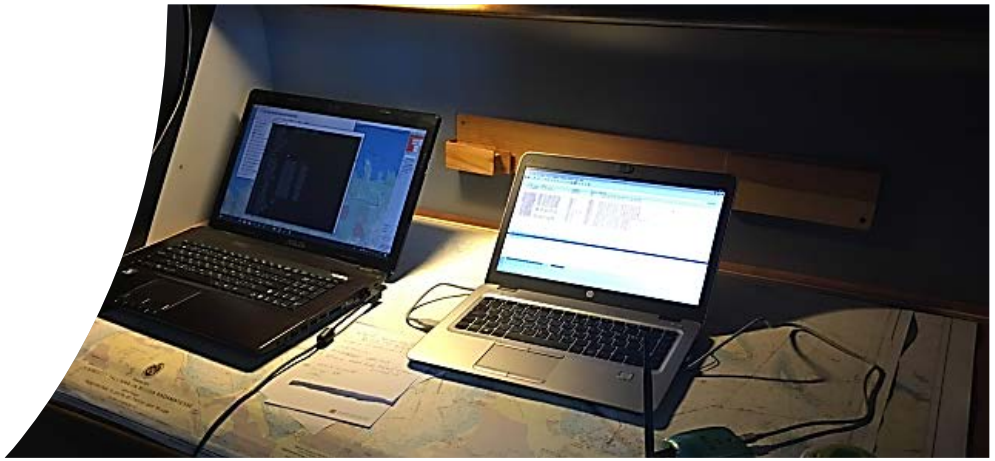
The Educational Package 'Digital Skills II'

How does it work and how can your institution benefit from it?

Dan Heering, MSc
Early Stage Researcher
TalTech Estonian Maritime Academy



Co-funded by the
Erasmus+ Programme
of the European Union

Bio

- Estonian Maritime Academy (2000)
- Deck officer in worldwide trade
- Public and private sector (Estonia, Norway)
- Director for Development at EMERA (2017 - 2019)
- MSc research on cybersecurity awareness (2017)
- PhD student at TalTech (2018 – …)
- Projects (MariCybERA, SkillSea, Human Xfactor)
- Teaching at EMERA:
  - Digitalisation in shipping (MSc)
  - Introduction to cybersecurity (BSc)

Co-funded by the
Erasmus+ Programme
of the European Union

Tallinn University of Technology and EMERA

TalTech schools

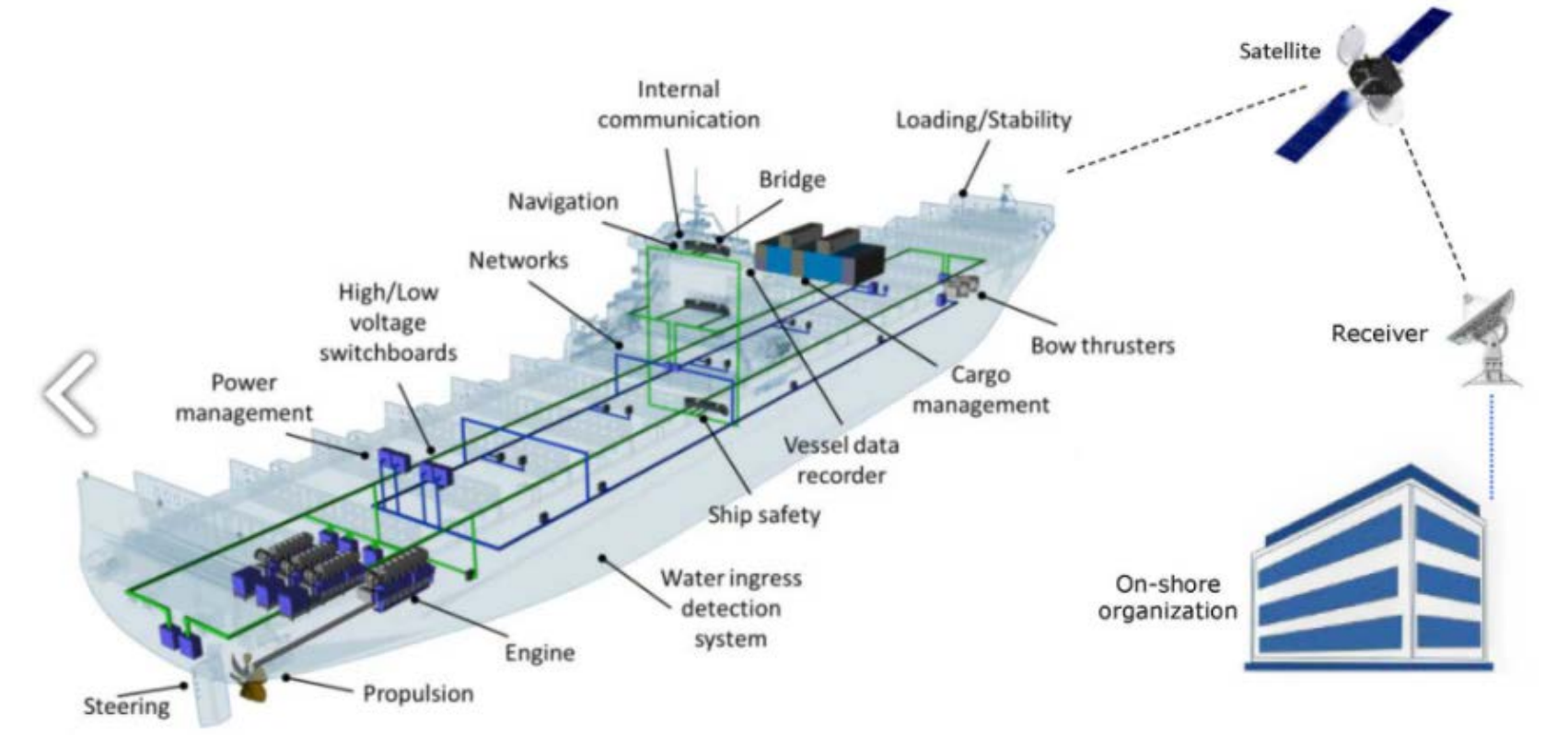
- School of Information Technologies
- School of Engineering
- School of Science
- School of Business and Governance
- Estonian Maritime Academy (2014)

