Vision, Action Strategy of The Maritime Cybersecurity Centre

Contents

1 Mission and Vision

The Maritime Cybersecurity Centre (Centre) was established as part of the EU funded Horizon 2020 project called MariCybERA. The project aimed to create an ERA Chair (European Research Area) in Maritime Cybersecurity at Tallinn University of Technology (TalTech) by integrating the research capabilities of TalTech's Estonian Maritime Academy and TalTech's Centre for Digital Forensics and Cyber Security. This integration was intended to address the cybersecurity challenges arising from the digital transformation of the maritime industry.

The Centre has the objective of becoming an internationally recognized academic research centre that supports a secure, reliable, and sustainable maritime sector. It takes advantage of Estonia's thriving ecosystem of cybersecurity and maritime stakeholders, including the NATO Cooperative Cyber Defence Centre of Excellence, Estonian maritime associations, research institutions, and private companies.

The purpose of this strategy document is to outline the goals, approach, and activities of the Centre in fulfilling its mission to enhance the cybersecurity of the maritime sector. Overall, the Centre serves as a hub for research and collaboration, bringing together expertise from various fields to address the cybersecurity needs of the maritime industry and contribute to its long-term security and resilience.

General challenges of the maritime industries' digital transformation

The maritime industry faces several challenges in its digital transformation such as lack of standardization and interoperability, resistance to change, cybersecurity risks and growing threat landscape, limited infrastructure and connectivity, integration with existing systems and processes, costs, regulations as well as compliance, and legacy infrastructure. However, despite the challenges, as supply chains are playing a central role in the world

economy, the digital revolution is crucial to the industry as it brings positive impact, while bearing major disruption risks. Digital transformation is coming with deep structural, organizational, and operational changes that will impact the way seafarers work, and the way vessels and infrastructures are designed and built. Maritime business processes at the core of maritime transport are also undergoing major transformations, which entail changes in the education and the careers of professionals in this industry, requiring everyone to learn new skills. These elements have resulted in the digitalization of maritime industry becoming the main emphasis of the United Nations Conference on Trade and Development (UNCTAD). The 2014 European Union Maritime Security Strategy (EUMSS), along with its 2018 action plan, has also emphasized the importance of this for the future of the EU. Leveraging on existing maritime future strategy documents, three categories of challenges can be extricated to address in priority in relation to digital transformation of maritime industries:

- **The ships and maritime infrastructure**

The first category of challenges relates to ships and maritime infrastructures. The goal is to create ships and infrastructures that have lower ecological footprint, reduced operation costs, are highly efficient, while also relying on secure and trustworthy digital systems that provide more autonomy, and higher operational flexibility in operations. While this will lead to Maritime 4.0, at the same time the widespread installation of Information and Communication Technology in the ships and infrastructures has increased their attack surface and made them more vulnerable to cyberattacks. Addressing this issue will require significant focus on and investment in cybersecurity research, which is directly related to fundamental research questions like trustworthy artificial intelligence and balancing security and performance trade-offs with the global objective to reduce human and economic risks from cyberattacks.

- **The digital maritime environment**

Digital transformation comes to the maritime industry with the promises of smoother and more secure information exchange, dematerialization of business processes, improved transparency and openness, and better integration of maritime sector into digital economy. This requires the creation of a supportive environment and an ecosystem, including regulations, policies, strategies, and digital infrastructures to foster the growth of maritime business processes. Cybersecurity is a fundamental requirement of this environment, as trust plays a central role in the logistic chains that form the backbone of maritime processes. The increased business flexibility and innovative business models brought about by the digital tools and infrastructures must be balanced with the cybersecurity risks, requiring closer cooperation and information exchanges among stakeholders. This opens several research avenues aiming to building and securing multi-stakeholders' information exchanges and trust.

