Maritime’s zero-day exploit: port cyber security

17 March 2021 • 14:00-14:45 GMT

Panellist documents

Page 2: Dr Kemedi Moara-Nkwe,University of Plymouth
Page 11: Lars Benjamin Vold, NORMA Cyber
Page 18: Paul Ferrillo, McDermott Will & Emery

Part of
Maritime Cyber Security
Webinar Week

16-18 March 2021

MARITIME
OPTIMISATION
& COMMUNICATIONS

Towards Secure Ports: Leveraging National Cyber-Security Centres to Improve Security

Dr Kemedi Moara-Nkwe
Cybersecurity Research Fellow

Maritime Threats Group, Uni Of Plymouth

Outline Of The Talk

Purpose: Briefly discuss issues leveraging National Cyber-Security Centres to decrease Maritime Port Cyber-Risk.

- (Background) Introduction to the Maritime IT/OT landscape
- Technology used on Vessels and Ports (How dependent are these on tech?)
- What are National Cyber-Security centres and how can we leverage them to better protect Maritime Ports
- General approaches used to address Maritime Cyber-Risks.

Tech In Used In the Industry - Vessels

In vessels, IT/OT infrastructure is used to:

- Aid Navigation & Improve Navigational Safety

+ Position tracking Systems, e.g. Automatic Identification System (AIS)

+ and the ECDIS system which is a system which allows a wide variety of quantities to be monitored .

Tech In Used In the Industry - Ports

- Planning Software
- Automated gates
- Electrified Cranes
- SCADA networks
- Enterprise Networks

Cyber-Attacks – What's at Risk at the Micro Scale?

- Potentially cause a vessel to lose access to on-shore services (no comms)
- Potentially lose access to electronic devices on-board the ship which are used for navigation or for safety purposes
- On-shore (i.e. Ports), potential consequences = disruption of port operations -> disruption of the supply chain.

National Cyber–Security Centres (NCSCs)

- NCSC help to monitor and assess threats, and promote and educate stakeholders on current best practice
- In the UK, both NCSC and DSTL relevant.

- DSTL:
  - Cyber-Security for Ports and Port Systems
- DfT:
  - Good Ports Guide
- NCSC:
  - Regular cyber-security guides and puts out bulletins on current security landscape.

National Cyber–Security Centres (NCSCs)

-NCSCs can play a big role in the better standardisation of

i) Cyber-Security Assessment in Ports
ii) Cyber-Security Plans
iii) Frameworks for the identification of attack mitigation measures

- The use of risk models, such as the one proposed within the Cyber-MAR project, would also provide a very good decision tool for practitioners.

- These are the main value additions NCSCs can bring.

Countermeasures (Main Classes)

- Direct Approaches:
  - Hardening IT/OT systems
  - Improving Training for personnel
  - Regulatory Changes

Countermeasures (Main Classes)

- Indirect Approaches
  - Risk Sharing: Promoting and encouraging the growth of the Cyber-Insurance market. This will allow players in the maritime space to adequately hedge against cyber risk.
  - Projects such as Cyber-MAR have the aim of quantifying the effects of cyber-attacks and proposing risk models that would aid with the above.

Open Questions we still have:

- What proportion of ports have mandatory cyber-security training for their port workers?

- Are workers aware of the existence of a cyber-security guides for Port stakeholders?

Norwegian Maritime Cyber Resilience Centre

NORMA CYBER

Building unified resilience against cyber threats for Norwegian Shipping and Maritime Sector

Riviera Maritime Webinar – Maritime's zero-day exploit: port cyber security

DEN NORSKE KRIGSFORSIKRING FOR SKIB
GJENSIDIG FORENING
The Norwegian Shipowners' Mutual
War Risks Insurance Association