EMERA study programmes

- Navigation
- Ship Engineering
- Port and Shipping Management
- Waterways Safety Management
- MSc and PhD studies

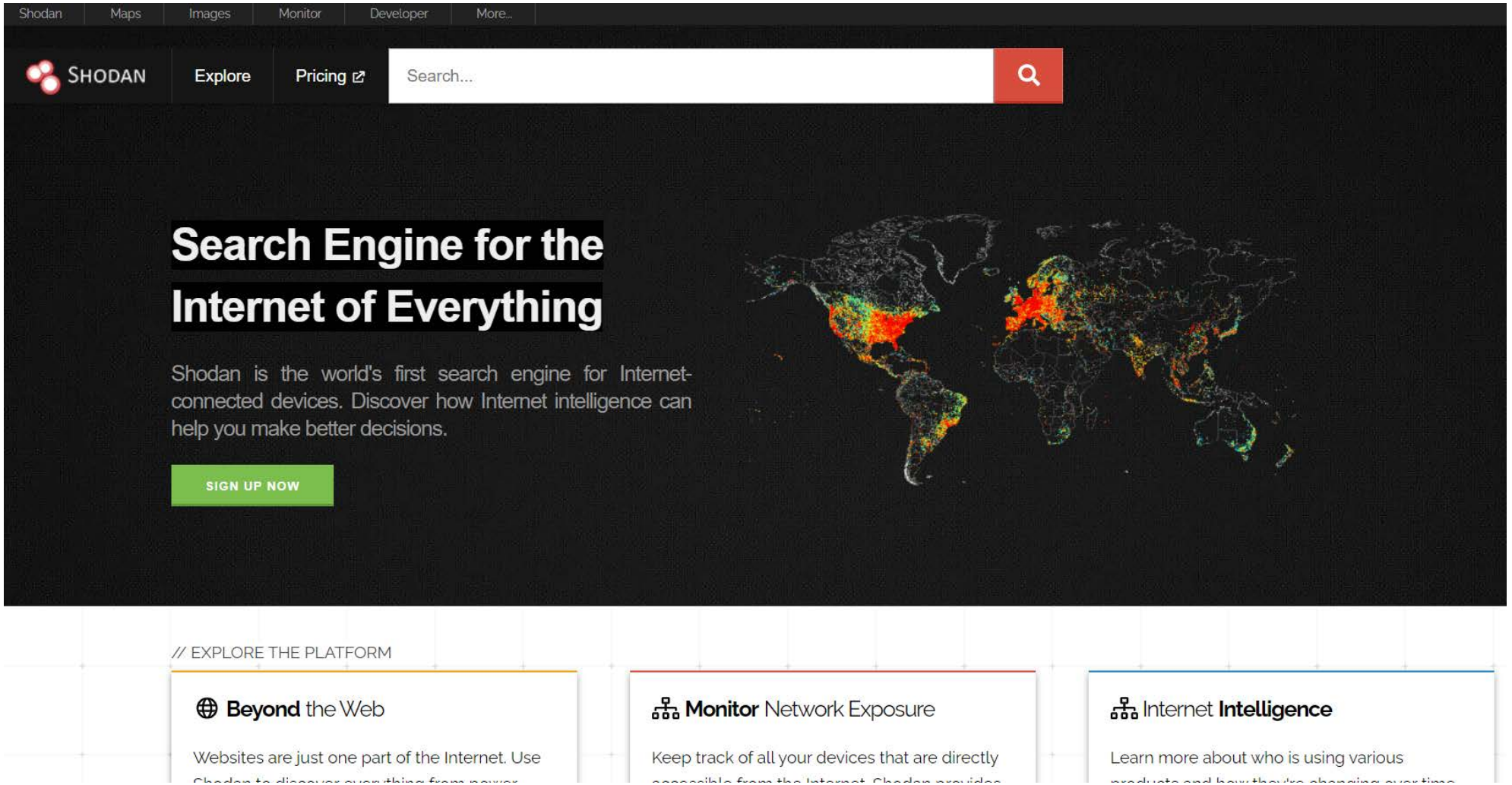
Co-funded by the
Erasmus+ Programme
of the European Union