- **The societal environment**

Maritime sector has played historically a central role in the economies of coastal countries and in their job markets. The digital transformation of the maritime sector will have major and challenging societal impacts. In a nutshell, the major challenge is to make maritime careers more appealing to the new generation by providing education and training in digital skills, analytic abilities, and cybersecurity awareness. To keep up with these changes current professionals also need to be equipped with digital skills and cybersecurity awareness. This requires the creation of new further education platforms, developing lifelong education programs that will transfer the skills needed to work in the digitalized maritime industries. This entails the creation of new expertise sharing platforms, workplaces, and exchange hubs to support all stakeholders and facilitate structural and societal changes in the maritime sector. Cybersecurity is a major aspect of this new set of skills, competencies, and expertise that must be imparted to both to the new generation of seafarers and to the currently working professionals. This is a large endeavour as maritime education happens at different levels in the society: for youngsters in yacht clubs, in vocational high schools, in maritime academies, in universities, in companies, etc. Moreover, several national and international frameworks regulate the education and the qualifications of maritime professionals. The mandatory curricular change is made more difficult in the seafarer education, as it must pass through an international accreditations process. However, if the goal is a resilient human workforce in the sector, these changes need to start.

1.1 Objectives

- **Conduct Research**

The first and main objective of the research Centre is to carry out fundamental research on maritime cybersecurity and promote best practices. The Centre will strive to stay at the forefront of research in this field, and to disseminate its findings to industry stakeholders to raise awareness and improve cybersecurity preparedness.

- **Provide Education**

The Centre will also provide training and support, to industry stakeholders disseminating its findings to raise awareness and to improve cybersecurity resilience. Through various training programs, the Centre will aim to equip maritime professionals with the knowledge and skills necessary to understand and address cybersecurity challenges in the industry. This will include winter and summer schools, hackathons, seminars, postgraduate education.

- **Foster Partnerships and Collaborations**

The third objective of the research Centre is to collaborate with other academic institutions, industry partners, and government agencies. It will encourage and facilitate international cooperation on maritime cybersecurity research and best practices, contributing to a safer and more secure maritime industry. By working with stakeholders across borders (in the Baltics, Nordic countries and beyond), the Centre will strive to ensure that the best ideas and practices are shared and adopted widely.

To achieve its objectives, the Centre will focus its research efforts and secure its long-term sustainability. The Centre's research focus must be in line with its objectives and guided by its mission to develop advanced cybersecurity solutions, conduct fundamental research, foster partnerships and collaborations, and encourage international cooperation. In the followings the Centre's research priorities and how it plans to allocate its resources to achieve its goals will be outlined. Additionally, the Centre's funding and revenue streams and how it plans to ensure its long-term financial sustainability will be discussed, ensuring that it can continue to fulfil its mission and achieve its objectives in the years to come.

2 Research Focus and Sustainability

2.1 Research focus

The research focus of the Centre is on developing innovative solutions to address the emerging security challenges in the maritime industry. This includes studying the threat landscape, identifying vulnerabilities in maritime systems, and developing cybersecurity measures to mitigate the risks posed by cyber-attacks. A key aspect of the research is to understand the unique challenges posed by the maritime environment, including e.g., limited connectivity and the need for real-time information exchange. Focusing on these specific areas, the Centre can ensure that its research has practical applications and can help to improve the cybersecurity of the maritime sector.

Focus aim: To conduct and support fundamental research in the field of maritime cybersecurity, to better understand the evolving threats and to develop new solutions in the later defined three main research areas of focus.

Key activities and timing: The Centre will carry out interdisciplinary research on various aspects of maritime cybersecurity. Initially two research groups are established to address the research focus areas and commence research in the designated areas.

Key performance indicators:

- Number of academic publications,
- Number of open access publications,
- Number of industry contracts,
- Number of winter/summer schools and other workshops organised,
- Number of PhD students affiliated with the project,
- Number of submitted grant applications,

- Secured funding.

