Hackers & Pirates

Cybersecurity at the High Seas

Christian Damsgaard Jensen

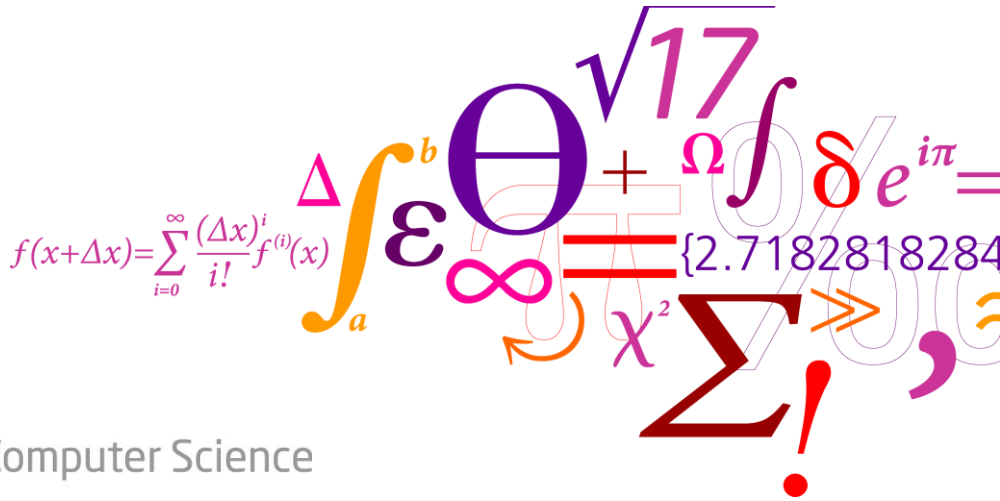
Head of Cyber Security Section

DTU Compute

Technical University of Denmark

cdje@dtu.dk

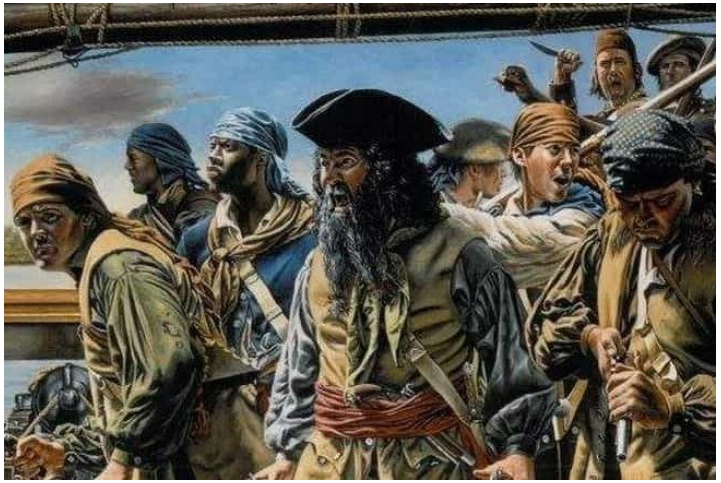
http://compute.dtu.dk/~cdje



DTU Compute

Department of Applied Mathematics and Computer Science

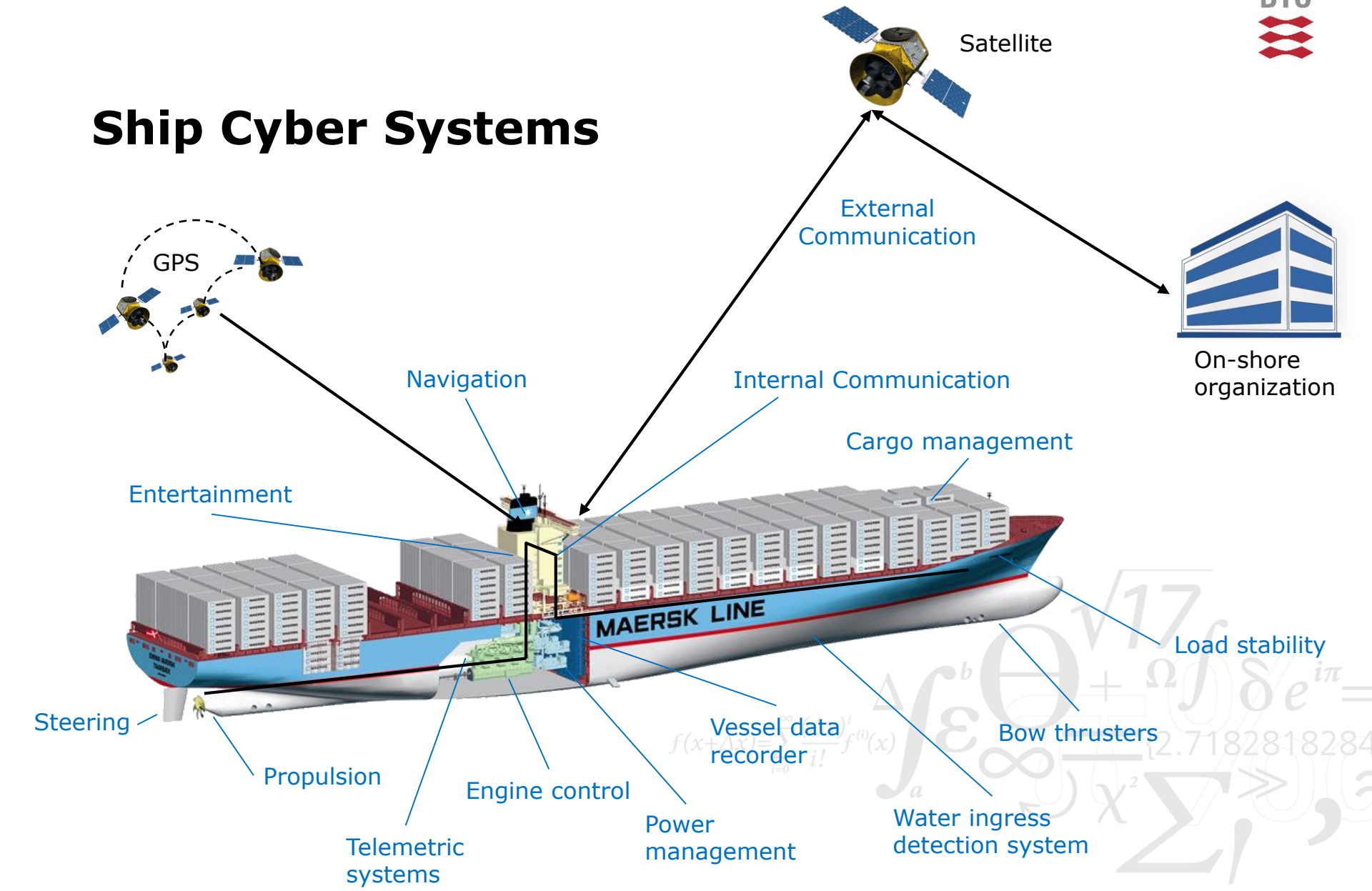
Pirates 1.0 – 4.0



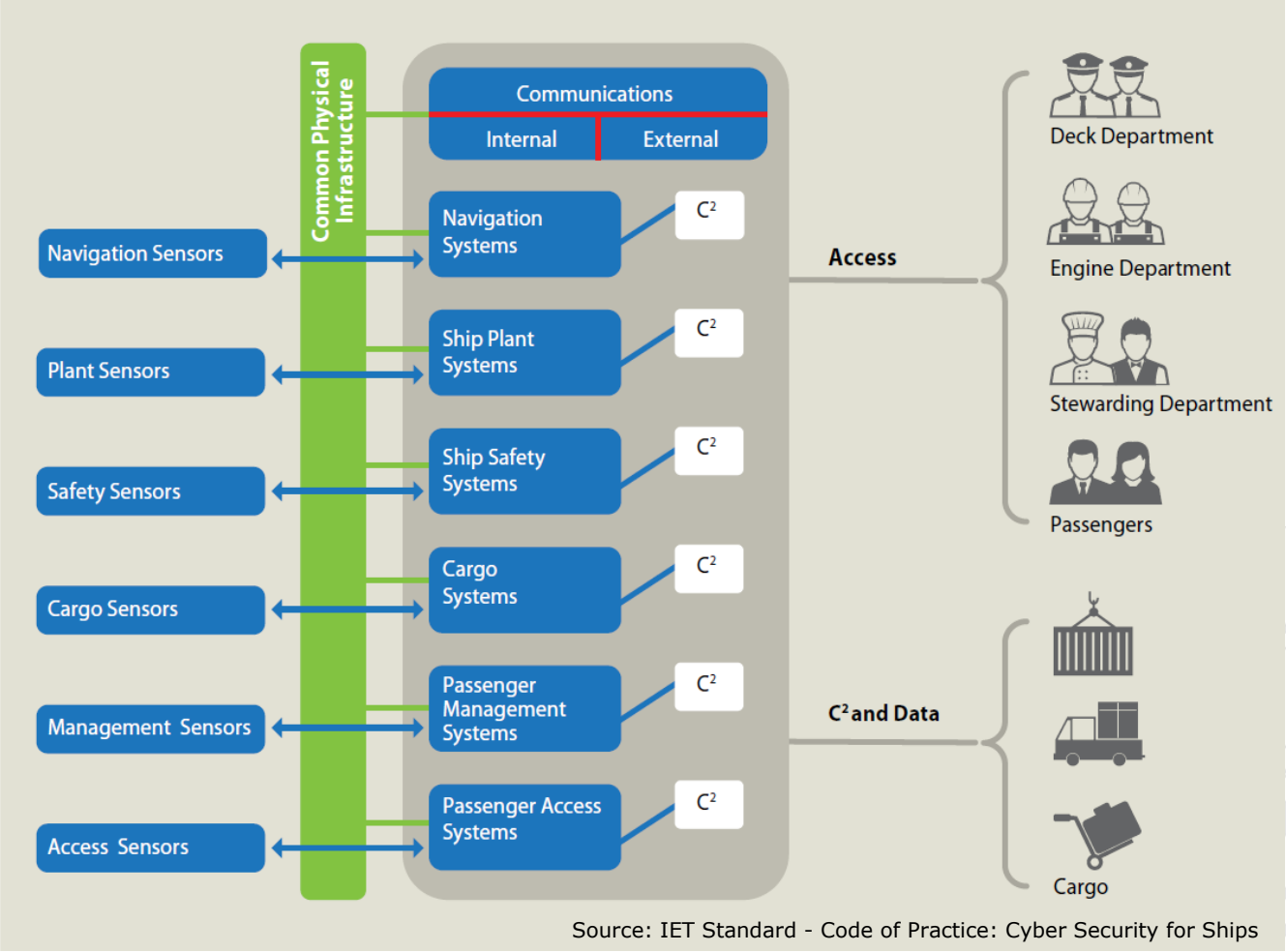
Cyber Threats for Cyber Ships

- Drug cartel hackers compromised terminal systems (Antwerp, 2011)
  - For two years, they were able to smuggle drugs and guns without notice and to release containers to their own trucks in the port
- Customers and Border Protection hacked (Australia, 2012)
  - Hackers could see what containers were suspected by customs
- US Navy warship grounded on a coral reef (Philipines, 2013)
  - ECDIS system identified as problem, alteration of nautical maps suspected
- Microsoft servers on ships vulnerable (CyberKeel, 2015)
  - Study shows 37% of Microsoft servers on ships not patched
- Cargo ship lost navigation system (Cyprus -> Djibouti, 2017)
  - Incident prevented the captain from controlling the ship's course for 10 hours, allowing pirates to attack the ship
- GPS spoofing (Russia/Black Sea, 2017)
  - Several ships reported location as Gelendzhik Airport (32 km inland)

