensors (Basel, Switzerland). 21. 10.3390/s21093195.

This version is still considered as a draft since the other related documents such as the feature catalogue and portrayal catalogue are under development. In version 1.0.0 the specifications concerning Data Integrity and encryption are out of scope because it was under development by S-100 WG at that time. These specifications will be part of the next edition of the document (version 2.0.0). The S-401 standard will follow the same rules as the S-101 standard.

Co-funded by the European Union

9 Countermeasures on cyber risks in IWT

This chapter gives an overview of some recommended specific cybersecurity countermeasures in the context of IWT. An overview of the most common general cybersecurity countermeasures or security controls is given in chapter 7.3.

Blockchain is often mentioned as a very interesting technology in the context of cybersecurity. During this Sub-Activity the usage of blockchain was also investigated. It can be used to proof the ownership of a digital good and the backtracking of the history of digital goods.
Considerations have to be made with the usage of blockchain to track where vessels have loaded and unloaded goods. In the current blockchain implementations this history will be forever in the blockchain and the blockchain will get bigger and bigger. For transactions on the waterways that are short lived it could be a bit overkill. Blockchain can be used for non-repudiation but other immediate benefits haven't been found.

9.1 Technical

Area of cyber risk	Countermeasure
Communication channel	• All communication channels should be hardened • Use data encryption • Enable authentication through the usage of certificates • A Public Key Infrastructure solution enables a safe generation and distribution of the certificates • It is perhaps a task for the certification authorities responsible for the certification of the Inland vessels
Remote Access to vessel train	• Use a layer 3 encryption and authentication for the control of the vessels
Positioning devices	• Receivers should be hardened • Positioning system should be extended with authentication & authorisation mechanisms to counter spoofing
Position data	• Captured data can be analysed by using AI • Anomalies (outliers) needs to be removed
All outgoing data and messages which influences the behaviour of vessels and transports	• Use digital signatures to enable the check of the source of the data and messages • For example: the skipper or system on board can verify the origin of a notices to skipper
Older insecure data exchange protocols (e.g.: NMEA0183, CAN Bus, etc.)	• Replace them by newer and up to date variants as soon as possible
Network systems	• Don't mix remote control, operational, recreational and office networks • Use preferably air-gapped networks for remote control and normal operation
Remotely controllable Sensors or Devices	• Implement detection algorithms to check if device is performing as expected • Compare the sensor output against the actuator input and the expected result • AI can be used to detect anomalies, if the infrastructure is subject of an attack (corrupting or hiding information) or an actuator attack (intercepting & modifying orders)

Software	• Ensure the SCADA software used is sufficiently updated and used safely • Regular software updates and patches need to be applied at all times.

The rollout or support of communication solutions with a much higher bandwidth is necessary to support the higher bandwidth requirements especially when encryption and digital signing will be used. Steps are already being taken with the introduction of VDES and 5G. These solutions allow a higher bandwidth but the coverage is much smaller. Many waterways are not even sufficiently covered by 4G. This could become an increasing problem with the decision to phase out 3G by some mobile operators.

9.2 Administrative/Organisation

Area of cyber risk	Countermeasure
System activities	• Monitoring and logging of activities of humans and systems • It enables to initiate immediate countermeasures, in case of a failure which could directly lead to dangerous situations for human safety, the safety of the ship and/or hazards for the environment
Remote control centres (ROC) and vessels	• Execute cybersecurity assessments • A cybersecurity certification for vessels and remote-control centres should be performed, before they are allowed to operate on European waterways • The automation level of the vessel should determine the type of cybersecurity resilience certification • Unmanned vessels should have the highest level of cybersecurity resilience because no human operator will be able to quickly intervene
IoT devices or other similar devices	• When selecting devices or equipment, the lifespan and support period needs to be considered • Only select devices with a sufficient lifespan • Change the password and default settings of the device • Respect the privacy and GDPR law, when recording sound and images

9.3 Physical

Area of cyber risk	Countermeasure
Physical access	• Take security measures to prevent unauthorised access to communication networks and related devices on board of a vessel (especially for unmanned vessels) • Take measures to prevent physical tampering or the planting of hijacking devices
Decommissioning of vessels and equipment	• All data carriers need to be securely wiped and destroyed during decommissioning of vessels and equipment • It is often proved that the waste disposal sites still contain enough equipment which can be activated to retrieve sensitive data

10 Conclusions

The analysis that has been performed in previous chapters of this report, demonstrates that cybersecurity is a critical issue in the field of inland waterway transport. With the increasing reliance on technology and automation in this sector, as can be observed in all of the business and technological developments of activity 2 and 3, the risk of cyberattacks and other security incidents will increase in the coming decade.