The Centre is dedicated to advancing the state of the art in cybersecurity for the maritime industry. To achieve its goal, two key focus areas for the research have been identified: “Technical dimensions of cybersecurity in maritime technology”, and “Human Aspects of Maritime Cybersecurity”. In the following paragraphs, each research area, and the strategy for pursuing research in these critical areas will be briefly outlined.

2.1.1 Research focus on Technical Dimensions of Cybersecurity in Maritime Technology

Member States of the International Maritime Organization (IMO), meeting at the Marine Environment Protection Committee (MEPC 80), have adopted the 2023 IMO Strategy on Reduction of Greenhouse gas-neutral (GHG) Emissions from Ships, with enhanced targets to tackle harmful emissions. The indicative checkpoints to reach net-zero GHG emissions from international shipping are to reduce the total annual GHG emissions from international shipping by at least 20%, striving for 30%, by 2030, compared to 2008; and to reduce the total annual GHG emissions from international shipping by at least 70%, striving for 80%, by 2040, compared to 2008. The EU has set an even more ambitious target of achieving GHG-neutral maritime transport by 2030. Despite these goals, the increasing maritime traffic presents significant challenges for the design, building and operation of ships and infrastructure to reduce the ecological footprint and operational costs to become more efficient through the widespread use of digital Operational Technologies (OT) and Information Technologies (IT) leading to Maritime 4.0.

The large-scale implementation of Information and Communication Technology creates a substantially vulnerable surface of these systems for the actions of malicious actors. This implies that the increased autonomy, greater operational flexibility, and lower environmental impact promised by digitalisation in maritime technology must be balanced with reliability and security. Secure-by-design principles should be integrated into the development life cycles of maritime systems to conveniently provide an optimal balance between security and performance with the overarching goal of minimising both human and economic risks caused by cyber-attacks. Thus, **one significant research line will be to develop and adapt methods that address the security efforts in the development life-cycle (e.g., requirement analysis, verification, implementation, maintenance) and showcase their applicability in the case studies selected from the ships and maritime infrastructures.**

Maritime systems are expected to benefit from various AI-based system components, raising concerns about the new security threats that may target the relevant development cycles and operational systems. **Conventional cyber-attacks that can expose the vulnerabilities of software, hardware and network components of AI-related assets and adversarial attacks launched against the data pipelines and operational systems constitute a major threat category** (i.e., it is highly likely to have a combination of conventional and adversarial cyber-attacks). Understanding these cyber threats within the context of maritime systems and developing effective countermeasures will be an essential part of the research agenda.

The abovementioned research activities will be complemented by the **research area focusing on developing security monitoring methods and tools that can be adapted and integrated into maritime systems**. This research line presents unique challenges, such as adapting existing intrusion detection and security information and event management (SIEM) systems to the maritime domain. Traditionally, monitoring of operational technology (OT) and information technology (IT) has been pursued separately. However, this area recognises the need for a more holistic approach that effectively monitors cyber-physical systems such as ships and maritime infrastructures. At the core of these applications lies a research challenge, effectively merging heterogeneous information with different temporal granularity to attain comprehensive security monitoring for better risk-based decisions. The data obtained from sensors about the situations in physical space will be fused into the monitoring data that aim to capture the activities of malicious actors in cyber space. Thus, operational, and tactical decision-makers will be better informed about the likelihood and impact of cyber-attacks.

2.1.2 Research focus on Human Aspects of Maritime Cybersecurity

Cyber-risk assessment based on human behaviour and interventions for behaviour change

- *Research on evaluating and quantifying education and large-scale exercise outcomes.*
- *Research on the use of simulator for cybersecurity awareness and optimization of system usability*