Cybersecurity



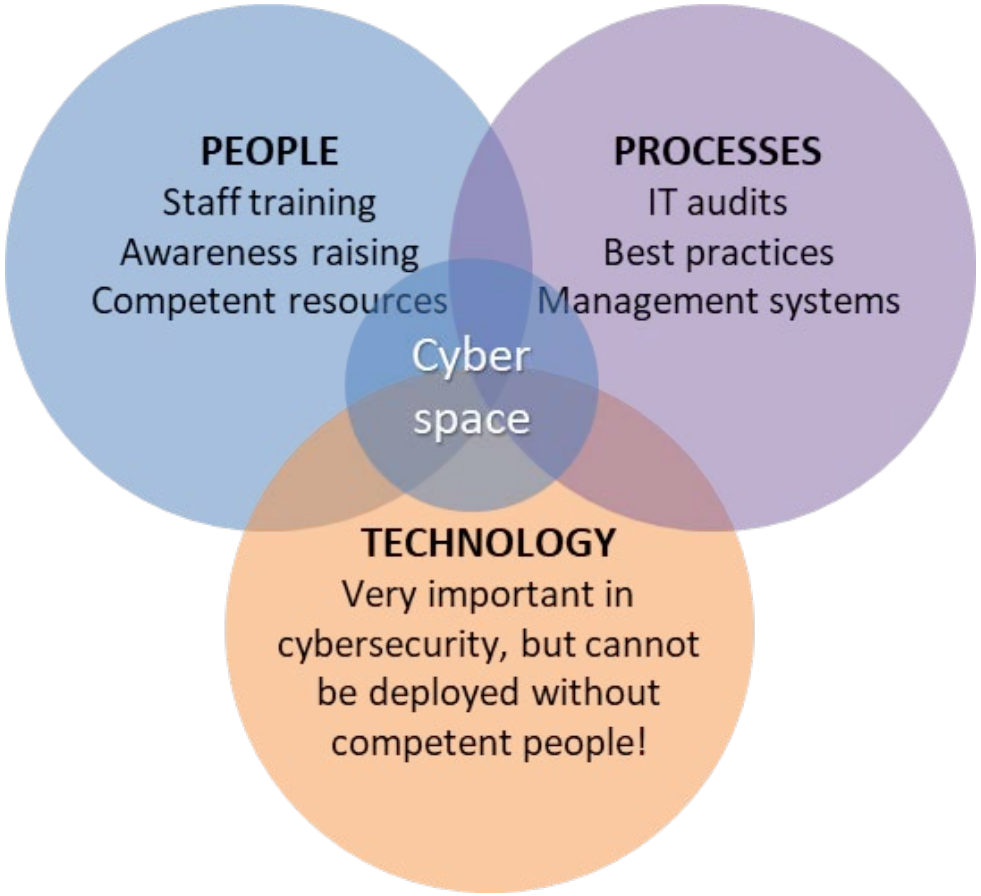
Co-funded by the Erasmus+ Programme of the European Union

Shodan.io – the Google of IoT



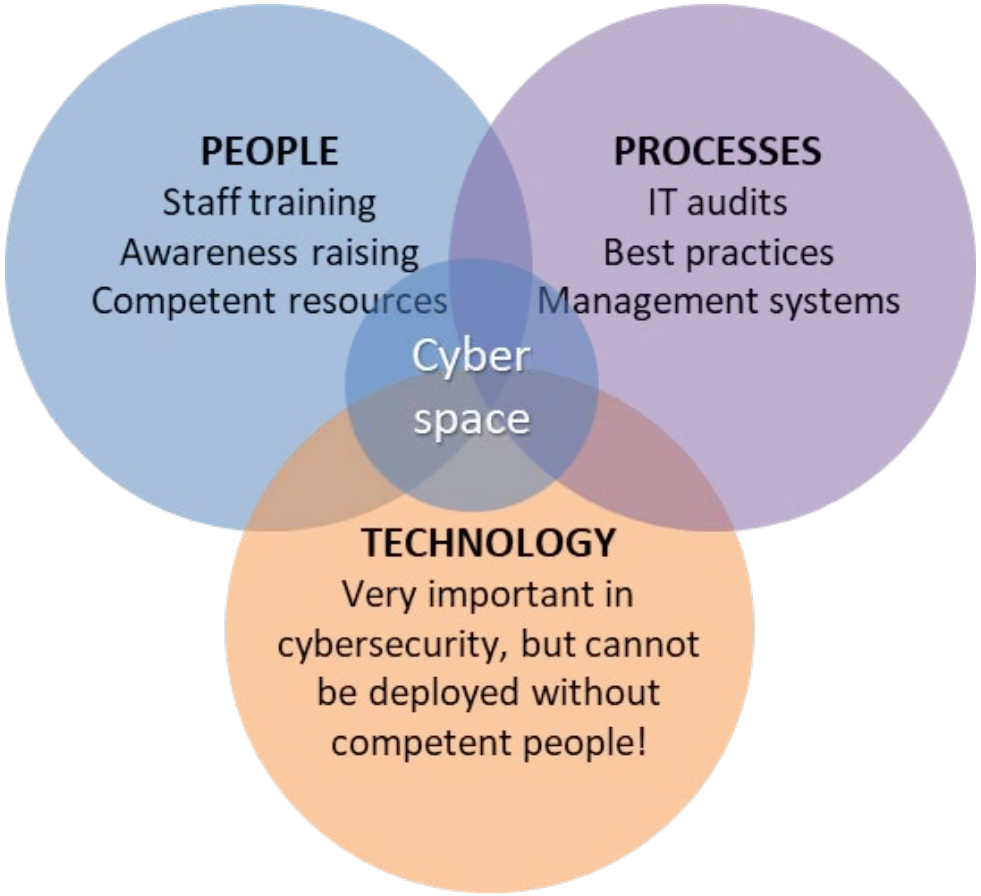
Co-funded by the
Erasmus+ Programme
of the European Union

