

Maritime Cybersecurity and Maintaining Resilience

The National Academies of Sciences, Engineering, and Medicine

Marine Board Spring Meeting

Capt. Alexander N. Soukhanov

15 April 2025



An aerial photograph of a busy port at sunset. Several large gantry cranes with red and white lattice structures are positioned along the pier. In the background, several cargo ships are docked or moving through the water. The sky is a mix of blue and orange from the setting sun.

Introduction

Mission: keep cargo and marine transportation moving by defending our clients against cyber threat.

Our Strategic Anchors

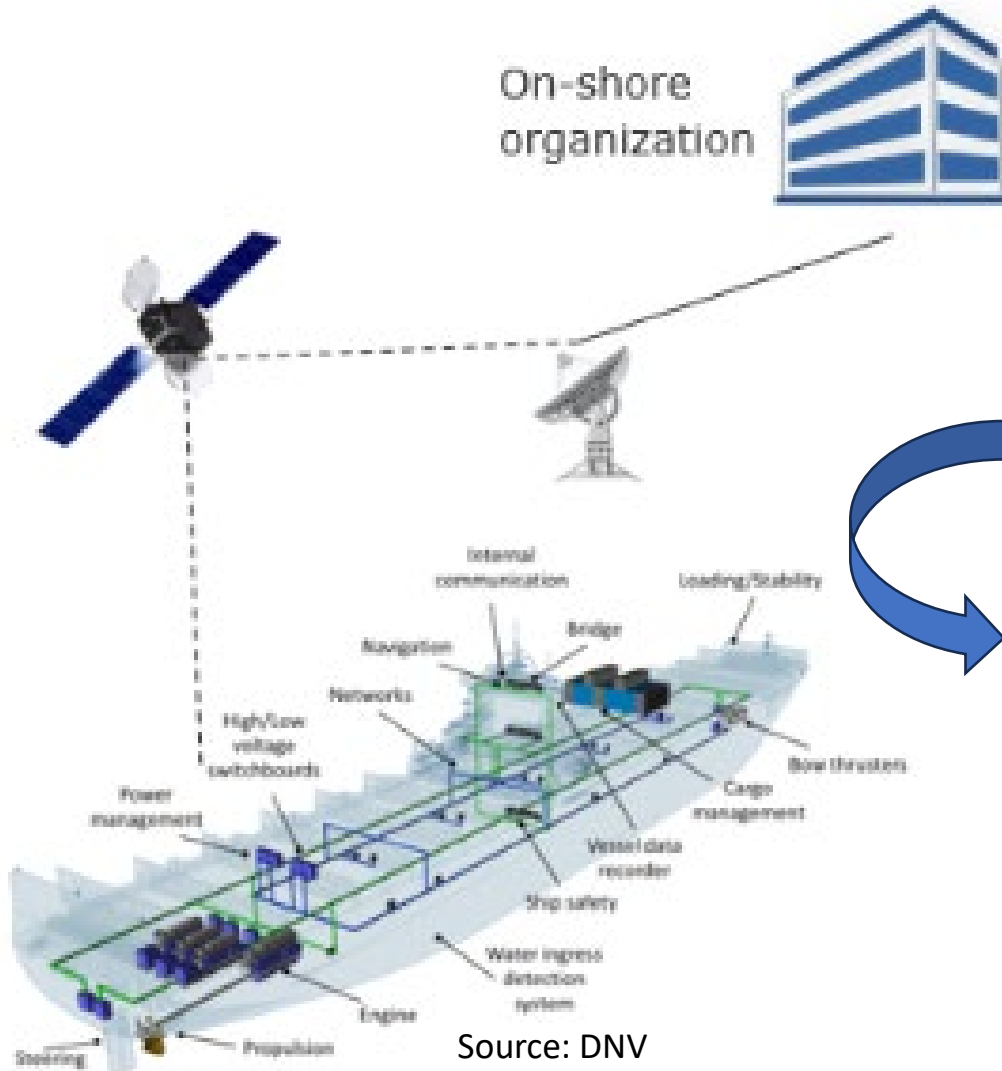


Situational
Awareness

Safety

Resilience

IT and OT on Vessels



Information Technology (IT)

(Enterprise IT – ashore and afloat)

- Desktops, Laptops, Servers
- Business network/LAN, email
- Satellite communications
- PMS, SMS, electronic docs

Operational Technology (OT) / Cyber Physical Systems

(Networked marine systems + sensors)