In maritime cybersecurity, international institutions have acknowledged the significance of focusing on human factors. International Maritime Organization (IMO), a United Nations specialized agency, has acknowledged the importance of human factors in maritime cybersecurity. The Maritime Safety Committee (MSC) of the IMO have been actively addressing cybersecurity issues, and their resolutions and guidelines stress the need for training, awareness, and human-centric approaches to improve cybersecurity in the maritime industry. In addition, the International Association of Classification Societies (IACS) has acknowledged the significance of human factors in cybersecurity and stresses the need to address human factors, training, and awareness programs in order to strengthen cybersecurity practices in the maritime sector. The European Union Agency for Cybersecurity (ENISA) report sets guidelines for human factors in maritime cybersecurity emphasizing the importance of addressing human factors, such as training and user awareness, when securing Internet of Things (IoT) devices in critical infrastructures, such as the maritime sector. The International Association of Maritime Universities (IAMU) has organized conferences and published research papers on maritime cybersecurity, which frequently include discussions on human factors, training, and organizational resistance to cyber threats.
The human aspects dimension focuses on human-technology interactions, as described above, as well as maritime operational personnel training, human-artificial intelligence (Human-AI) interactions and trustworthiness and building organizational resilience against cyber threats. **Humans play an important role in the maritime domain, and their actions can have an immediate effect on cybersecurity. Focusing research on these areas will enhance the maritime industry's cyber defence capabilities by enhancing organizational resilience against cyber threats.**

Maritime operational personnel research in the maritime industry, crews and port administrators are the first line of defence against cyber threats. To equip them with the knowledge and skills necessary to identify, prevent, and respond to cyber-attacks, it is essential to implement effective training programs. **Research on personnel training can aid in the design and implementation of effective training approaches that can increase cybersecurity-aware culture and behaviours, foster responsible cybersecurity practices, and reduce the risk of human error resulting in cyber incidents.** Such maritime cybersecurity training programs can be evaluated using a variety of techniques to determine their efficacy and identify areas for enhancement (e.g., knowledge assessments, simulation performance evaluations, and real-world cyber defence scenarios). Approaches to training and assessing competency development may utilize the Maritime Academy's infrastructure, i.e., simulators, cyber defence labs, that include incident response exercises where assessments of response times, coordination, communication, and decision-making under pressure can be measured, and help develop key performance indicators (KPIs) to measurements of reduced incident rates, improved incident response times, enhanced employee awareness, or increased report volume.

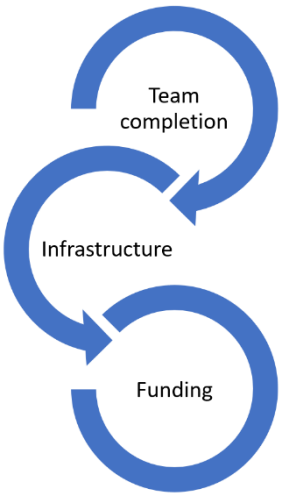
Human-AI interactions will also be the focus of human aspects research. Integrating artificial intelligence (AI) systems into maritime operations has several advantages, but also introduces new obstacles. **Understanding how humans interact with AI systems, establishing confidence in their capabilities, and addressing potential vulnerabilities are crucial**. Human-AI interaction research can result in the creation of user-friendly interfaces, effective decision support systems, and trustworthy AI-based cybersecurity solutions. Increasing confidence in AI technologies enables human operators to effectively leverage their capabilities and make informed decisions in cyber threat situations. Studying human-AI interaction in the context of trust development and repair, and decision-making may involve examining psychological processes and conducting experiments to understand how humans perceive, trust, and make decisions based on AI systems. Experimental studies can aid in the identification of trust levels, cyber threat situations, and decision-making processes. Assessing the cognitive load experienced by individuals during human-AI interactions by measuring psychological factors such as mental effort, attention, and working memory can also aid in understanding how AI trust formation is influenced, as well as how AI influences cognitive processes and decision-making. This information can be used to inform the design of AI systems, user interfaces, and training programs to optimize human-AI collaboration and increase

confidence in AI technologies.

