AI and Cybersecurity: Research in Maritime

CSP007

PRESENTATION BY: STYLIANOS KARAGIANNIS, (PDMFC, PORTUGAL)

AI for Maritime Cybersecurity

Essentials

- Maritime industry relies on digital technologies.
- AI integration introduces cybersecurity concerns.

Importance of AI in Maritime

- AI enhances operational efficiency.
- However, increases cybersecurity vulnerabilities.

Objective

- Explore AI-cybersecurity intersection in maritime.
- Identify threats and strategies.

Adversarial AI vs. Defensive AI in Cybersecurity

Adversarial AI: deliberate attempts to manipulate inputs to AI models and tamper datasets in order to cause errors or misclassifications.

Defensive AI: Aims to mitigate vulnerabilities and enhance the reliability of AI systems in defending against cyber threats.
Focuses on strengthening security measures, such as intrusion detection, anomaly detection, and threat analysis, to protect against adversarial attacks.
Works towards improving the resilience of AI systems to withstand attacks and maintain their functionality.

Offensive AI: Goes beyond targeting AI systems specifically and can encompass a broader range of targets, such as traditional IT infrastructure or IoT devices. Focuses on developing and deploying AI-driven techniques to conduct cyber attacks, such as automated penetration testing, evasion techniques, or malware generation.

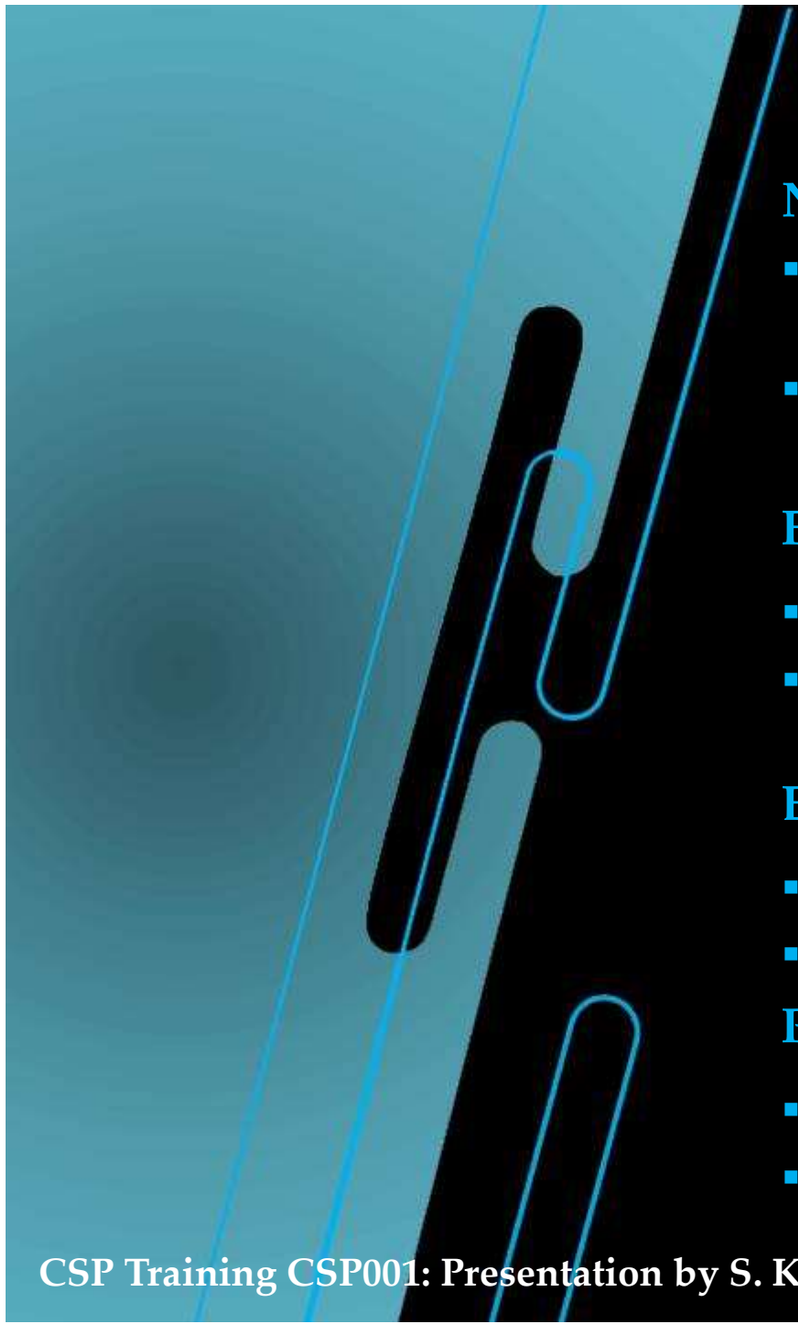
Adversarial AI

- **Definition:** Utilizes AI techniques to exploit vulnerabilities or deceive AI systems.
- **Objective:** Aimed at compromising or subverting AI systems for malicious purposes.
- **Examples:** Adversarial attacks, such as poisoning, evasion, or data manipulation.
- **Focus:** Targeted towards exploiting weaknesses and undermining the integrity of AI models and systems.

Defensive AI (AI in Cybersecurity)

AI in Cybersecurity Defense

- **Definition:** Utilizes AI techniques to enhance cybersecurity measures and defend against threats.
- **Objective:** Aimed at safeguarding systems, networks, and data from cyber threats.
- **Examples:** Intrusion detection, anomaly detection, malware analysis, and threat intelligence.
- **Focus:** Proactively identifying and mitigating threats, enhancing resilience and security posture.



AI in Maritime

Navigation and Route Optimization

- AI analyzes past behaviors to navigate vessels autonomously or with minimal crew.
- Provides optimized routes based on fuel use, water traffic, and weather patterns.

Fuel Consumption

- Tracks fuel consumption and suggests strategies for reduction.
- Offers insights into inefficient processes for improved resource management.

Equipment and Vessel Maintenance

- Uses sensors to detect equipment performance issues.
- Alerts crews for timely maintenance, increasing efficiency and safety.

Port Density and Traffic

- Analyzes radar, sonar, and GPS data to navigate safely through traffic.
- Helps avoid heavily trafficked areas, reducing collision risks.

Thank you

Organization: PDMFC

Please send all questions to:
stylianos.karagiannis@pdmfc.com