A comprehensive study of cybersecurity in inland waterway transport is therefore an important step towards improving the security and reliability of this critical sector. By taking a proactive approach to address these risks, it is possible to facilitate the business and technological developments of the sector while maintaining business continuity, safety of operations and respect for privacy.
Based on the findings of the study, recommendations can be made for improving the overall state of cybersecurity in inland waterway transport. This includes the implementation of stronger security measures, such as encryption and multi-factor authentication, the development of incident response plans, and the creation of cybersecurity awareness programs for employees. Additionally, the industry should consider investing in research and development to advance the state of cybersecurity technology, and to ensure that new technologies are developed with security in mind.

The role of (fairway) authorities in cybersecurity is two-fold: they must both safeguard their own operations and encourage other actors in the inland waterway transport sector to apply best practices in terms of cybersecurity:
Both in their physical operations (e.g. management of locks and bridges) as in their online operations (e.g. providing data platforms), fairway authorities must ensure that their systems and networks are secure and protected from cyber threats, as well as regularly monitoring and updating their systems to detect and respond to any security incidents.

At the same time, (fairway) authorities also have a responsibility to encourage other operators in the sector to apply up to date standard processes in terms of cybersecurity. This may involve working with industry organisations to establish standards and guidelines, conducting audits or imposing certification of other operators' systems and networks, and providing cybersecurity awareness programs for employees.

The cyber risks in IWT and their countermeasures were introduced in chapters 8 and 9 respectively. For the in-depth discussion of the conclusions, we refer to the recommendations (chapter 11) that provide specific and actionable steps that can be taken to address the issues outlined in the study. They are the tangible outcome of the analysis and research conducted, and serve as a guide for future decision making and implementation.
However, in order to highlight the key findings of this study, the main conclusions for this report can be summarised as follows:

- As digitalisation and the use of more connected systems increase, the surface of attack for cybersecurity risks also increases. On top of that, as the reliance on digital solutions to actively intervene in the system (e.g. in smart shipping) increases, the probability and potential impact of cyber incidents also increases. Hence it is increasingly important that **organisations need to be prepared to address cyber risks**.

- It is noted that IWT is not currently the most cyber resilient transport mode[71], through vulnerabilities in certain systems, such as AIS. While AIS has been implemented as a safety measure to improve vessel navigation and reduce the risk of collisions, it relies on VHF radio transmissions which are prone to spoofing, which is the act of transmitting false AIS data to deceive other vessels or systems. However, **there are some measures that can be taken** to improve the cybersecurity of these IWT systems.

[71] PIANC (2019): Awareness paper on cybersecurity in inland navigation (see also 8.2.2.2)

- Developments such as initiatives by organisations like PIANC and CESNI demonstrate a growing awareness of cybersecurity risks in the transport industry. This is a positive development, but efforts should continue to be made to keep **awareness** at a high level, as it is difficult to maintain this level of awareness over time. Also, cybersecurity is not a goal that can be achieved, but rather an ongoing process. Cyber threats and vulnerabilities are constantly evolving, and **organisations must continuously adapt** their security measures to keep pace.

11 Recommendations

Listed below are the recommendations of this Sub-Activity. These recommendations are based on the inventory of cyber risks which aren't or only partly covered by countermeasures (gaps) or when the provided countermeasures aren't applied yet. For example: encryption and digital signatures are existing known countermeasures but are often not applied in the IWT environment.
This list is also amended with the more general best practices in cybersecurity such as implementation of an ISMS (Information Security Management System), dedicated security team, regular software updates, ….

REC 1: Certification of vessels and ROCs

It is recommended that both vessels (and especially remotely operated vessels) and remote operation centres (ROC) are additionally certified against a standard that needs to be drafted by the proper authorities on the field of cyber resilience. Vessels and remote operation centres should have such a certification before being allowed to operate on European waterways.
The type of cybersecurity resilient certification should depend on the level of automation foreseen for the vessel. Unmanned vessels should have the highest level of cybersecurity resiliency because no human operator will be able to quickly intervene. In this case the remote operation centres (ROC) should also be subject of a very thorough screening.
Gaining an ISO 27001 certificate for remote operation centres is also recommended.

REC 2: Public-key infrastructure

Public-key infrastructure (PKI) uses asymmetric cryptography to encrypt data between a known infrastructure and an (sometimes) unknown accessor. The asymmetric part of PKI means that a private key is used to encrypt data and a second key, the public key, is used to decrypt the data. Therefore, an organisation has full control over its implementation and can choose, in accordance with their standards, which suitable encryption algorithm they wish to implement. It differs from symmetric encryption where both the parties involved in a communication flow would need the same encryption key, namely the shared key.

Setting up a PKI will result in the possibility to sign and / or encrypt almost all information flows. The encryption of information flows covers 2 of the 3 basic values of Information Security, namely "Confidentiality" and "Integrity" of the CIA triad, but also provides authentication and nonrepudiation.
PKI should be used in all processes related with data exchange: AIS, Electronic reporting, IENC exchange, Notices to Skippers, remote control, …
Figure 29 shows a possible certification path in which a root authority (EU) certifies national competent authorities (NCA). These NCA's certifies the fairway authorities and the certification authorities. The latter are responsible for providing real and digital certificates for the vessels. Using this approach valid certificates are available for encrypting and digitally signing data exchanges.

