DUT DURBAN UNIVERSITY OF TECHNOLOGY

NRF National Research Foundation

Stellenbosch UNIVERSITY IYUNIVESITHI UNIVERSITEIT

Cybersecurity in the Maritime Domain: Incidents and Best Practices

Brett van Niekerk

Introduction

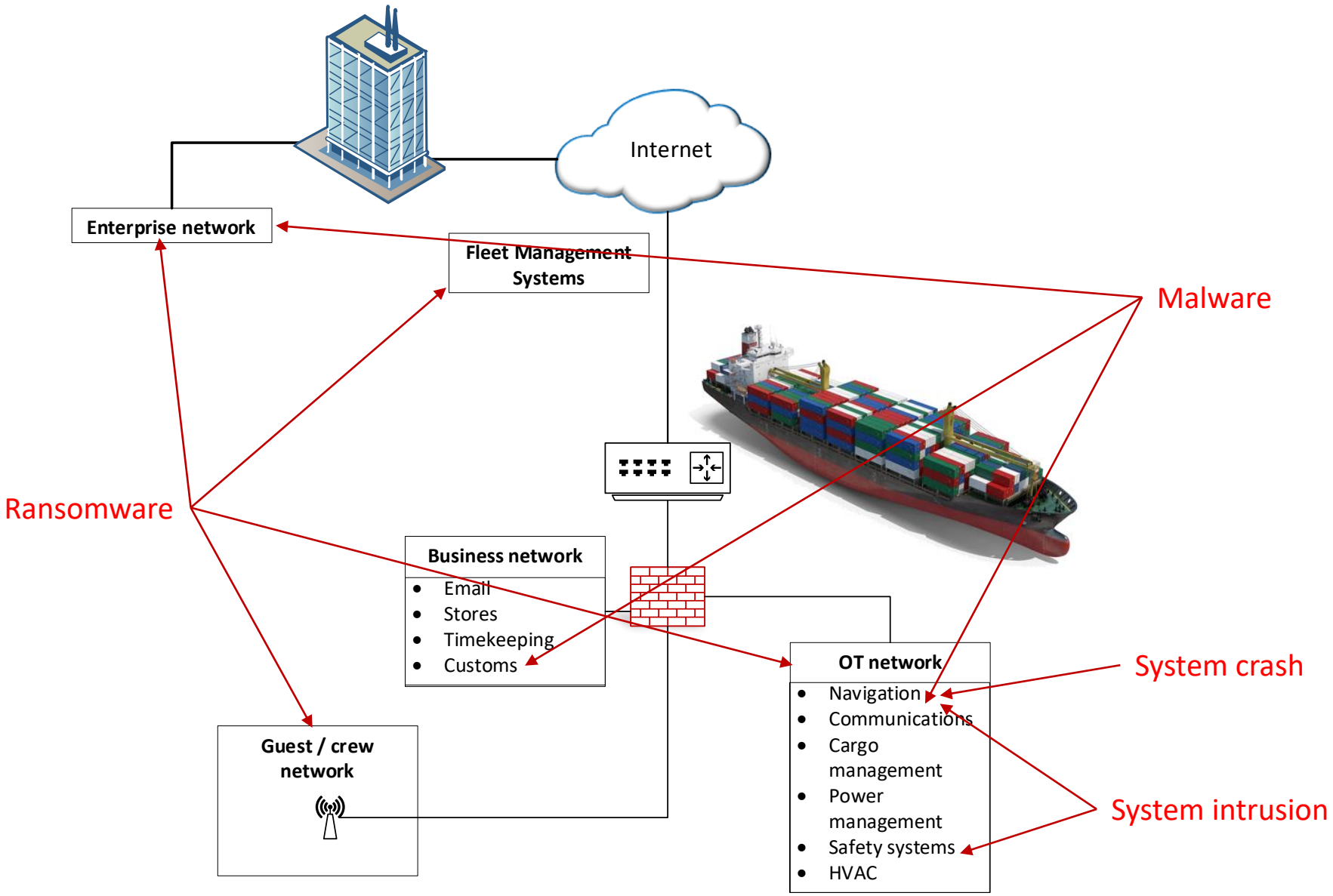
- The purpose is to give an indication of current cyber incidents in the maritime domain, with some best practices, and legal perspectives
- The maritime domain is a critical infrastructure, and a potential target for economic information warfare and cyber crime
- Maritime domain = Ports + vessels + undersea infrastructure
- ‘Cyber incident’ vs ‘cyber attack’ vs ‘cyber warfare’

This presentation is supported in part by the National Research Foundation of South Africa (Grant no. 150720). The opinions, findings and conclusions or recommendations expressed in this presentation are those of the authors, and not of the respective institutions or funding agencies.