Cybersecurity



Co-funded by the Erasmus+ Programme of the European Union

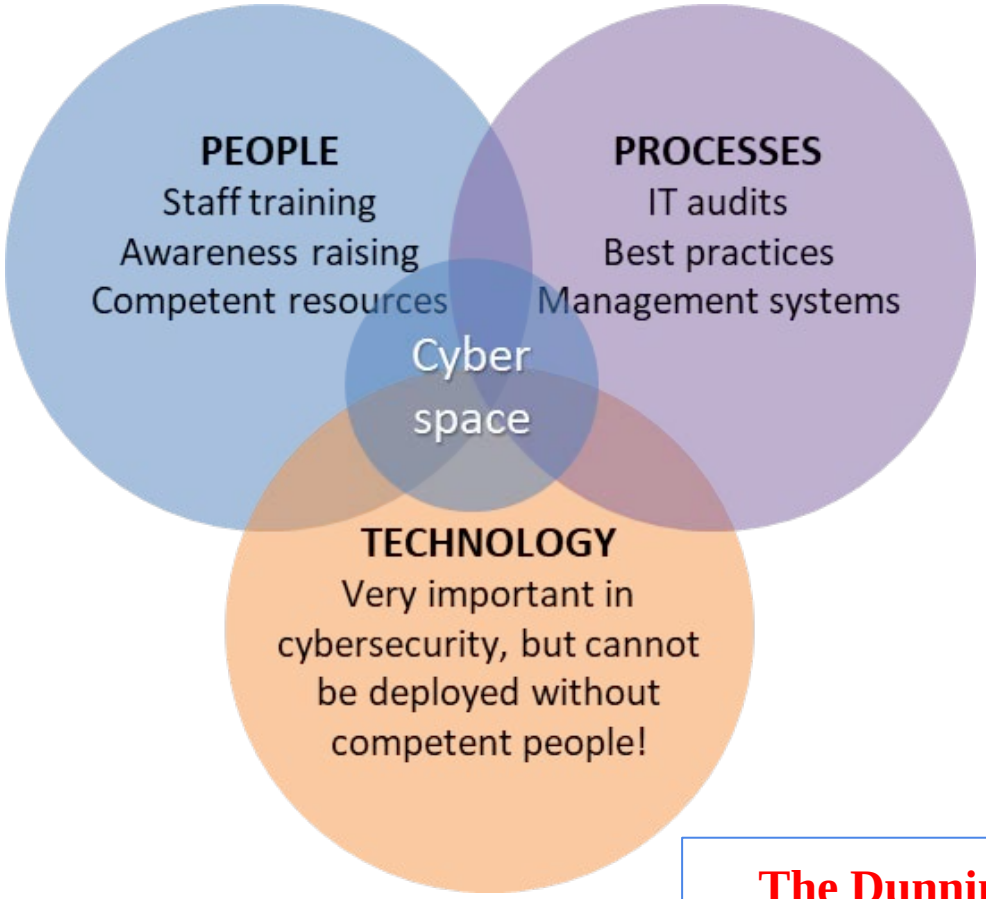
Cybersecurity



- no mandatory cyber awareness and cyber hygiene educational programmes for seafarers
- lack of knowledge and no experience to handle cyber incidents onboard ships
- no IT person onboard ships
- inability to detect anomalies or possible incidents onboard
- lack of knowledge how to preserve digital evidence for further digital forensic investigation

Co-funded by the Erasmus+ Programme of the European Union

Cybersecurity



- no mandatory cyber awareness and cyber hygiene educational programmes for seafarers
- lack of knowledge and no experience to handle cyber incidents onboard ships
- no IT person onboard ships
- inability to detect anomalies or possible incidents onboard
- lack of knowledge how to preserve digital evidence for further digital forensic investigation

The Dunning-Kruger Effect
LOP - Level of paranoity?