Norges Rederiforbund
Norwegian Shipowners' Association

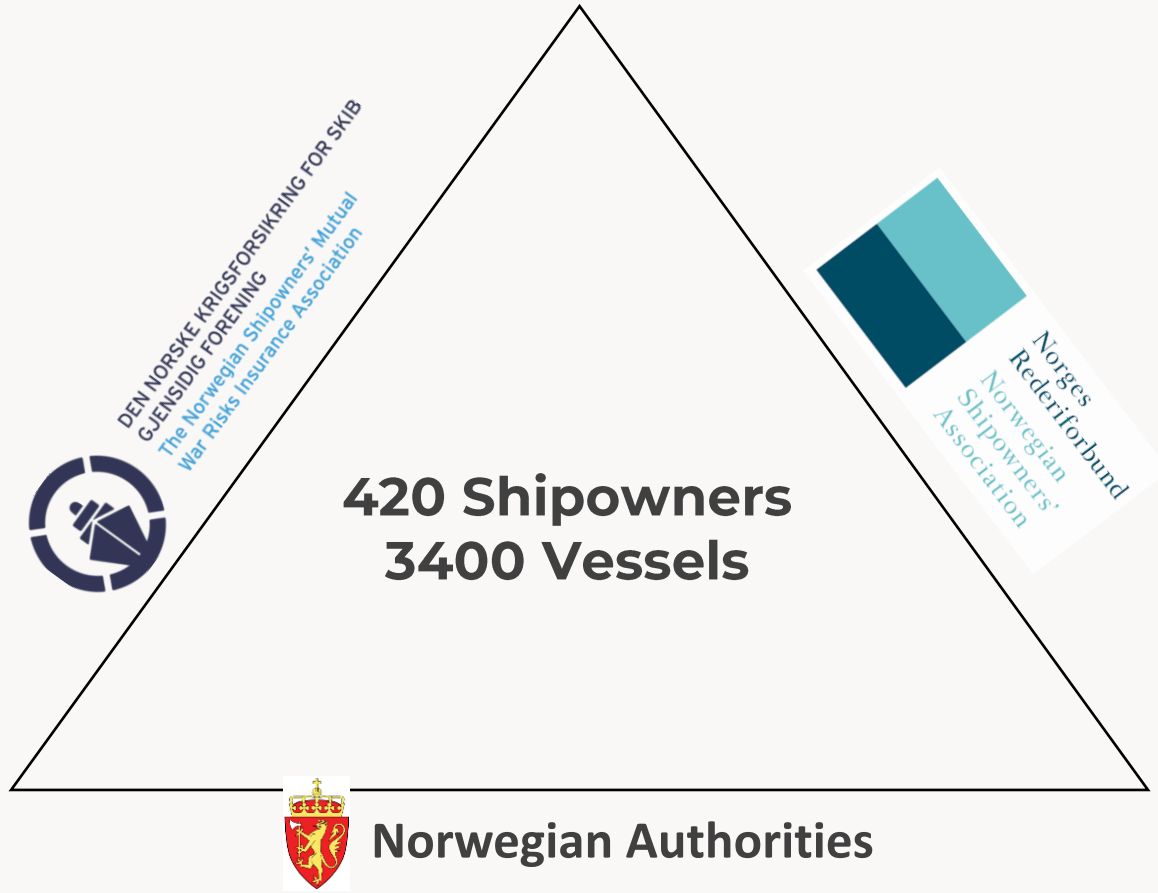
DNK/NSA Member Vessel's Footprint in 2020

Project findings

- Complex structures within shipping and the supply-chain within maritime industry
- Few established information sharing centers or similar
- Communication challenges within companies – IT staff, OT staff, mid-level leaders and executive level
- Sharing of information and experiences comes with a cost
- The regulatory side is coming slowly along

On the Positive Side

- Several organisations are willing to move forward and invest time and money in collective cyber resilience
- New technology to utilize for cyber defence purposes
- Already existing structures and organisations which can be build on