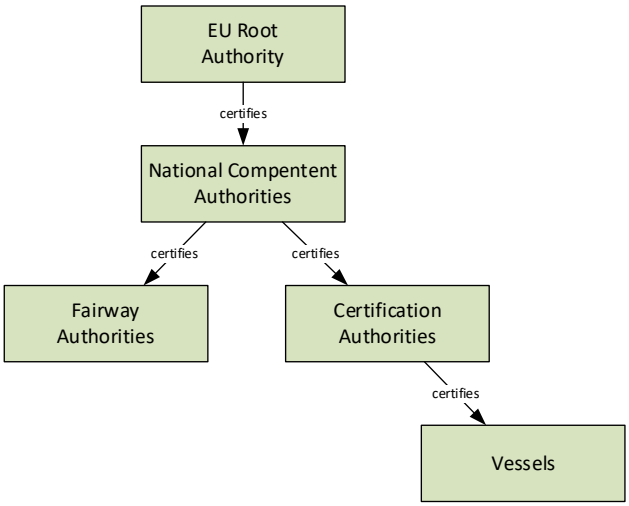


Figure 29: Certification path

The recently finalised development of the SECOM protocol for secure ship-shore and shore-ship data exchange communication as defined in an international/European standard (EN IEC 63173-2) can help to achieve a standardisation on this subject. The protocol was originally developed in the maritime domain in the context of e-navigation for the provision of data products by shore-based organisations to shipboard applications in particular as defined in the 'S-100 World'. In SuAc 3.5 the SECOM standard was evaluated and deemed as possible solution. However, the full implementation of SECOM can have large resource requirements. A possibility to only implement the "just secure data protocol option" is foreseen.

A similar solution for PKI has been drafted by the IHO for the standard S-63 (IHO Data Protection Scheme). An updated version of these principles is used in the S-100 standard.

REC 3: Implementation of an ISMS

The implementation of an ISMS (Information Security Management System) is not only highly recommended, it should be a necessity to be able to follow-up on the implementation of an organisation's security controls. It provides a structured way to keep track of the overall state of an organisation's state of security.
To set up an ISMS one can follow a plan-do-check-act process or check in detail the ISO 27001 international security standard. The most important steps that should be taken are:

- **Define the scope and objectives**. Determine which assets need protection and the reasons behind protecting them.
- **Identify assets**: This can be achieved by creating an inventory of business-critical assets including hardware, software, services, information, databases and physical locations
- **Recognise the risks**: the risk factors should be analysed and scored by assessing the legal requirements or compliance guidelines.
- **Identify mitigation measures**. The ISMS not only identifies risks and weights but also provide measures to effectively mitigate them.
- **Make improvements**. All the measures taken should be monitored and audited. It is useful to implement Key Performance Indicators to measure the effectiveness of the measures taken. For example: all known applications dealing with sensitive data should encrypt the stored data.

This recommendation is especially for fairway authorities, larger companies and for operators of remotely operated vessels.

REC 4: Dedicated security team

To ensure that the implemented ISMS is followed up correctly and with the necessary expertise it is highly recommended to appoint a dedicated "security" team consisting of a Chief Information Security Officer (CISO) together with cybersecurity experts.

It is the main responsibility of that team to monitor the continuously evolving cyber threats. Based on their expertise the team will be able to formulate practical implementations of controls. Furthermore, a strategic, tactical or operational plan will need input from this team as things evolve.

REC 5: Security awareness training

Security awareness training has the objective to help prevent, reduce and mitigate user risk and user targeted attacks. Every user, regardless of job function, who comes in to contact with (digital) information should be trained on how to handle it properly. As an analogy it should be considered to treat sensitive information as "highly flammable". Special requirements, special tools, equipment, procedures, etc. should be followed to handle this "highly flammable" information.

The goal of security awareness training is to keep an extra set of eyes open for potential attacks. Security awareness training can be an excellent input for practical implementations. People "in the field" can provide very useful information to further sharpen security on strategic places which are often overlooked.

Security awareness training for all users who handle (digital) information should be given on regular intervals (e.g. yearly). The input/feedback from these sessions should be used to revise the implemented practical controls and procedures.
In general, this recommendation applies to larger organisations such as fairway authorities, ports and logistics companies for which established general training packages are readily commercially available.
In order to elevate the level of cybersecurity awareness across the sector and address specific vessel related cyber vulnerabilities it is however recommended for EU IWT organisations such as CESNI, CCNR, EU commission, etc. to jointly develop and provide an online free cybersecurity awareness course, similar to the EMSA course mentioned in section 6.3.7 or the Tactical Advice for Maritime Cybersecurity – Top 10 published by Pen Test Partners[72] , containing specifics for EU inland shipping.
In addition, fairway authorities are encouraged to take an active role in assisting vessel operators becoming and staying aware of cyber risks at appropriate contact moments (e.g. presence at events frequented by vessel operators, during inspections on board, etc.). Efforts should be made to not only raise awareness, but also to provide basic practical advice on how to mitigate common cyber-threats. Although it is ultimately the responsibility of the vessel owner to implement cybersecurity measures, it is the asset of the fairway authority which is in danger of being damaged when a vessel gets hacked.