Ship Cyber Systems



Ship Assets Affected by Cyber Security

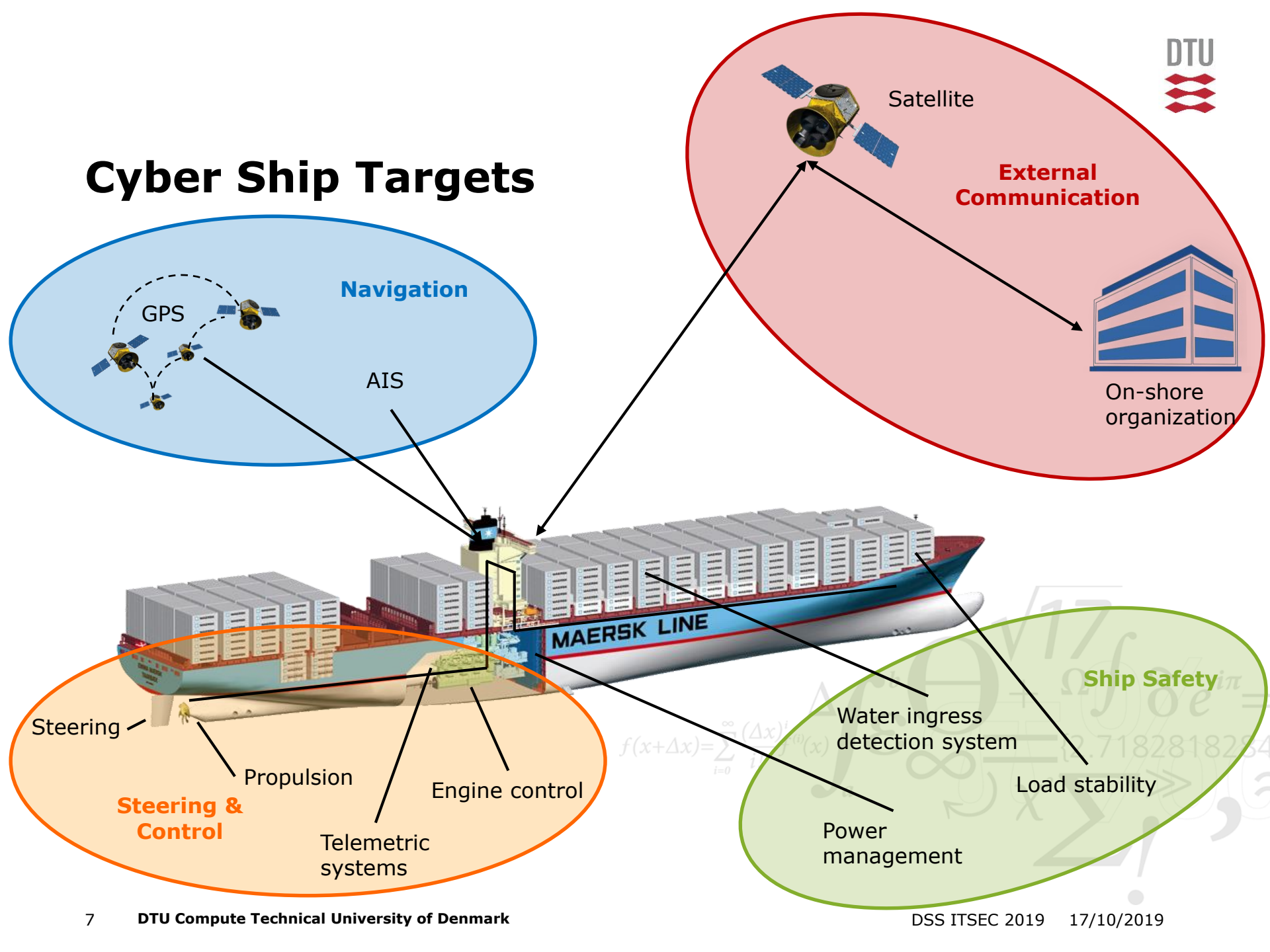


Source: IET Standard - Code of Practice: Cyber Security for Ships

Cyber Ship Attack Surface

- Communication systems (SATCOM, VHF, VOIP, WLAN)
- Navigation systems (GNSS, ECDIS, AIS, Radar)
- Propulsion and power control systems
- Access control systems (CCTV, BNWAS, SSAS)
- Cargo management system (CCR)
- Plant Management Systems (PMS) and ship's certificates store
- Passenger servicing and management systems
- Passenger and crew networks (WiFi, LAN)
- Core communication infrastructure (Router, RW, VPN)

Cyber Ship Targets



BIMCO Cyber Security Approach

Summary

- Ships are large complex cyber systems (both IT and OT)
  - IT vulnerabilities may effect OT and vice versa
  - Long lifetimes implies legacy systems
  - Frequently change of crews implies untrained staff
  - Poor awareness among crews and organisations
- Ships are integral parts of the logistics chain
  - Ship IT/OT systems must be relatively open to support the value chain
  - Security is a growing concern in shipping
- Standards and best practices are emerging and evolving
  - Guidelines on Cyber Security Onboard Ships (BIMCO et al., 2018)
  - Code of Practice – Cyber Security for Ships (IET, 2017)
  - Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2018)
  - Guidelines on maritime cyber risk management (IMO, 2017)
    - *Also recommends ISO 27001 for IT-systems*