Co-funded by the Erasmus+ Programme of the European Union

REPORT: Current skills need – Reality and Mapping

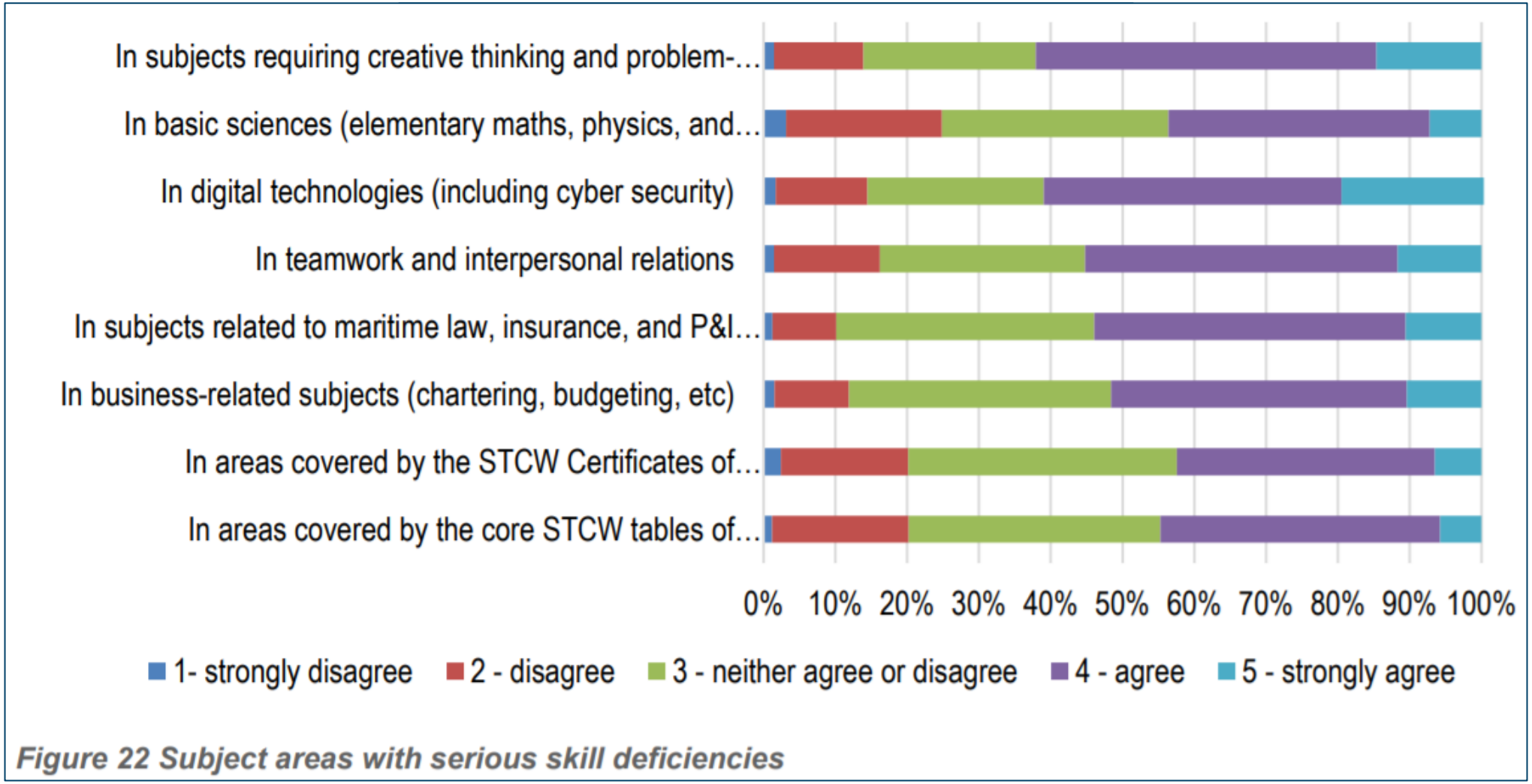


Figure 22 Subject areas with serious skill deficiencies

Co-funded by the
Erasmus+ Programme
of the European Union

Cybersecurity

- Cybersecurity has been overlooked by the maritime industry.
- Internet access across all shipping fleet sectors has significantly increased (43% in 2015 to 82% in 2019). Seafarers have identified the provision of free internet access as the most significant contribution that could be made by employers to the improvement of mental health and wellbeing on board.
- IMO requires that cyber risks are appropriately addressed in existing safety management systems (SMS) but is not requiring to have any IT personnel on board.
- There are no requirements for competence in cybersecurity awareness for a seafarers and STCW Convention does not address the digital and cybersecurity skills in seafarer's education and training, that are needed to handle modern technology and digital solutions onboard ships.