REC 6: Apply updated standards

For almost every topic regarding controlling or maintaining security, risk, governance, … there is a certain standard that defines a structure for implementation. As threats and risks evolve, so do these standards. It should therefore be recommended that an organisation should look into these evolved and newer versions of applied standards to consider whether an update of their own implementation is deemed necessary.

Standards are updated with relatively long intervals (mainly years, rather than months). So the anticipation on a standard update can be specified in a strategic plan.

Some examples of protocols/standards/systems with limited security are IEC61162-1, NMEA0183, CAN Bus, SCADA, …

REC 7: Software defined devices

In order to overcome the long lifetime of hardware devices on board and their inflexibility to adapt to new environments and threats it is recommend to use more software defined devices.

An example of this is a software defined radio. This is a radio communication system where components that are normally implemented by hardware such as analogue mixers, filters, amplifiers, … are instead implemented by means of software. By shifting from hardware components which have a very long lifetime to software components this allows for a more flexible and agile approach. These systems can then be more easily upgraded and making them thus more cyber resilient. New functionality and new application messages can also be more easily introduced. The opportunity to use software defined radios is now present with the rollout of VDES. Several manufacturers are already providing base stations using the concept of Software defined radios.

REC 8: Internet of Things - Consider limited lifetime in design

Special consideration has to be taken when selecting Internet of Things devices. Since they are often poorly made (from a cyber-security point of view) with a very short support life span (few years) it is not wise to use them in environments/solutions with a long life time or for important applications. Vessels are often used for decades.

It is recommended that the limited lifetime of IoT devices is taken into account when building new vessels or infrastructure, anticipating that IoT devices can be replaced during the lifetime of the vessel/infrastructure.

[72] https://www.pentestpartners.com/security-blog/tactical-advice-for-maritime-cybersecurity-top-10/

REC 9: Internet of Things - Increase support period/apply CRA

It is recommended to require suppliers to support those devices for a longer time and provide an easy interoperable upgrade path. This is also necessary to reduce the digital waste.
The upcoming EU Cyber Resilience Act (CRA) will increase the cyber resilience of IoT devices distributed and sold within the EU (see 6.1.3). It may however take same time before less cyber resilient devices are phased out. Until that time, it is recommended to not consider IoT devices safe "out of the box" and add cybersecurity measures "on top of" and around these devices and sensors to mitigate risk (see also[73]). This is especially important when employed on (semi)autonomous vessels since there is most likely no one on board to take manual control of the vessel when equipment is compromised by cyberattacks. It is possible to encrypt data created and transmitted by IoT and other small devices using authenticated encryption and hashing algorithms (e.g. Ascon[74], standardised for lightweight cryptography applications by the U.S. National Institute of Standards and Technology (NIST)). This significantly improves the security of IoT systems, but further measures need to be taken to minimise the risks of still remaining vulnerabilities (e.g. side-channel attack, fault attack) of an IoT environment

REC 10 Secure cloud provider

Cloud technology is a very interesting technology to maximise the efficiency of used computing resources and the gain flexibility depending on the needs. However, since the (big) cloud providers all implement the environments in a different way there is a risk for vender lock in. There could also be some risks with the ownership of data when it is hosted by external cloud providers. National laws often foresee the possibility to consult data stored in their region.

Choose a provider/data centre which hosts the data that protects the data confirming the European privacy laws (GDPR), and the planned EU Cloud Rulebook[75]. Also check if the provider has information security related certifications such as ISO 27001, ….

REC 11 Artificial Intelligence for data validation

Artificial Intelligence is a very promising technology which can be applied to many different problems. The combination of Artificial Intelligence and Big Data Analytics can be used to support the cyber defence. Artificial Intelligence can be employed to aid in the detection (see 7.2.3) of anomalies/irregularities indicative of cyberattacks. Rijkswaterstaat has implemented a system where (IT) network traffic of a lock or bridge is fed to an algorithm for a certain period to build up a baseline of "normal" pattern behaviour. This baseline is subsequently used by a monitoring system which "listens" to the network traffic of a lock or bridge, comparing the current traffic to the baseline. Irregularities such as new devices becoming part of the network or unusual commands being sent trigger an alert, prompting cybersecurity experts to investigate the cause. Attempts to gain unauthorised digital access to the lock or bridge can thus be detected and contained or thwarted before causing serious damage. It is recommended to investigate the use of this technology in case of connected infrastructure where risk assessments point to significant cybersecurity risks.