Ports

- Since the beginning of the pandemic, the Port of Los Angeles has seen incidents double, peaking at 40 million per month
- Ransomware
  - Transnet (2021), Nagoya (2023) resulted in operation disruption
  - San Diego (2018), Lisbon (2022) did not experience operational impact
  - NotPetya, reclassified as a wiper
- Cyber espionage (IceFog, Indian aircraft carriers)
- State actors: Iran, US Pacific command
- GPS and AIS jamming and spoofing
- Systems intrusions at customs
- ‘Normal’ cyber crime: phishing, scams, BEC, malware

Vessels


Internet
Enterprise network
Fleet Management Systems
Malware
Ransomware
Business network
Email
Stores
Timekeeping
Customs
OT network
Navigation
Communications
Cargo management
Power management
Safety systems
HVAC
Guest / crew network
System crash
System intrusion

Undersea Infrastructure

June 16, 2023 12:07 PM

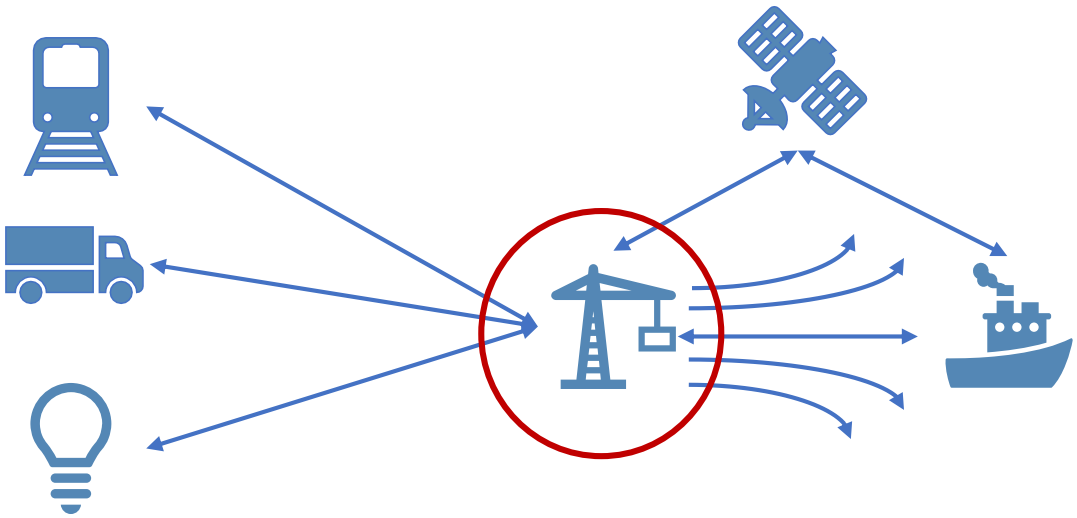
Associated Press

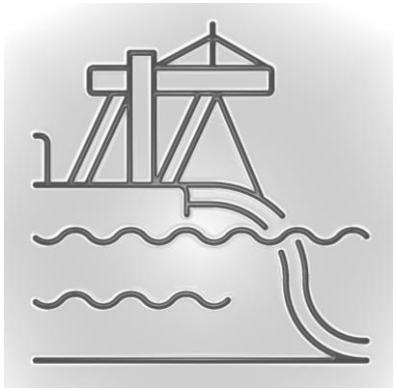
NATO Moves to Protect Undersea Pipelines, Cables Amid Concern Over Russian Sabotage Threat