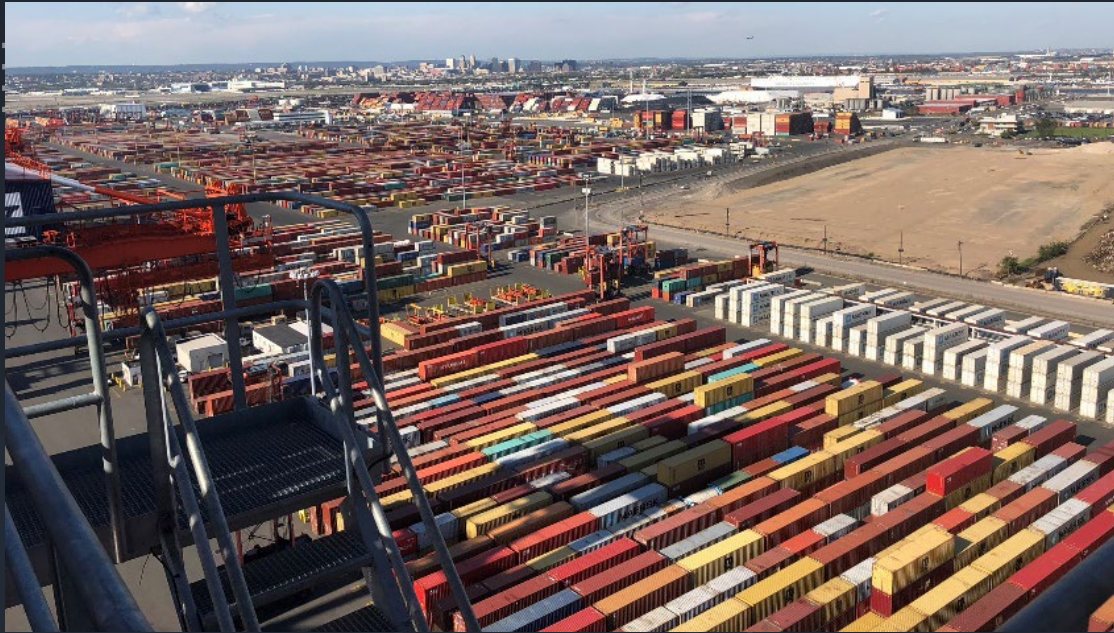
- Engine controls and monitoring
- Navigation equipment: ECDIS, DP, etc.
- Cargo management
- Safety, ballast, auxiliary systems
- Data logging and remote collection

At Risk

The Business:
Communications + Data
+ Operations
(Confidentiality, Integrity,
Availability)

At Risk

Life, Property, and the
Environment
+
All the above
(Availability (Safety),
Integrity, Confidentiality)



Marine Terminals and Converged Technologies

- Enterprise and business IT environments
- OT: Cargo management systems, industrial controls systems (ICS), networked heavy equipment and machinery
- Telematics, wireless networks, and GPS-integration
- Third party technologies for industrial process management
- Networked access controls, cameras, and facility security

Case Study: Cargo Ship Fleet Cyber Assessment

Challenge

- Vessel owner required cyber assessments of their cargo ships

Approach

- Executed baseline assessments to understand security gaps
- Performed asset discovery and inventory of all systems
- Remediated vulnerabilities while working with the client's third-party vendors
- Continuous process improvement of fleet cybersecurity program

Results

- Increased safety and security through a foundation of knowledge, visibility of networked assets, crew confidence and training, and reduced threat surfaces from untrusted or semi-trusted networks



Case Study: Marine Cargo Handling Terminals Assessments

Challenge

- Several container terminals working in consortium required assessments and testing to determine cyber vulnerabilities and impacts to their businesses, the supply chain and the port, and remediation of vulnerabilities.

Approach and Solutions

- Established a baseline from which to understand gaps and strengths, and build enduring cybersecurity
- Integrated key vendors to ensure a comprehensive approach for maximum impact and accuracy
- Provided additional testing, remediation, and training to further drive risk mitigation and positive impact

Results

- Established enduring cybersecurity (now 6 years) by identifying and remediating cyber risk across the businesses through a unified approach as a port community.





Thank you!

Capt. Alex Soukhanov, Partner &
Owner,

asoukhanov@truenorthusa.net

Chris Dunlay, Partner & Owner,

cdunlay@truenorthusa.net

www.truenorthusa.net