Artificial Intelligence (and more traditional algorithms) can also help in the sanity check of incoming data. Irregularities such as multiple vessels with the same MMSI or ENI number, invalid AIS position information, tampering, unexpected behaviour of vessels, … can be detected. Quality indicators (how trustworthy is the data?) can also be assigned to the data and the processed information.
It is important that the sanity checks are in place so that the right decisions can be made based upon the assigned quality indicators.

[73] PenTestPartners (2022): https://www.pentestpartners.com/security-blog/tactical-advice-for-maritime-cybersecurity-top-10/
[74] Ascon (2019): https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/ascon-spec-round2.pdf
[75] EU commission (2023): https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

REC 12: Network coverage

The volume of data to be sent across networks for Inland navigation is increasing. New business developments like IoT or remote operation of vessels generate new data streams. Encryption of existing data streams creates additional data volume.
The data streams also become more critical for operations.

Inland navigation will hence rely more and more on the communication channels that are used to enable the information exchange. But increased data flow requires increased bandwidth, which typically reduces the range over which data can be exchanged. Geographic coverage of all inland waterways will prove even more difficult in 5G than 4G or 3G. VDES requires a denser network of receivers than AIS but it can solve the current bandwidth issues of AIS and allow for more application specific messages and data exchange.

Hence it is recommended to include in all related processes sufficient fallback solutions if data flow is interrupted. These fallback solutions can include temporary standalone operation or the switch to other communication channels (with reduced bandwidth).

Also, it is recommended that fairway authorities strive to improve communication network coverage over their fairway network by the network providers.

REC 13: Supplier Risk

Dependency on very limited numbers of suppliers for equipment and network operators in 5G but also satellite communication is possible, whereby a single, often non-European, supplier can control data flow or interrupt services.
Also, for cloud computing, there is a non-negligible risk of vendor lock-in and dependency on a single supplier.
When buying equipment and/or software the lifecycle of the product needs also to be taken into account. How long is the vendor willing to support the product (especially on the field of security updates since more and more the devices are software based)?

In addition the cyber-resilience of other contracted parties should be taken into account when they are requested to provide services to/for an organisation. Cyber security requirements should be part of the contract in order to safeguard that cyber resilience of the contracted works (e.g. building locks & bridges[76]) are in line with the cyber security policy of the contracting organisation.

It is recommended that clear rules (cybersecurity requirements for procurement) and commitments concerning the availability of the services are provided

REC 14: Protect data exchange

All data exchanges have to be protected. This means that the integrity, confidentiality and availability of data exchange should be guaranteed. This becomes more and more important. For example, with the advent of track pilots and automated navigation a new stream of predicted traffic information is created based on models. The data streams (AIS, GPS, Radar) on which the predicted traffic is calculated can however be falsified, which can invalidate the output.

When the predicted traffic data is shared with other parties (intention sharing), issues can also arise if the communication stream is intercepted and/or altered.

It is therefore recommended to secure all communication data links between vessels and between vessels and shore stations/infrastructure and guarantee the validity of the originator and recipient. New developments should include cyber resilience in the design of solutions (see 8.3.2). This should be encouraged by authorities and possibly required to be demonstrated by suppliers before being allowed to be used operationally on inland waters. This should be a part of the certification of vessels and ROC's procedure.

[76] CERT Watermanagement (2023): https://www.cert-wm.nl/csir

REC 15: Risk assessments for new developments

Many of the new digital technologies provide better efficiency and functionality. However, the increased interconnection of systems through internet, cloud computing, modelling and data exchanges, also increases the surface of attack and potential impact of malicious actions. E.g. in a digital twin with bi-directional real-time link, there is an opportunity for a hacker to impact the physical twin by breaching the digital twin.

It is therefore recommended to monitor the trade-off between increased functionality and increased risk, perform a risk assessment for each new development and define and implement mitigating actions.

It is often difficult for end-users to make a trade-off whether a new technology is safe to use and has sufficient cyber defence in place. Therefore, the initiative of the European Union to draft the Cyber Resilience Act (see chapter 6.1.3) is very important.
Another aspect is that cybersecurity is often evaluated from a technical perspective. The human behaviour is also a very important aspect. When evaluating new developments also pay attention to the human behaviour like described in chapter 6.3.5 - Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity (ENISA).

The risk assessment should also have a focus on the privacy aspect. For example, the placement of microphones and cameras on remote controlled vessels could lead to privacy issues. Unwanted sound and images could be recorded leading to privacy issues and potential violations of GDPR.

REC 16: Regular software updates

It is important that all devices, applications and operating systems on shore and on board of a vessel are regularly updated (patched) to ensure the proper working and to remove possible vulnerabilities. This is one of the most common pitfalls in cybersecurity.
Hardware and software manufacturers need also to be obligated to provide security updates longer than the common 2 or 3 years (especially on the field of low cost IoT devices).

REC 17: Hardening of devices and software

Many devices and software are often installed with default settings. These default settings are often insecure or not following the best practices. Therefore it is recommend to follow the best practices on secure deployment during the installation. For example, the NIST standards already give a lot of advice on how to harden an operating system to reduce the attack surface.

