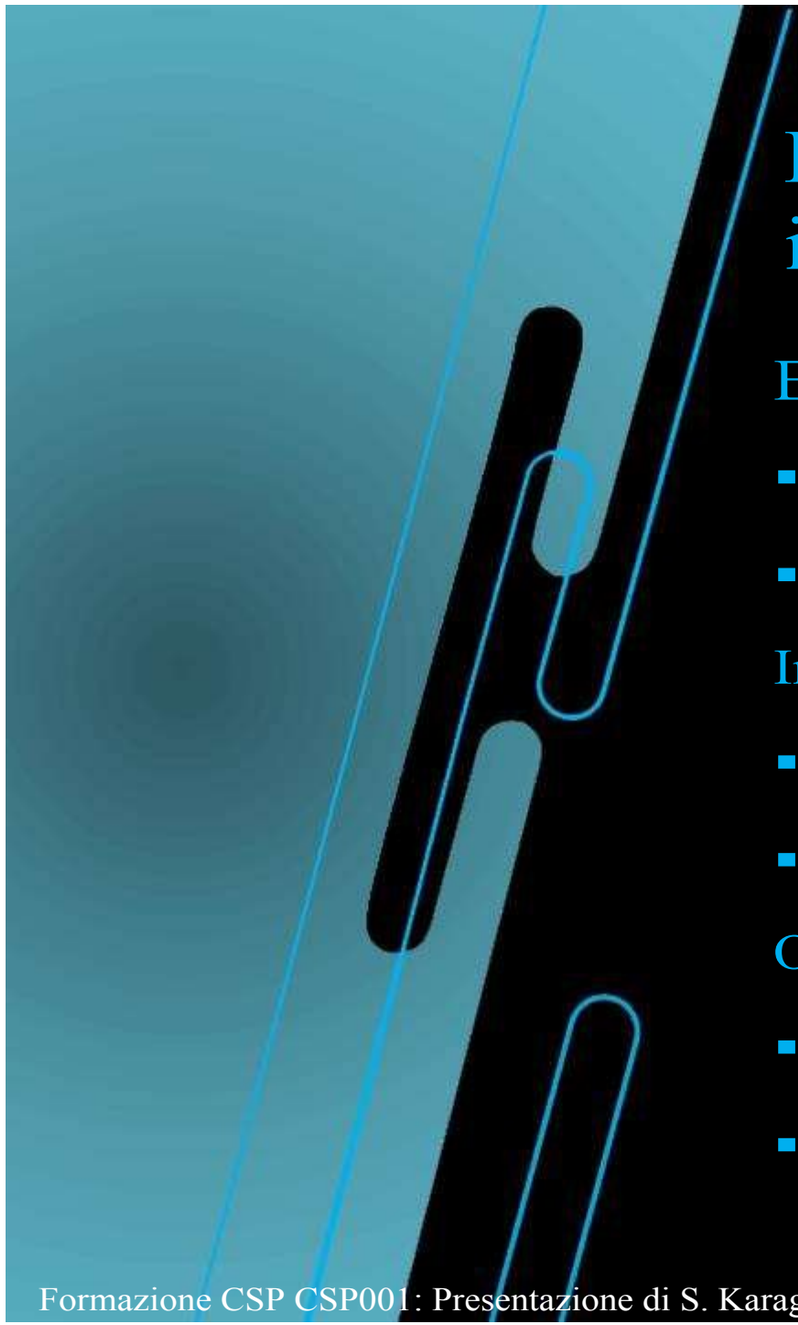
IA e sicurezza informatica: Ricerca in ambito marittimo

CSP007

PRESENTAZIONE DI: STYLIANOS KARAGIANNIS, (PDMFC, PORTOGALLO)



L'intelligenza artificiale per la sicurezza informatica marittima

Elementi essenziali

- L'industria marittima si affida alle tecnologie digitali.
- L'integrazione dell'IA introduce problemi di cybersecurity.

Importanza dell'IA nel settore marittimo

- L'intelligenza artificiale migliora l'efficienza operativa.
- Tuttavia, aumenta le vulnerabilità della sicurezza informatica.

