## LECTURE 12 • PSM-28 • 2 H 30 MIN

## Leveraging Technology for Enhanced Port Facility Security

**Purpose.** Evaluate security technology by operational outcomes, integration, cyber risk, human decision-making, privacy, lifecycle cost and measurable assurance.

**Learning outcomes supported.** 3, 4, 6, 7 and 10

**Suggested time plan:** Read and annotate 30 min | Research and analyse evidence 45 min | Create the required output 60 min | Review 15 min | Total 2 h 30 min

### Research questions

1. What operational requirement should be defined before selecting surveillance, access or analytics technology?
2. How can a cyber incident affect physical access, cargo handling or emergency response?
3. What evidence demonstrates detection quality, availability, usability and response performance?

### Independent-learning activity

4. Define a fictional requirement such as detecting waterside intrusion or improving restricted-area identity assurance.
5. Compare three options using risk reduction, integration, privacy, resilience, competence, maintenance and whole-life cost.
6. Create a cyber/OT risk register covering identity, configuration, logging, suppliers, backup and incident response.
7. Recommend an option with acceptance tests, performance measures and a fallback process.

### Recommended further reading

IMO: Maritime cyber risk

NCSC: 10 Steps to Cyber Security

ICO: Biometric recognition guidance

NPSA: Security Culture Tool

Also use the corresponding London Gateway College lecture material and any tutor-approved local or sector source.