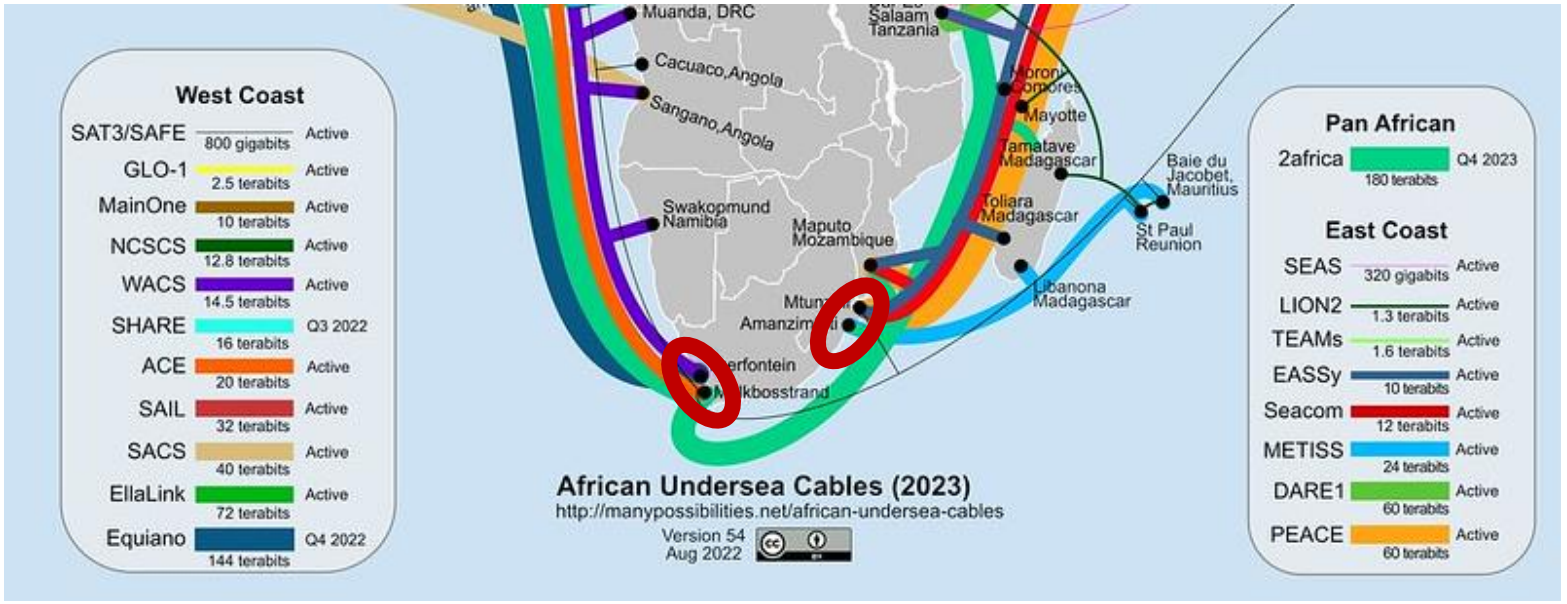
https://www.voanews.com/a/nato-moves-to-protect-undersea-pipelines-cables-amid-concern-over-russian-sabotage-threat/7140442.html

- Undersea cables
  - US prevented successful incident (2022)
  - Seacom ransomware (2023)
  - Undersea datacentres
  - Landing points – espionage & sabotage
- Undersea pipelines
  - Alleged physical sabotage in Baltic
  - Colonial Pipelines as an example
  - Account compromise used in both cyber & influence

Critical Infrastructure & Economic Information Warfare Perspectives







Hypothetical Scenarios

https://www.fleetmon.com/maritime-news/2017/20007/mayhem-durban-harbor-2-vlcs-aground-video/

- Spoofing GPS so:
  - automated equipment navigate into the water;
  - a ship runs aground in narrow channels;
- Malware interfering with:
  - HVAC systems in extreme cold/hot climates
  - the ballast tanks of a submersible;
  - automated mooring systems in heavy weather so ships break their moorings;
- Causing erratic behaviour in cranes or conveyer belts to force a shutdown;
- Using a time-activated logic bomb aboard a vessel to infect USB drives copying information to the port systems;
- Compromising fleet management systems to deliver malware to vessels;
- Affecting valves to fluctuate the pressure in undersea pipelines

Best Practices

- Identify single points of failure:
  - Key facilities in the infrastructure;
  - Key systems in facilities / infrastructure;

- Risk analysis of IT & OT
- Implement protective & detective controls
- Segregate OT / fibre network core from the corporate network & Internet

- Strictly control remote access
  - Strong authentication
  - Indirect access (jump box)
  - Regular reviews to remove unnecessary connections
- SLAs need to clearly indicate security requirements / expectations