Co-funded by the
Erasmus+ Programme
of the European Union

EP of Digital Skills 2 (cybersecurity)

The following subject areas are covered by the package:

- Cybersecurity in general
  essential elements, actual context and scenarios, main threats, actors, techniques and tactics
- Maritime cybersecurity
  risks and threats for shipping industry and vessels instigated by onboard IT and OT systems vulnerabilities; digital transformation for the shipping industry and on board ships
- Legislation and guidelines
  EU framework on cybersecurity, IMO references and industry guidelines
- Maritime cyber risk management process
  key elements and best practices for maritime professionals
- Cyberattacks in the shipping Industry
  analysis and case studies

Co-funded by the
Erasmus+ Programme
of the European Union

EP of Digital Skills 2 (cybersecurity)

Target group:

- The course is intended for maritime professionals who hold responsibility positions onboard and also for ashore personnel to make them aware of the safety and security management related to cyber threats on board, in particular:
  - **Onboard**: Master, Navigating officers, Engineers, Ship Security Officer (SSO), Ship Safety Officer, and any other position identified by the company.
  - **Ashore**: Company Security Officer (CSO), Data protection officer (DPO), Designated Person Ashore (DPA), IT manager, Chief Information Security Officer (CISO), and any other position as identified by the company.

Co-funded by the
Erasmus+ Programme
of the European Union

EP of Digital Skills 2 (cybersecurity)

Estimated duration of the course

- The suggested number of contact hours is of indicatively **24 hours.**
- The contact hours may be delivered during **3 working days**, distributed over **4 weeks**.
- Also, at least **21 hours** are suggested for independent learning and research.

Co-funded by the
Erasmus+ Programme
of the European Union

EP of Digital Skills 2 (cybersecurity)

Piloting at TalTech Estonian Maritime Academy

- 38 students – 2nd year deck cadets (*„forced“ volunteers*)
- Period: November – December 2021
- 15 hours in total over 4 weeks, on Mondays (*time restriction*)
- 4 hours of independent work (reading guidelines, preparing for the class, videos)
- Via MS Teams + Moodle platform
- 1 lecturer

Co-funded by the
Erasmus+ Programme
of the European Union

Learning outcomes

Knowledge and understanding

- Understand essential cybersecurity terms and concepts.
- Identify main cyber risks and threats, threat actors and their objectives.
- Recognise and assess potential cyber risks and threats on board (IT and OT systems).
- Indicate and summarise the EU legal framework and guidelines, and IMO guidance on maritime cybersecurity.
- Summarise the Cyber Risk Management process according to the relevant maritime-related guidelines.

Co-funded by the
Erasmus+ Programme
of the European Union

Learning outcomes

Skills and competences

- Interpret the data integrity and recognise alerts.
- Use digital devices onboard to ensure required security levels for digital networks, servers and applications.
- Detect and prevent cyber-attacks and decide on actions to be taken (preventive and reactive measures).
- Be familiar with cybersecurity risk management and assessment.

Co-funded by the
Erasmus+ Programme
of the European Union

Learning outcomes

Responsibility and autonomy

- Apply the cyber risk management framework to prevent attacks in accordance with Safety Management Systems (SMS) requirements.
- Recognise incidents or cyber attacks on board IT and OT systems and devices connected to the digital networks services.
- Facilitate information sharing among key actors.

Co-funded by the
Erasmus+ Programme
of the European Union

Content of the Educational Package

Example Assessment Case 3

OT Case - ECDIS infected with ransomware

Set bup ECDIS station with charts and sensors connected (real equipment or emulated) and infect it with ransomware (https://github.com/ytisf/theZoo/tree/master/malwares/Binaries).
The participant should:

- understand, what happened with the system;
- know, what are the following actions (from killcard);
- know, where to get the system configuration backup files, operating system DVD, etc.;
- reinstall the operating system, ECDIS software and get the charts back.

	onboard ships			

Co-funded by the
Erasmus+ Programme
of the European Union

What do you remember from the SkillSea DS2 course?

Co-funded by the
Erasmus+ Programme
of the European Union

Feeback

Please share your feedback to the course content and let us know, what would you like to learn during maritime cybersecurity course in the future!

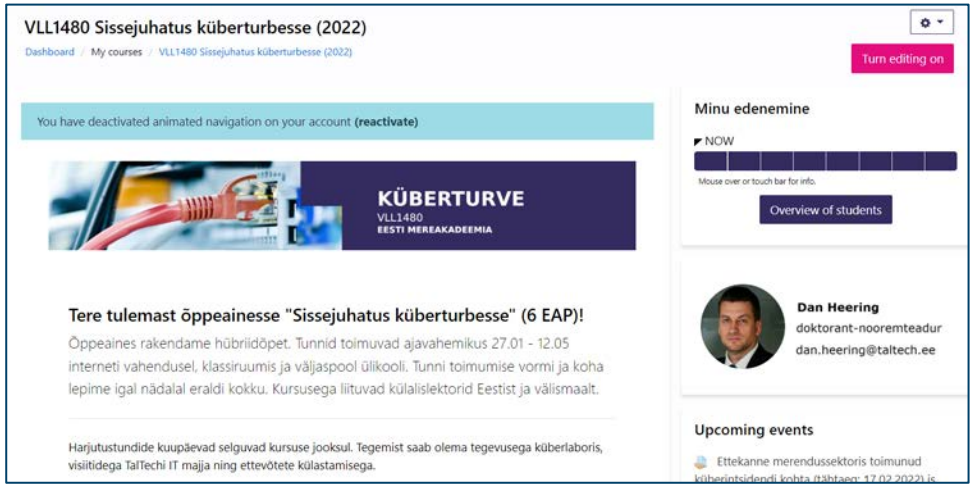
11 responses

- It was quite confusing sometimes but it was quite interesting.
- Kursus oli tore ja loodame, et edasine kursus tuleb veel toredam.
- Mulle meeldib, kasulik info, aga natukene keeruline inglise keeles kõik õigesti aru saada.
- Social engineering
- The course was helpful and different than usual, It was nice.
- what to do when you get hacked?
- looking forward to future lessons about maritime specific cybersecurity lessons and learn the best practice available.
- All is useful,nothing to add
- Oli huvitav ja kasulik!