Manufacturers should also investigate on how to harden their devices and give advice on what measures need to be taken. For example: harden GNSS receivers by providing anti-spoofing algorithms on receiving side.

REC 18: Network segregation/segmentation

It is strongly recommended to provide correct network segmentation/segregation and not to mix operational, control and office networks. The network for remote control for infrastructure needs to be completely separated from the other networks. An air-gapped network for the remote control (actuators) is advised. In this case a secondary network to detect the state of operation and infrastructure can be used (sensors).
The same applies also for vessels where it is strongly advised to separate control, office and for example entertainment network (television, public WIFI, …) from each other.

REC 19: Decommissioning of vessels/equipment

An often overlooked fact is that data carriers aren't securely wiped. During the decommissioning of vessels and equipment all data carriers need to be securely wiped and destroyed to prevent possible leakages of sensitive data.

REC 20 Privacy assessments

All stored data needs to be evaluated on privacy and sensitivity. The best practice is to store privacy related and sensitive data in an encrypted form at rest. Position information which can be linked to natural persons needs to be treated as personal information. Recorded sound and camera images can only be used by authorised persons and not be distributed without consent.

It also recommended when starting new projects or data exchanges to execute a Data Protection Impact Assessment (DPIA) when risks are expected with the processing of personal data. This is required by the GDPR.

12 Roadmap for Cybersecurity

12.1 Introduction

To draft a roadmap for Cybersecurity several factors were investigated. Based upon the recommendations and a high-level assessment of legal, technical, financial and organisational impact a grading based on the adaptation resource demand is given for each recommendation. The following grades are used, see Table 12-1.

Adaption resource demand	Remarks
++	Little adaptation resource demand
+	Intermediate adaptation resource demand
0	Substantial adaptation resource demand
-	High adaptation resource demand
--	The resource demand for adaptation exceeds reasonable limits.

Table 12-1: Grading based on Adaptation Resource Demand

Also, recommendations were grouped according to the development scenarios based on the timeframe for realisation of the corresponding action:

- Basic = 0 – 5 years
- Intermediate= 5 – 10 years
- Advanced >10 years

There are two views for the given recommendations:

- A matrix with all recommendations assigned to different stakeholders.
- A diagram with all recommendations grouped per category and horizon.

12.2 Stakeholders

Figure 30 gives the overview of involved stakeholders. The Cybersecurity recommendations are relevant for the different stakeholders. In the following matrix (see Table 12-2)
an overview of the recommendations assigned to the stakeholders is given. For the stakeholders, vessel operators and logistic operators a division into small and large is made. Some recommendations are only feasible for larger organisations.

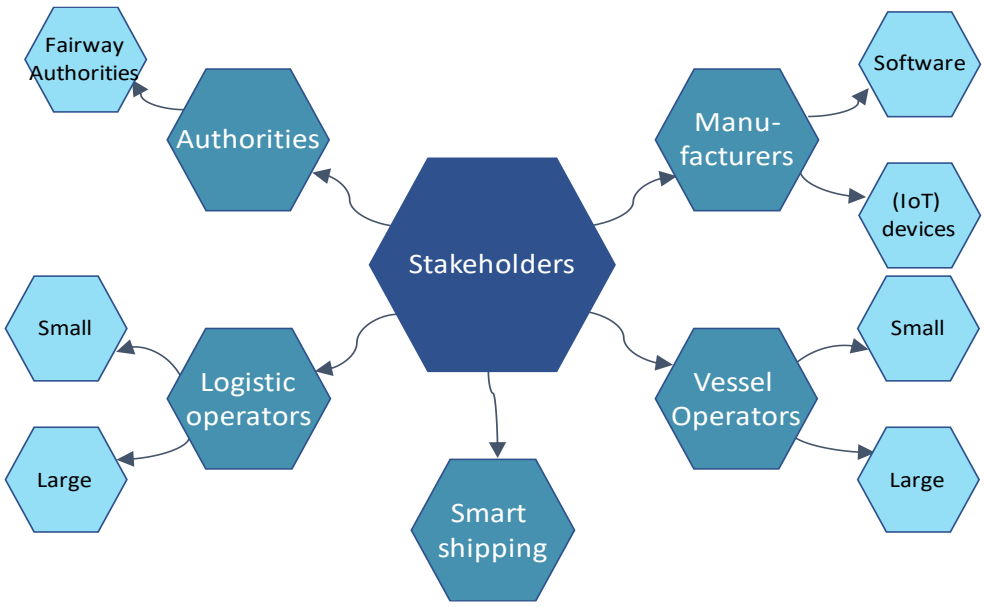


Figure 30: Stakeholder overview

12.3 Recommendation matrix

Based upon the methodology for determining the impact on needed resources a matrix with the recommendations was compiled. In this matrix we also show the potential stakeholders and a potential horizon (timeframe). There are two types of impact:

Stakeholder needs to implement this or follow the guidelines.