Best Practices

- Security by design
- Incident response plans
  - Key stakeholders included (Corp comms, HR, Legal)
  - Training & practice;
  - Challenge for incident response on seagoing vessels?
- Awareness of **ALL** employees
- How to identify and report possible incidents
- Bridge crew to aid in incident response
- Make sure incident response is familiar to all those required to assist

https://hyperproof.io/resource/cybersecurity-incident-response-plan/

Best Practice Documents

- Maritime-specific documents
  - International Association of Ports and Harbors Port Community Cyber Security
  - ENISA report on Port Cybersecurity
  - IMO resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems
  - IMO MSC-FAL.1/Circ.3/Rev.1 Guidelines on Maritime Cyber Risk Management
  - BIMCO The guidelines on cyber security onboard ships
  - ENISA report on Subsea cables
  - MTS-ISAC
- Other cybersecurity documents
  - ISO/IEC 27001 Information security management systems
  - ISO/IEC 27032 Cybersecurity
  - NIST Cyber Security Framework
  - ISA/IEC 62443 standards for industrial automation and control systems
  - MITRE ATT&CK Framework for industrial control systems
  - GCSC Advancing Cyberstability
  - 2015 UN GGE Norms
  - Tallinn Manual 2.0

Conclusion

- Ports, vessels & undersea infrastructure impacted by cyber-incidents
- Cyber crime & state actors
- Trade in general can be disrupted; specific commodities can be targeted
- Need to ensure cybersecurity best practices are followed for IT and OT networks

UNIVERSITY OF KWAZULU-NATAL ™

INYUVESI YAKWAZULU-NATALI

Legal Consideration for Maritime Cybersecurity

Trishana Ramluckan

Introduction

- Ports, ships, maritime supply chains and major offshore infrastructure including oil and gas installations are vulnerable to cyber-attacks.
- The international maritime industry relies on cyber systems for all aspects of operation and management and may face cyber-attacks from so-called activists, terrorists and transnational cyber criminals
- The IMO (SOLAS)
- UN Convention on Law of the Sea (UNCLOS):
  - Territorial sea 12nm
  - Exclusive economic zone (EEZ) 200nm
  - High seas >200nm
- Tallinn Manual 2.0
- 2015 UN GGE Norms – responsible state behaviour in Cyberspace
- GCSC – norms for protecting public core of the Internet

Introduction

- Some concepts from international law:
  - Sovereignty – applies to warships
  - Jurisdiction – flag nation for ships
  - Interference
  - Use of force
  - Armed attack – physical damage / injury
  - Attribution
  - Proportionality

Laws Related to Ports

- Local regulation/law
- Points to consider:
  - Who is responsible if a ship causes damage to a port due to a cyber incident?
  - Who is responsible if a ship is damaged while under pilotage / docked due to a cyber incident?
  - Ship can’t offload due to cyber-incident?

Vessels at sea

- Responsibility to deliver cargo
- Ship adrift if systems crash due to cyber incident
- Spoofed GPS: piracy / collision
- Tallinn Manual
  - Rule 45: Cyber operations in high seas allowable for ‘peaceful purposes’
  - Rule 46: Right to board if suspected using cyber for piracy, slave trade, unauthorised broadcasts

Undersea cables

- Tallinn Manual 2.0 – Rule 54
  - s(3-5): State sovereignty applies to cables in territorial waters – state laws and regulations apply to laying and maintenance. However, states need to respect existing cables in their waters, laid by others that do not make landfall.
  - s(6-8): States may lay cables in the EEZ & continental shelf of a coastal state with due regard to the rights and duties of the coastal state (who may not regulate or impede maintenance).
  - s(10): States have right to lay cables beyond continental shelf
  - s(11): Land locked states have right to access
  - s(15): It is prohibited for states to damage undersea cables
- GCSC – norms for protecting public core of the Internet applies as undersea cables a major component

Discussion

- Spoofing of GPS
  - In territorial waters or port, state legislation applies; responsibility difficult as any damage arising is not the fault of the ship operator or nation/port authority. Possibly considered an armed attack if serious damage/injury occurs.
  - On high seas can be considered interference or use of force; armed attack if damage or injury occurs. Potentially a breach of freedom of navigation.
- Malware impacting a ship in high seas affects freedom of navigation, puts lives at risk. Attribution problematic. Responsibility shipping operator
- Espionage or interference of undersea infrastructure in territorial waters is a breach of sovereignty

Discussion

- Currently South African maritime legislation does not explicitly consider cyber incidents
- Clarity/guidance is required for interference of navigation, responsibility and liability due to cyber incidents under South African law
  - E.g. reporting cyber incidents as a danger to navigation
- Critical Infrastructure Protection Act (also does not explicitly consider cyber) and the Cybercrimes Act can apply
- Responsibility for a cyber incident can include:
  - A malicious actor
  - Negligence of an insider
  - Failure of governance

Cybersecurity in the Maritime Domain: Incidents and Best Practices

Brett van Niekerk – brettv@dut.ac.za

Trishana Ramluckan – ramluckant@ukzn.ac.za