Focus will also be placed on the investigation of organizational resilience factors against cyber hazards. The sophistication and rate of evolution of cyberthreats are accelerating. Organizations in the maritime industry must develop resilience to effectively withstand and recoup from cyberattacks. **The emphasis of organizational resilience research is on the development of robust cybersecurity frameworks, cybersecurity governance, and cybersecurity policies where the effectiveness of existing policies, the identification of gaps or challenges, and the identification of strategies for improved cybersecurity governance can be determined.** Additionally, investigating and evaluating how maritime organizations identify, assess, and manage cyber risks and threats can assist in identifying areas for development in responding to and recovering from cyber incidents. Exploring the role of organizational culture in shaping cybersecurity practices and behaviours entails examining the factors that influence cybersecurity awareness, determining how organizational culture influences employee attitudes toward cybersecurity, and identifying strategies for fostering a cybersecurity-aware culture. This includes the adoption and implementation of technology and intersectoral communication. By examining these organizational aspects, researchers can contribute to the development of best practices, guidelines, and frameworks that enhance the maritime organizations' cybersecurity posture. This research can help mitigate cyber risks, safeguard vital maritime infrastructure, and ensure the maritime sector's secure and resilient operation.

2.2 Sustainability

The Centre for Maritime Cybersecurity recognizes the importance of sustainability, and it is committed to ensuring the enduring excellence of the centre. In response to the challenges posed by digitalisation in the maritime industry, the Centre will concentrate on developing innovative solutions to address emerging security concerns. Sustainability holds central position in the Centre's strategic framework. This entails ensuring both the sustainability of its research activities and the sustainability of the solutions it develops. In terms of research sustainability, the Centre aims to establish robust partnerships with industry, government, and academia to ensure that its work remains sustainable, relevant and up to date. Concerning the sustainability of solutions, the Centre will strive to develop solutions that are economically viable and can be easily integrated into existing systems. By prioritizing sustainability, the Centre will help to ensure that its work has a lasting impact and continues to contribute to the security of the maritime sector well into the future.



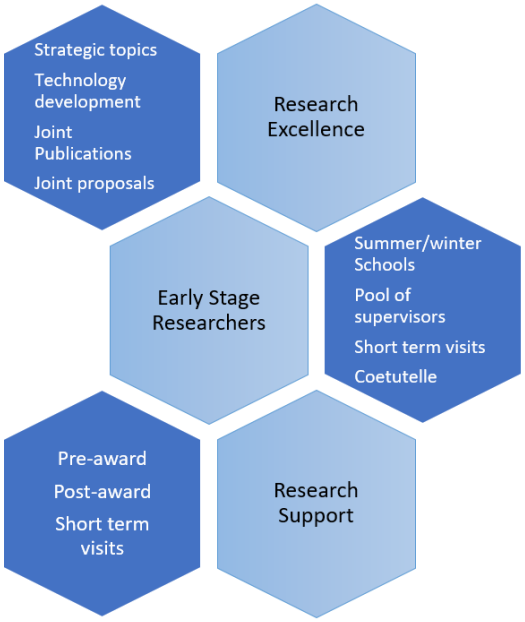
The Centre's sustainability is supported by four individual pillars that mutually reinforce each other:

1- Research excellence and institutional acceptability

2- Human resources and infrastructure

3- Financial resources

4- Collaboration



The MariCybERA project funded by the EU, was initiated with the goal of establishing a sustainable centre of centre of excellence in maritime cybersecurity. The Centre's sustainability will be ensured through its long-term relevance within TalTech's academic environment, defined through a balance of education and research efforts. This balance aligns with TalTech's overall strategy, which is achieved through an interactive process between the university and the Centre.

The Centre operates as a multi-disciplinary entity that collaborates with different units within TalTech such as the TalTech Centre for Digital Forensics and Cyber Security under the department of software Science, and the Estonian Maritime Academy (the main stakeholders, the applicants for the ERA chair grant). It also collaborates with other departments, such as the Dependable Software RG the Department of Power Electronics and Mechatronics (involving the "NYMO robotic vessel" project), the School of Business and Governance, and the Thomas Johann Seebeck Department of Electronics, etc. The Centre is aiming to work efficiently within this institutional environment and receive support from the various stakeholders, fostering complementary and mutual benefits.