Obiettivo

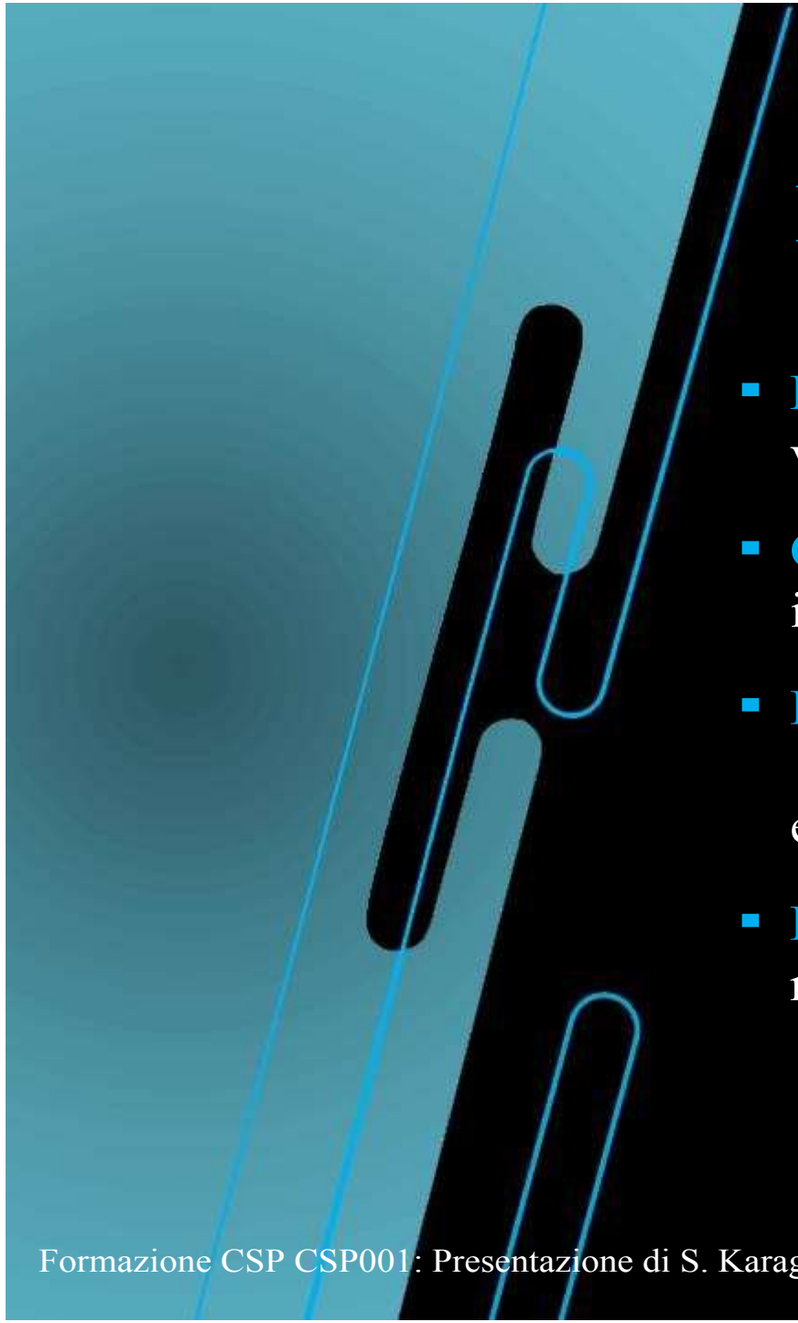
- Esplorare l'intersezione tra AI e cybersicurezza nel settore marittimo.
- Identificare le minacce e le strategie.

IA avversaria e IA difensiva nella sicurezza informatica

Adversarial AI: tentativi deliberati di manipolare gli input dei modelli di AI e di manomettere i set di dati per causare errori o classificazioni errate.

AI difensiva : Obiettivi di mitigare le vulnerabilità e potenziare il sistema di sicurezza.
affidabilità dei sistemi di intelligenza artificiale nella difesa dalle minacce informatiche. Si concentra sul rafforzamento delle misure di sicurezza, come il rilevamento delle intrusioni, il rilevamento delle anomalie e l'analisi delle minacce, per proteggere dagli attacchi avversari.
Lavora per migliorare la resilienza dei sistemi di intelligenza artificiale per resistere agli attacchi e mantenere la loro funzionalità.

IA offensiva: va oltre l'obiettivo specifico dei sistemi di IA e può comprendere una gamma più ampia di obiettivi, come l'infrastruttura IT tradizionale o i dispositivi IoT. Si concentra sullo sviluppo e sull'impiego di tecniche guidate dall'IA per condurre attacchi informatici, come test di penetrazione automatizzati, tecniche di evasione o generazione di malware.



IA avversaria

- Definizione: Utilizza AI tecniche per sfruttare vulnerabilità o ingannare i sistemi di intelligenza artificiale.
- Obiettivo: Obiettivo: compromettere o sovvertire i sistemi di intelligenza artificiale per scopi malevoli.
- Esempi: Attacchi avversari attacchi, come come avvelenamento, evasione o manipolazione dei dati.
- Focus: mirato a verso sfruttare debolezze e minare l'integrità dei modelli e dei sistemi di IA.

AI difensiva (AI nella sicurezza informatica)

L'intelligenza artificiale nella difesa della sicurezza informatica

- Definizione: Utilizza AI tecniche per migliorare le misure di sicurezza informatica e difendersi dalle minacce.
- Obiettivo: Obiettivo: salvaguardare i sistemi, le reti e i dati dalle minacce informatiche.
- Esempi: Intrusione rilevamento, anomalia rilevamento delle anomalie,
  analisi delle minacce informatiche e intelligence sulle minacce.
- Focus: Identificare proattivamente e mitigare le minacce, migliorare la resilienza e la sicurezza.

L'intelligenza artificiale nel settore marittimo

Navigazione e ottimizzazione del percorso

- L'intelligenza artificiale analizza i comportamenti passati per navigare le imbarcazioni in modo autonomo o con equipaggio minimo.
- Fornisce percorsi ottimizzati in base al consumo di carburante, al traffico acqueo e alle condizioni meteorologiche.

Consumo di carburante

- Traccia il consumo di carburante e suggerisce strategie di riduzione.
- Offerte approfondimenti su inefficiente processi per una migliore gestione delle risorse.

Manutenzione di attrezzature e imbarcazioni

- Utilizza i sensori per rilevare i problemi di prestazione delle apparecchiature.
- Avvisa le squadre per una manutenzione tempestiva, aumentando l'efficienza e la sicurezza

Densità e traffico delle porte

- Analizza i dati radar, sonar e GPS per navigare in sicurezza nel traffico.
- Consente di evitare le aree ad alto traffico, riducendo i rischi di collisione.

Grazie

Organizzazione: PDMFC

Si prega di inviare tutte le domande a:
stylianos.karagiannis@pdmfc.com