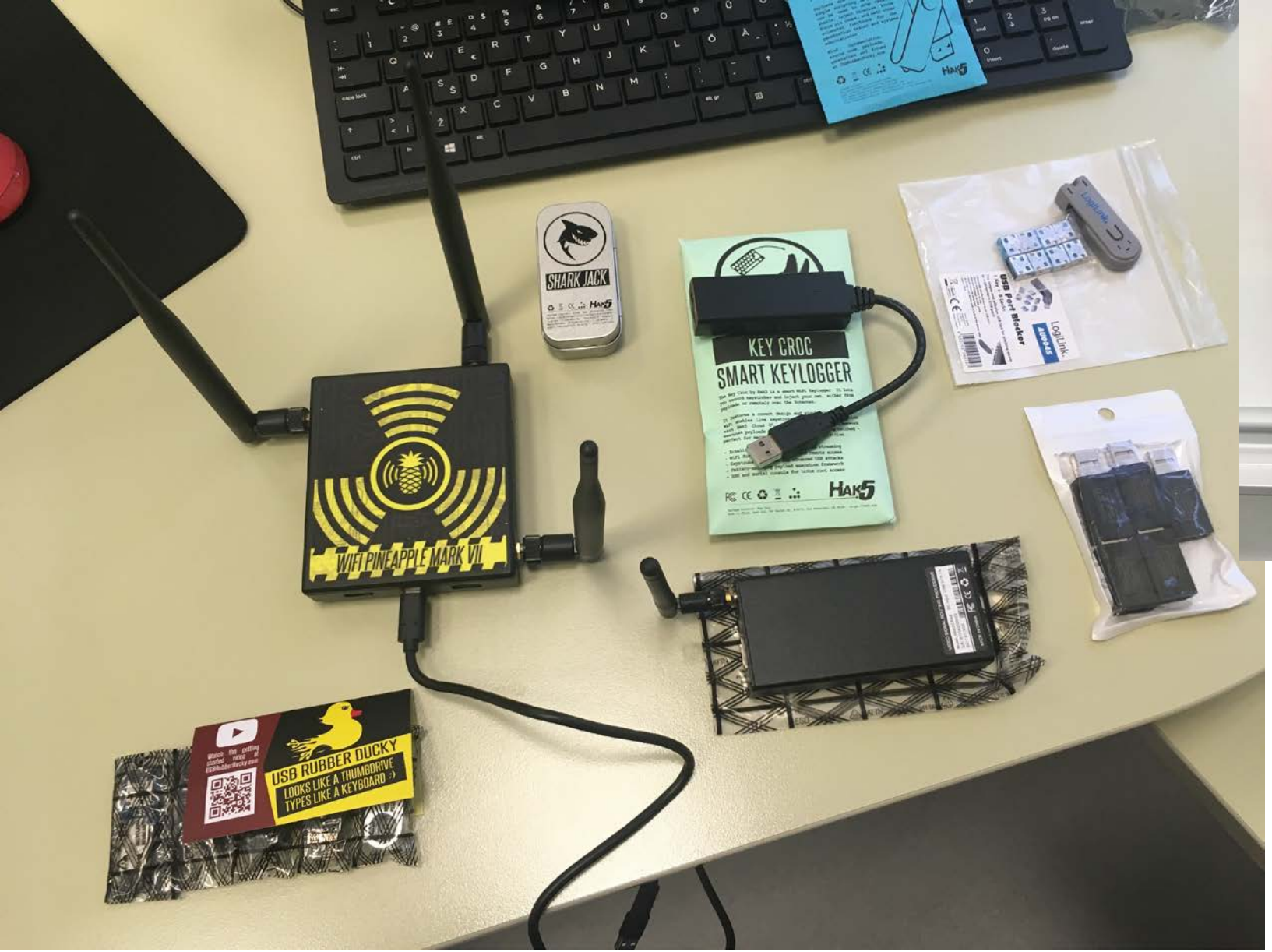
Co-funded by the
Erasmus+ Programme
of the European Union

