




Securing the Future of Dry Bulk Terminals:

Navigating Cyber Threats in the
Maritime Sector

Richard Hodder

ABTO 2024 October 24th



How confident are you that your port or terminal could continue operations if it were hit by a cyberattack today?

How would you even know?...

The Cyber Threat Landscape for Bulk Terminals

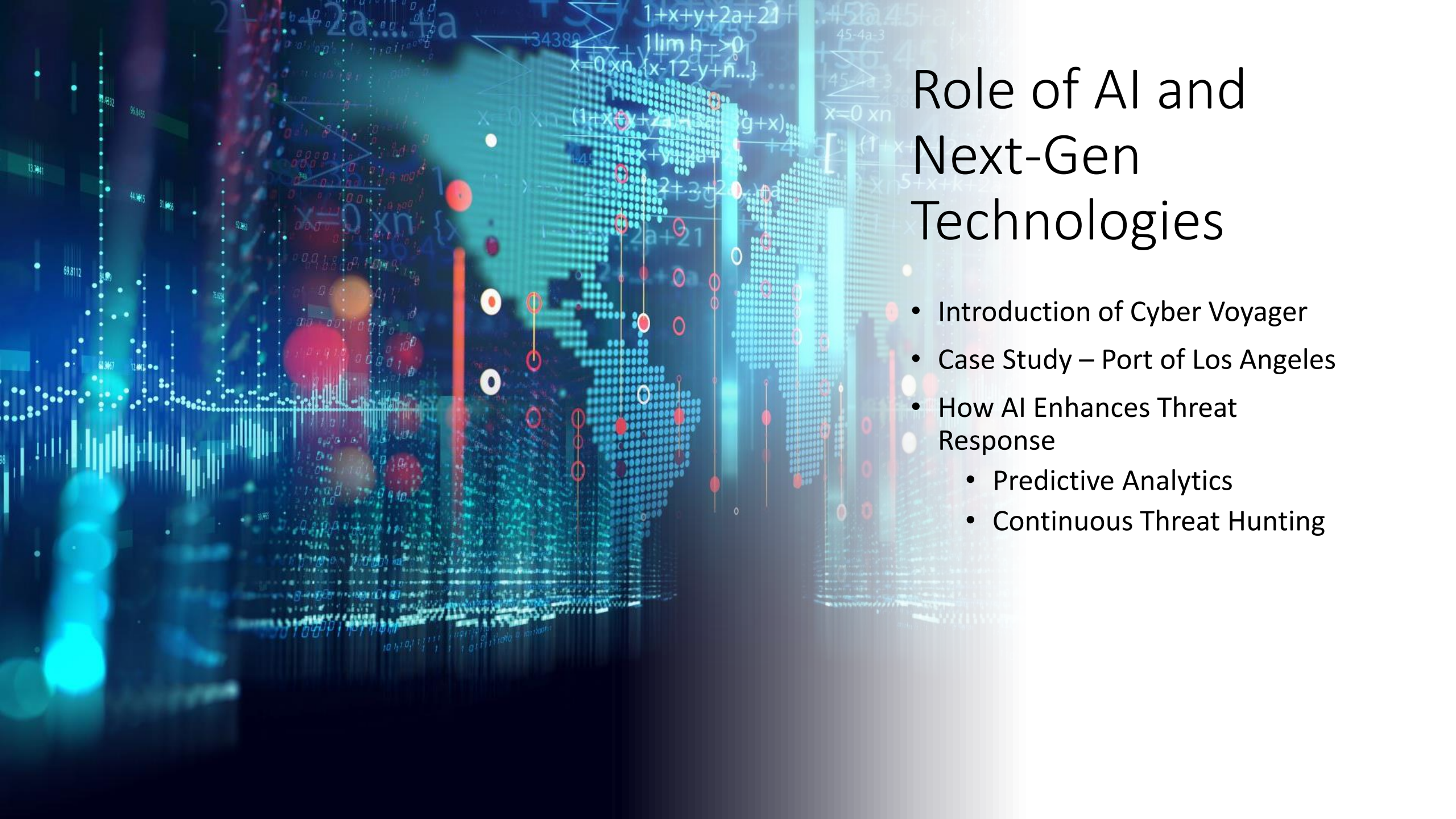
- Traditional Piracy vs. Cyber Piracy
- Recent Cyber Attacks Affecting Ports and Terminals
 - Transnet Attack (2021)
 - Port of Lisbon Attack (2022)
 - Colonial Pipeline Attack (2021)
 - Port of Los Angeles (Ongoing)
- Emerging Cyber Threats - Geopolitics



Defensive Strategies and Best Practices

- Building Cyber Resilience
 - Risk Assessments
 - Incident Response Plans
 - Employee Training
- Learning from Recent Attacks
 - Transnet
 - Port of Lisbon
- Compliance & Standards
 - NIS
 - GDPR
 - ISO 27001





Role of AI and Next-Gen Technologies

- Introduction of Cyber Voyager
- Case Study – Port of Los Angeles
- How AI Enhances Threat Response
 - Predictive Analytics
 - Continuous Threat Hunting

What the Future Holds: Mitigating Evolving Threats



Adapting to the
Future



Collaboration



Enhanced
Defences



Employee
Knowledge



Questions

- Richard Hodder
- rh@engagecyber.ai
- Find me on LinkedIn

Tips and Tricks

- Strong passwords and password manager
- Use VPN on public WIFI
- Never deal with sensitive data on public WIFI
- Keep software up to date
- Use a good firewall
- Don't share passwords
- Don't let USB sticks run automatically
- Adopt good policies
- Implement a robust Incident Response Plan