TalTech has defined a strategic plan for the period 2021-2025 that encompasses studies and research activities, entrepreneurship, and relations with society, and organizational management components. This global strategic plan was translated into a dialogue with faculties and departments that resulted into concrete objectives, key performance indicators, and operational goals. The Centre for Maritime Cybersecurity must align itself with these objectives to become sustainable.

Research excellence is a key ingredient of TalTech's strategic plan and therefore it is a major objective of the Centre. This includes a focus on conducting high-impact research, publishing in high-quality and highly visible journals, and attracting talented researchers. These efforts will have significant impact on the research community and beyond. The Centre should also align with TalTech's educational initiatives, including the strategic emphasis on cooperation with EUROTEQ, and the doctoral program.

2.2.1 Human resources and Infrastructure

Human resources and infrastructure are the backbone of the Centre and play a pivotal role in achieving its objectives. The Centre's strong foundation in human resources and infrastructure enables it to attract and retain the top talent and provide the necessary facilities and equipment to support research activities. Strategic approaches are essential to ensure continued success and impact of the Centre in the field of maritime cybersecurity.

2.2.1.1 Human resources

The Centre employs a strategic approach to recruit and retain highly skilled professionals with experience in IT, cybersecurity and maritime operations from withing TalTech. This ensures that the Centre has the necessary knowledge, skills, and access to expertise, to carry out its research effectively. Recruitment procedures are aligned with the (https://op.europa.eu/en/publication-detail/-/publication/6ab3ec79-8e10-11ec-8c40-01aa75ed71a1/language-en) 40 principles of the EC's Charter for Researchers and Code of Conduct for the Recruitment of Researchers, with customization as necessary. The Centre is also exploring the possibility of applying for the EC's HR Excellence in Research Award.

To foster sustainability, the Centre recruits employees at different level of experience, who are involved in activities related to education, research and innovation. To achieve objectives in the research areas, the following types of recruits are considered:

- Academic staff

1. Senior research fellows
2. Post-doc and mid-career researchers
3. PhD students/Early-Stage Researchers
4. Master's or undergraduate level students (interns).

- Non-academic staff
  5. Research managers for pre- and post-award
  6. Partnership and technology officer

The Centre temporarily utilizes staff from other structural units of the University, hires individuals on temporary contracts, subcontracting, and other similar agreements.

Strategy of Human Resource recruitment includes the following initiatives to enhance the attractiveness of the field of maritime cybersecurity:

- Development of postgraduate training programs in maritime cybersecurity to create a pipeline of PhD and postdoctoral researchers.
- Generating interest in doctoral studies among students in master's programs, such as the one-year maritime digitalization program (starting in 2023/2024)
- Participation in sectoral events and training programs to attracts talent through targeted searches in the Centre's network.
- Developing pre- and post-award project support through professional training programs, short-term visits (2-4 weeks) to strategic partners, structural changes, and sharing best practices to support the professional development of research managers and researchers.
- Utilizing financial instruments for recruiting human resources, including base funding, target funding, and project-based fundings.
- Prerequisites for obtaining financial instruments include establishing an ERA Chair Training program to develop research management, project writing, and project management skills, improving performance in national and EU R&D funding programs, and effectively disseminating the results of the ERA Chair.

2.2.1.2 Infrastructure

Infrastructure has important role in enabling sustainable research and education within the Centre. To facilitate productive work, it is essential for everyone to have designated workstations and access necessary testing facilities. To support the development of the framework for research and innovation, and technological development, the Centre recognises the need for modern infrastructure and continuously assesses available opportunities for infrastructure development, renewal.