Stakeholder needs to draft the guidelines or regulations. In case of regulations the stakeholder also needs to enforce it.

		(Fairway) Authorities	Logistic operator (large)	Logistic operator (small	Software/ IoT device provider	Smart Shipping	Vessel operator (large)	Vessel operator (small)	Resource impact	Horizon
REC1	Certification of vessels and ROCs	✓				✓	✓	✓	-	Basic
REC2	Public-Key Infrastructure	✓ ✓			✓				0	Basic
REC3	Implementation of an ISMS	✓	✓		✓	✓	✓		0	Intermediate
REC4	Dedicated security team	✓	✓		✓	✓			-	Intermediate
REC5	Security awareness training	✓	✓	✓	✓	✓	✓	✓	++	Basic
REC6	Application of updated standards (NMEA, VDES, …)	✓			✓	✓	✓	✓	0	Intermediate
REC7	Software defined devices	✓			✓		✓	✓	0	Basic
REC8	IoT devices – Consider limited lifetime in design	✓			✓	✓	✓	✓	+	Intermediate
REC9	IoT devices – Increase support period/apply CRA	✓			✓				0	Basic
REC10	Secure cloud provider	✓			✓	✓			-	Basic
REC11	Artificial Intelligence for data validation	✓			✓	✓			0	Intermediate
REC12a	Network coverage – Implement fall back solutions	✓			✓	✓			0	Intermediate
REC12b	Network coverage – Strive for better coverage	✓							--	Advanced
REC13a	Supplier risks – Define SLA's for network operator	✓							+	Basic
REC13b	Supplier risks – Define standards for contractors	✓							+	Basic
REC14	Protect data exchange	✓ ✓	✓	✓	✓	✓	✓	✓	0	Intermediate
REC15	Risk assessments for new developments	✓			✓	✓			+	Basic
REC16	Regular software updates	✓	✓	✓	✓	✓	✓	✓	++	Basic
REC17	Hardening of devices & software	✓ ✓	✓		✓	✓	✓		-	Basic
REC18	Network segregation/segmentation	✓	✓			✓	✓		0	Basic
REC19	Decommissioning of equipment	✓					✓	✓	++	Basic
REC20	Privacy assessments	✓				✓			0	Basic

Table 12-2: Recommendation matrix

12.4 Recommendations per category

In this chapter we grouped the recommendations according to these categories: Vessel related; Infrastructure related; Common and organisational recommendations; Information / data platform related; RIS Technology related

In this overview some recommendations are split (repeated) because they belong to two or more categories. The overview also gives an indication of the timing horizon.

