cPAID

Securing Autonomous Ships in the Age of AI-Driven Threats

NTNU
Norwegian University of Science and Technology

CISaR
Critical Infrastructure Security and Resilience

Safeguarding Norway's Critical Societal Functions:
Building Resilience Through Innovation, Research, and Education

The cPAID project, involving European universities and industry partners, aims to develop a structured framework for AI security, with NTNU (Norway) contributing through autonomous maritime systems.

Autonomous Maritime Deployment in Trondheim

The deployment of the autonomous ferry demonstrates that self-driving vessel technology is already operational and progressing toward larger-scale adoption.

Safety-Critical Role of AI in Autonomous Ships

Future autonomous ships will integrate multiple AI systems performing critical functions, where failures or manipulations could lead to severe operational consequences.

Vulnerability of Object Recognition Systems

Object recognition systems present significant risk, as adversarial data manipulation may lead to dangerous misinterpretations in navigation.

Need for Security-by-Design in AI Systems

AI security must be embedded from early design stages, requiring proactive, worst-case-oriented threat modelling rather than reactive mitigation.

Funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The project funded under Grant Agreement No. 101168407 is supported by the European Cybersecurity Competence Centre. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.