The Centre is equipped with the following infrastructure:

- Developed workplaces, providing conducive environment for research and collaboration (ca 10);
- Maritime cybersecurity research and study lab, which includes:
  - Learning and study environment,
  - Testing environment comprising a testbed for hardware and software.
- Access to the simulators of the Estonian Maritime Academy
  - Simulation environment including online/software based simulations;
  - Global network of simulators.
- High-Performance Computing (HPC) resources available at the School of IT.
- Access to research vessel, enabling hands-on experimentation and data collection.

Laboratories and infrastructure of strategic partners through strategic collaborations, these already established collaborations are:

- National infrastructure and expertise, such as the CR14 cyber range.
- Private sector infrastructure and expertise including NYMO, autonomous robotic vessel.
- International infrastructure and expertise, such as the digital twin at NTNU Aalesund and the HPC/virtualisation platform at XAMK, Kotka.

In terms of infrastructure strategy, the Centre plans to expand the Autonomous System Research lab into an experimental lab focusing on offensive tools for maritime cybersecurity. The expansion aims to enhance the Centre's capabilities in addressing emerging challenges and advancing research.

The coordination and management of infrastructure within the Centre are overseen by the Director for Research and Development at the Estonian Maritime Academy, with support from the ERA Chair holder, heads of research directions and the Research Administration Manager.

2.2.2 Education and Training

The Centre recognizes the importance of education and training in advancing cybersecurity in the maritime sector. In collaboration with other TalTech programs, the Centre will develop a range of educational and training activities to deepen understanding and engage with leading researchers in the field. These activities will provide hands-on trainings, lectures and workshops to expand knowledge, build skills, and make valuable connection with others in the community.

The Centre's commitment to education is an essential part of its mission of driving progress and innovation in maritime cybersecurity. One of the objectives is to offer a diverse range of education and training programs to various stakeholders. These programs aim to raise awareness about importance of cybersecurity and equip participant with practical skills and knowledge to protect against cyber-attacks. A specific focus is on enhancing the general level of awareness and resilience of the students of the Estonian Maritime Academy.

To achieve these goals, the Centre will offer workshops, courses, and training programs dedicated to maritime cybersecurity. These initiatives aim to provide participants with valuable insights, practical skills and up-to-date knowledge regarding the latest threats and effective and to raise awareness of the latest threats and mitigation techniques. The Centre seeks to ensure that these programs make a tangible impact on the cybersecurity landscape. Summer and winter schools will be organized jointly with collaboration partners with guest lecturers from all the strategic partners supporting the programme.

Key performance indicators for the success of these educational and training activities can include the number of programs offered, the number of participants who engage in these activities, and feedback received from participants, which can provide valuable insight into their effectiveness and relevance. By monitoring these indicators, the Centre can continuously evaluate and improve its educational offerings to meet evolving needs of the maritime community.

2.2.3 Supporting and promoting early-stage researchers (other supporting activities)

Active search for additional funding: the Centre will actively seek for additional funding to support the events for early-stage researchers. These events could include workshops, conferences, seminars, or other activities that provide valuable learning and networking opportunities for young researchers.

Pool of supervisors: to support the PhD studies and share the excellence between partners, also building connections to pillar research excellence, the Centre aims to establish a pool of supervisors. The initiative promotes collaboration and knowledge sharing among different research institutions and partners.

Platform for short term visits: Aiming to set up a platform to facilitate short term visits (2-4 weeks) for early-stage researchers to take part in summer and winter schools and visit supervisors.

Preparatory course for PhD studies: The Centre plans to offer a preparatory course to help future PhD students get ready for their doctoral studies. This course aims to introduce them to the possibilities available in their field of study and connect them with potential supervisors. This serves as a foundation to their research journey.

Career planning support: Preparatory course for PhD studies to prepare future students, introduce the possibilities and supervisors. Also, develop in collaboration with partners a career planning support model for early-stage researchers.

2.2.4 Financial short- and long-term sustainability

The long-term financial sustainability of the Centre is necessary for the development of a successful maritime industry and excellence in maritime cybersecurity. The Centre relies on various sources of funding, including Governmental funding, European Union funding and support from private sector and non-profit organizations.