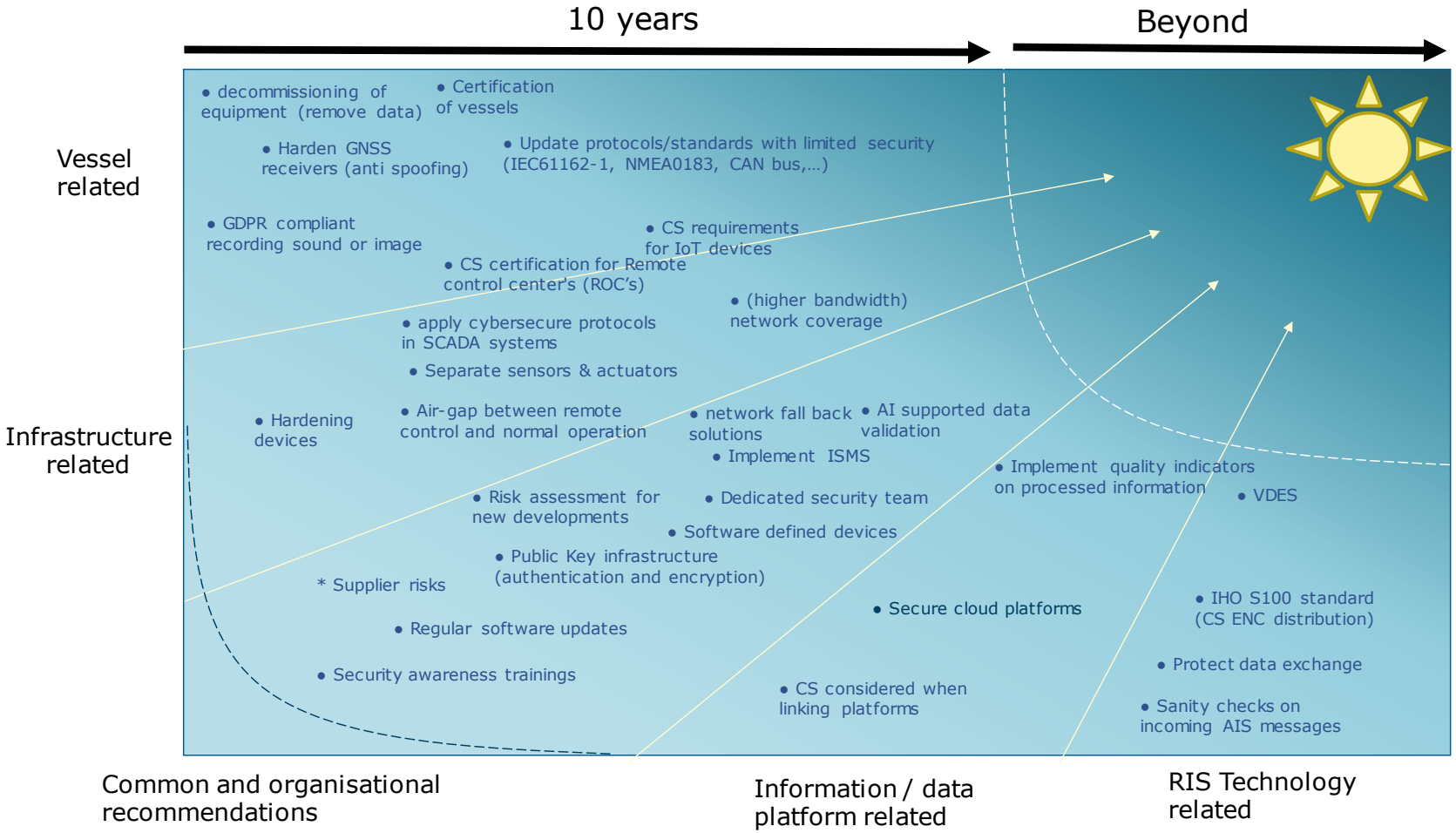


Figure 31: Recommendations per category

13 Annexes

13.1 Glossary

AI:	Artificial Intelligence
AIS:	Automatic Identification System
API:	Application Programming Interface
AR:	Augmented Reality
ASM:	Application Specific Messages
AtoN:	Aids to Navigation
BCM:	Business Continuity Management
CAN:	Controller Area Network
CCNR:	Central Commission for the Navigation of the Rhine
CESNI:	European Committee for drawing up Standards in the field of Inland Navigation
CIA:	Confidentiality, Integrity and Availability (of information)
CISO:	Chief Information Security Officer
CRA:	Cyber Resilience Act (EU)
CS:	CyberSecurity
CSIRT:	Computer security incident response team
CTI:	Cyber Threat Intelligence
(D)DOS:	(Distributed) Denial of Service
DLP :	Data Loss Prevention
DPIA:	Data Protection Impact Assessment
DR:	Disaster Recovery
DSC:	Digital Selective Calling
EC3	European Cybercrime Centre
ECDIS:	Electronic Chart Display and Information System
EDR:	Endpoint detection & response
eFTI:	Regulation (EU) 2020/1056 on electronic freight transport information
EMSA:	European Maritime Safety Agency
ENI:	European Number of Identification or European Vessel Identification Number
ENISA :	Agency for Cybersecurity of the European Union
ENC:	Electronic Navigational Chart
ERTMS :	European Rail Traffic Management System
ERI:	Electronic Reporting
EuRIS:	European River Information Services (www.eurisportal.eu)
GDPR:	EU General Data Protection Regulation
GNSS:	Global Navigation Satellite System
IALA:	Association of Marine Aids to Navigation and Lighthouse Authorities
IDS:	Intrusion Detection System
IEC:	International Electrotechnical Commission
IENC:	Inland Electronic Navigational Chart
IMO:	International Maritime Organisation
IHO:	International Hydrographic Organization
IoT:	Internet of Things
IPS:	Intrusion Prevention System
IRS:	Intrusion Reaction System
ISAC:	Information Sharing and analysis center
ISM:	Information Security Management
ISMS:	Information Security Management System
ISO:	International Standards Organisation
IT:	Information Technology
ITS:	Intelligent Transport Systems
ITU:	International Telecommunication Union
LBM:	Lock and Bridge Management

MFA:	Multi Factor Authentication
MMSI:	Martime Mobile Service Identifier
NIS:	EU Directive on the Security of Network and Information Security
NIST:	National Institute of Standards (US)
NMEA:	National Marine Electronic Association
NtS:	Notices to Skippers
OT:	Operational Technology
PNT:	Position, Navigation and Timing
PKI :	Public Key Infrastructure
QCI :	Quantum communication infrastructure
RIS :	River Information Services
ROV :	Remotely Operated Vessel
SCADA:	Supervisory Control and Data Acquisition
SECOM:	SEcure COMmunications protocol as defined in EN IEC 63173-2
SIEM:	Security Information and Event Management
SOAR:	Security Orchestration Automation and Response
SOC:	Security Operations centerTBB: Terrestrial Bulletin Board
TGAIN:	Track guidance assistants in Inland Navigation
VDES:	VHF Data Exchange System
VHF:	Very High Frequency
VR:	Virtual Reality
VLAN:	Virtual Local Area Network
VPN:	Virtual Private Network
XSS:	Cross Site Scripting

13.2 Table of figures

Co-funded by the European Union