Cybersecurity

e-Navigation underway 2019
12 Nov 2019
Maritime Cyberspace
An Operational Domain

• Maritime Commerce is the engine of Global Trade
• Exclusive Economic Zones (EEZs) susceptible to incursion
• Vast Resources move throughout the Marine Transportation System
  • Where there is wealth, there is crime
• Where there is military projection, nation states will strive to disrupt
• Cyber Risks Must be Managed by Operators, supported by skilled technicians.

Establish a Physical/Business Model Analogy aligned to Organization to Educate Operational Principals of Cyberspace.
US Maritime Cybersecurity Efforts

• Draft NVIC 05-17
  • NIST Cybersecurity Framework
  • Identify, Protect, Detect, Respond, Recover (Defense)

• Port Security Grant Funding
  • 2019 - $100M; Cybersecurity is a Category

• NIST Cybersecurity Framework Profiles
  • Maritime Bulk Liquid Transfer, Offshore Operations, Passenger Vessel
Identify Key Cyber Terrain
Strive to Reduce Attack Surface
Risk; Inverse for IT/IS vs OT/PIT

Information Technology (IT) ~ DoD’s Information Systems (IS)

Operational Technology (OT) ~ DoD’s Platform IT (PIT)

Confidentiality

Integrity

Availability
Operationalize IT and OT as a Unified System

IT Systems Mission Platform

- Fog of IT Inhibits Measurement
- Can crew set Zebra?
- Clear Measurement

- Tub of IT (Unmanageable w/ Low Accountability)

- Existing system architecture is difficult to understand/isolate
- SPAWAR DFIA provides consistent standard and control points for isolations

- COMMS
- NAVIGATION
- WEAPONS
- BUSINESS SYSTEMS
- HM&E
• Configuration Management is critical
  • Create configuration baseline
  • Create updated configuration baseline
• Maintenance Management must be controlled
  • Compare post maintenance to configuration baseline
• Physical Security is paramount
  • Verify Maintainers and their computer equipment.
  • Code ports authorized for maintenance use
  • Physical & logical block of unused ports
• Radio/Network Traffic
  • Potential to trigger imbedded malware to obfuscate surface activity and navigation info
Certification approach must measure holistic understanding of cyber risk starting at component and system level, then moving up to enclave, platform, and mission level.
Develop a Damage Control Plate for Crew
Minimize Attack Surface; Increase Use of Emerging Services

Regional Edge Node
Network/Cloud Aggregation Core Router

Organization A
Organization B
Organization C
Organization D
Organization E
Organization F

Dense port capacity
Individually purchased, centrally managed

Vendor Neutral Edge Node

Cloud Exchange

Cloud 1
Cloud n
RaaS
Nav/Wx Services
RM Services
Virtual TIC

500+ XaaS
AI Services

Corporate WAN
AT&T POP
Level 3 POP
Verizon POP
Sprint POP
CenturyLink POP
500+ alternative Networks

Private Fiber Cross-Connect
CSP dark fiber

Management Plane
- Cloud Access Point
- Cybersecurity
- Configuration Baseline
- IDAM & Logging

Low-latency virtual connections
Interconnection of Corporate Network


Outcomes

- Mission data interconnected to tactical edge (e.g. biometrics, imagery, Multi-INT, etc)
- Complete, centralized monitoring
- Mobility at the Global Edge
- Aggregated Cloud Access
- Software defined connections
- Cost savings
- Minimize latency for users

MPLS or Layer 2 as appropriate for cost/performance
Global Architecture to Minimize Latency
Maritime Safety Information Bulletin-5-19

- Phishing and Malware threats
  - Accessing NOA sensitive info
  - Malicious software designed to disrupt shipboard computer systems

- Suspicious activity and breaches reported to the NRC

- Cyber attempts/attack that do not impact the operating condition of the vessel alternatively report to DHS NCCIC
Invest in Intelligence

• SCADA Search Engine
  • SHODAN
• Dark Web Search Services
  • TORNADO
• Logistics Supply Chain Research
  • A Military Camera Said ‘Made in U.S.A.’ The Screen Was in Chinese.
  • Surveillance equipment manufactured in China, raising concerns that Beijing could have used it for spying, prosecutors said.

United States attorney in Brooklyn, discussing the charges against the Long Island firm Aventura.
Nov 7, 2019
Invest in Information Sharing

• The MPS-ISAO, an Information Sharing & Analysis Organization (ISAO)
• Authorized by the 2015 Presidential Executive Order, “Promoting Private Sector Information Sharing”.
• The MPS-ISAO is the Information Sharing and Analysis Center (ISAC) for the Maritime & Port critical infrastructure.
Maritime Cyberspace
An Operational Domain

• Determine your Key Cyber Terrain
• Create an Operational Model of your Cyber Risk
  • ‘Draw the IT Fire Main’
• Modernize Your Network In Preparation for Leveraging the Cloud
  • Manage Approved Cloud Services with a Cloud Access Point
  • Strive to reduce your Cyber Attack Surface
  • Use to test Configuration Management
• Identify your Potential Cyber Adversary
• Invest in Intelligence, Invest in Information Sharing