In the Short-term, the centre seeks funding through base funding that includes:

- 75% support for doctoral students,
- basic funding for curriculum development,
- teaching digital skills and cybersecurity in maritime sector,
- addressing national interests and needs (ie fleet requirements)

The funding goal for short-term sustainability is to secure permanent funding of 400 KEUR.

In the Long-term, the Centre aims to secure a targeted funding such as

- sectoral targeted fundings,
- education (maritime, digital skills, cybersecurity, etc.)
- science (maritime, digital skills, cybersecurity, etc.)

Competitive funding opportunities, including grant agreements (ETAG Grants) and funding calls from the European Commission (i.e., Horizon Europe) are also considered. The funding goal for long-term sustainability is to secure 15+ national proposals and 10+ European proposals, amounting to 700 KEUR per year.

Additionally, procurement contracts with organisations such as OLAF, EDF and private sector entities from the maritime and cybersecurity sectors (e.g., Port of Tallinn, Tallink, Guardtime, Cybernetica, CybExer etc.) are pursued, with a funding goal of 3-5 agreements, totalling 150 KEUR per year.

Intellectual Property (IP) licensing through patenting cybersecurity technologies is also considered as a potential funding source, although it is important to note that patenting is not the primary goal of the Centre's research activities.

To ensure a sustainable funding strategy, the Centre aims to Increase its independence in executing funding proposals and procurement contracts. This includes improving performance through training and practice programmes to increase the success rate of proposals in national and EU R&D funding programmes, as well as effective dissemination of the Centre's results.

The coordination and the management of funding activities within the Centre are overseen by the Director for Research and Development at the Estonian Maritime Academy, with the support from the ERA Chair holder, heads of research directions, and the Research Administration Manager.

2.2.5 Collaboration principles

The Centre regards collaboration as fundamental principle and actively seeks partnerships with industry, government, and academic organizations, to leverage collective knowledge and resources, and to work together to address the common challenges of maritime cybersecurity. The aim is leverage collective knowledge and resources through joint projects and initiatives. The centre's key activities include participation in collaborative projects, sharing information, expertise, and resources with partners in various sectors. The number of partnerships and collaborations established can serve as key performance indicators for measuring success in this area.

Complementarity

Recognising the broad scope of maritime cybersecurity, the Centre aims to collaborate with partners who possess complementary expertise. This approach ensures that the Centre avoids direct competition in areas where established expertise already exists and focuses its efforts on areas where mutual benefit and complementarity are evident.

Access to resources

Access to resources is the second fundamental element for effective collaboration. The Centre seeks access to three main categories of resources: talented early-stage researchers, experimental facilities, and expertise in areas where the Centre may lack proficiency. This access to resources enhances the Centre's research cooperation and enables it to leverage the strength and capabilities of its partners.

Strategic positioning

Strategic positioning is a vital asset sought though collaboration. By strategically positioning itself within the environment that impacts the goals of the Centre, such as the Excellence hub, the Centre can engage with stakeholders in the Baltic region or wider in Europe to build network of relationships. This Strategic positioning will contribute to achieving the objectives of the Centre and enhance its influence.

Strategic partner profiles

The Centre welcomes different type of partners to strengthen its strategic goals. These partners include academic and research institutions, entrepreneurial entities (industry, SMEs, spin-offs, etc.), governmental bodies (ministries, local governments), and third-sector organisations (NGOs, associations). Strategic partners should possess expertise in the field and align with the Centre's strategic goals.

The collaboration process follows five-step approach.

Step 1: forming a dedicated team and identifying relevant partners within TalTech.

Step 2: finding national partners from different sectors to map the needs and expertise and establish a national maritime cybersecurity network platform.

Step 3: developing collaboration with Baltic States, Nordic countries, and Baltic Sea countries.

Step 4: collaboration extended to other European areas (UK, France, Romania, Cyprus etc.).

Step 5: collaboration with other countries, expanding the Centre's reach and impact.