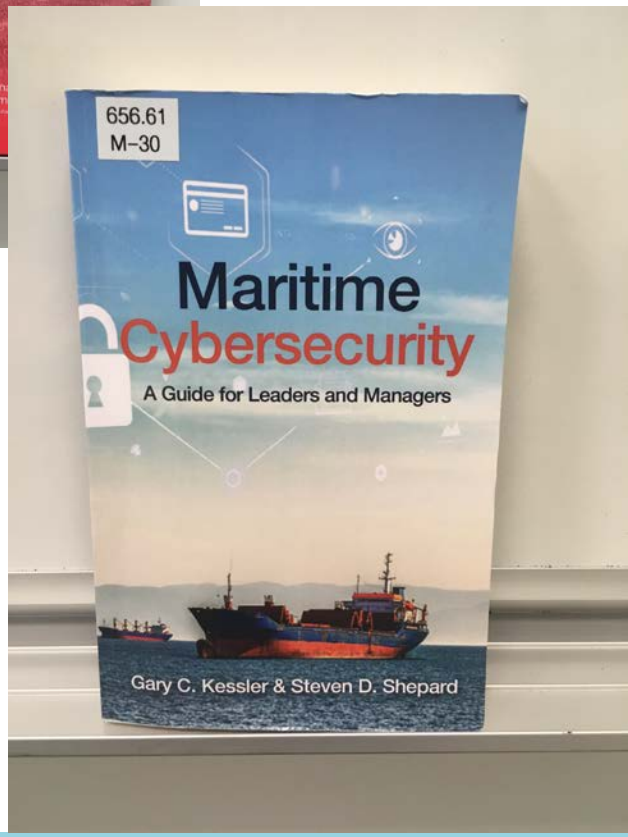
Introduction to Cybersecurity

- 38 students (2 groups)
- Theory, homework, games, practice, demos
- Guest lecturers, professionals (IT, maritime)
- Topics:
  - terminology and cybersecurity in general
  - individually online course (CISCO)
  - cryptography, secure e-mails, backups
  - legislation
  - cyber exercises (NATO CCDCOE)
  - Security Operation Centre (SOC)
  - digital forensics, evidence handling, reporting
  - cyber risk management onboard ships
  - password management, insiders, etc.



Co-funded by the Erasmus+ Programme of the European Union





Co-funded by the
Erasmus+ Programme
of the European Union

Conclusions

- Maritime industry needs more holistic approach towards better cybersecurity!
- Cybersecurity education and training is very important for maritime specialists!
- Increasing the level of cybersecurity awareness among senior management.
- Increased collaboration between the academia and industry.
- Cybersecurity awareness education should start already from academia.
- Competent lecturers needed for cybersecurity awareness training.
- **How can we achieve sustainable behaviour change?**

Co-funded by the
Erasmus+ Programme
of the European Union

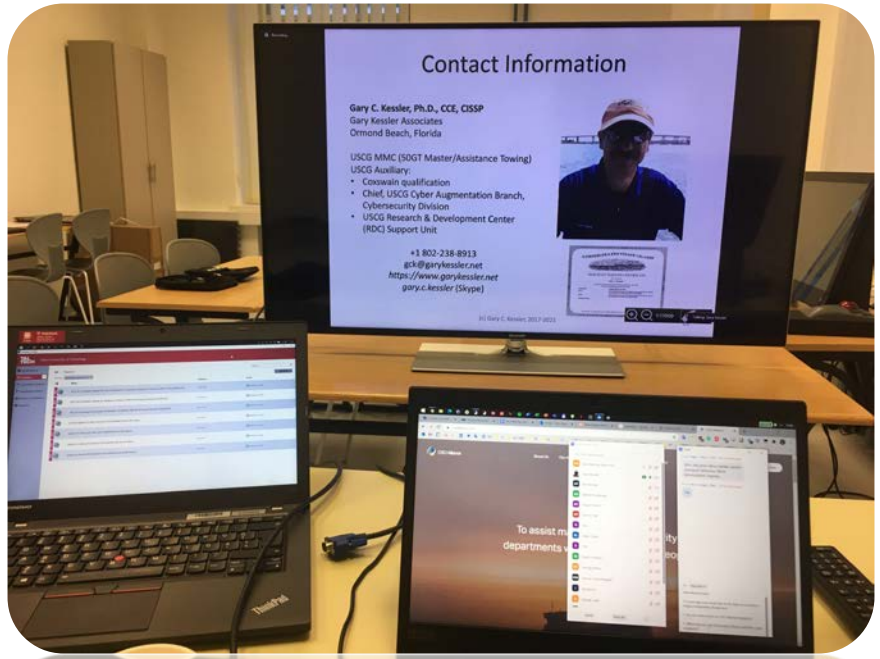
MariCybERA

Budget:	2 497 500 €
Duration:	01.01.21 – 31.12.2025 (60 months)
Partners:	Estonian Maritime Academy, School of IT
ERA Chair:	Professor Kave Salamatian

- Establish a new multidisciplinary Centre for Maritime Cybersecurity by integrating the research capabilities from TalTech's Estonian Maritime Academy and TalTech's Centre for Digital Forensics and Cybersecurity.
- Building a network of academic and non-academic stakeholders for research and technology transfer projects.
- Develop post-graduate training programs.
- Summer and Winter schools.
- Develop proposals for research grants.

MariCybERA has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952360

Co-funded by the Erasmus+ Programme of the European Union



Thank you!

Dan Heering
dan.heering@taltech.ee

Co-funded by the
Erasmus+ Programme
of the European Union