Our small contribution

Yet another Cyber Security Centre ☺

Intelligence

Part of Membership

- Intelligence and Information sharing service

Response

Part of Membership

- Incident and crisis support to members

Security Operations

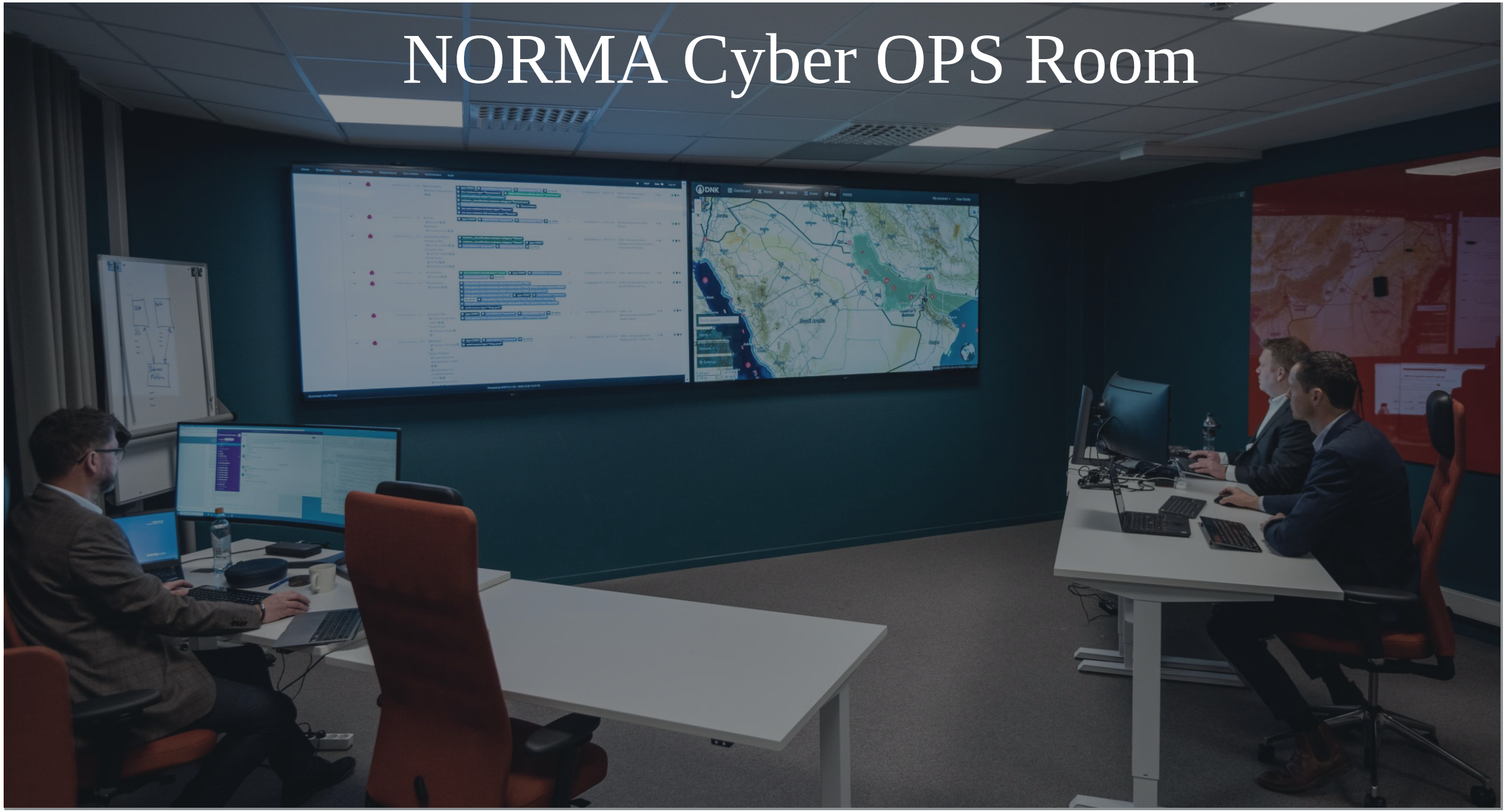
1 June 2021

Additional Service

- Managed Security Operations Centre (SOC) service tailored for shipping and maritime sector

Member log-in portal (encrypted sharing, reports, self-service), Webinars / Seminars, User Council

NORMA Cyber OPS Room



NORMA CYBER

Q/A

How can we make sure organisations communicate better within cyber security both horizontally (between different departments) and vertically (between staff, mid level leaders and executive leaders)?

How can we increase the information and knowledge sharing regarding cyber security for maritime Operational Technology (OT)?

How can we reduce the human factor within cyber security?

Questions?

US National Maritime strategy: upcoming plans, policies and procedures

Paul A. Ferrillo

March 17, 2021

Risks and Standards and Priorities of the National Maritime Cybersecurity plan

- Establish clear line of command (“De-Conflict”) who is in charge of maritime security. Generally its the US Coast Guard in the continental US.
- Develop maritime standards and best practices for IT and OT technologies – NIST orientated and guided.
- Strengthen port cyber security best practices through contractual requirements
- Develop procedures to identify, prioritize and mitigate cyber security risks for ports and vessels, including developing a framework for ports and vessels assessments to follow
- Better information sharing and more timely sharing of cybersecurity threat intelligence
- Increased educational training to produce more Cybersecurity specialists for ports and vessels

Role of the US Coast Guard – chief maritime law enforcement agency in the US.

- National Maritime cybersecurity plan rides side by side with US Coast Guard NVIC 01-20 “Guidelines for addressing cyber risks at Maritime Transportation Security Act (MTSA) regulated facilities” which generally require these ports to address and document network and cybersecurity vulnerabilities – see also 33 CFR 105.305(D)(2)
- MTSA requirements are mandatory – NVIC is “guidance” reminding port facilities of the need to comply with MTSA regs
- Identify cybersecurity Vulnerabilities – vulnerability assessment - Facility Security Assessment or FSA
- Plan to address cybersecurity vulnerabilities — Facility Security Plan or FSP

Elements of an FSA cybersecurity assessment (as found in the NVIC).

- Assessment of cybersecurity roles and responsibilities of facility personnel
- How to test for cybersecurity vulnerabilities
- How are security conditions communicated to and between vessels and facilities to the port captain and local authorities and internally amongst personnel?
- How are updates and patches being handled by the facility?
- What measures are in place to regulate access to the port network (2FA?)
- What measures in place to handle cyber related interfaces with vessels?
- What measures are in place to handle the security of cargo?
- What measures are in place to continuously monitor the facility?

The government, the ports, the Coast Guard, and the flag carriers – policies and procedures

- Will the National Maritime plan gain traction in the pro-cybersecurity Biden administration?
- Will the NIST cybersecurity framework become maritime "cyber law" for the ports? Or will there be another "framework?" See e.g. https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/
- What level will there be of port compliance with cyber risk and vulnerability assessments?
- How do you make the flag carriers more cybersecurity safe? US carriers only? World carriers? Both? What are the jurisdictional boundaries?
- Cybersecurity knows no international boundaries – we are all targets