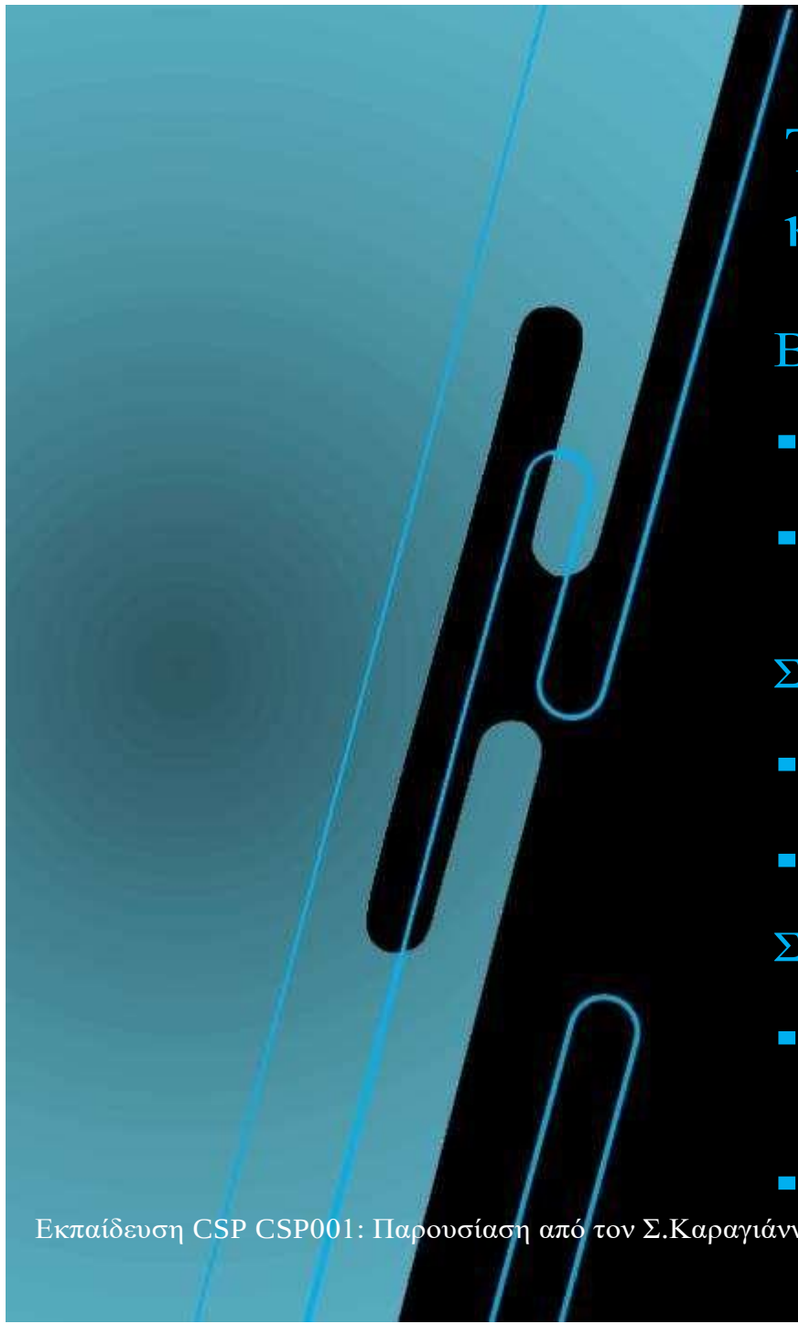
Τεχνητή Νοημοσύνη και κυβερνοασφάλεια: Έρευνα την Ναυτιλία

CSP007

ΠΑΡΟΥΣΙΑΣΗ ΑΠΌ: ΣΤΥΛΙΑΝΌΣ ΚΑΡΑΓΙΑΝΝΗΣ, (PDMFC, ΠΟΡΤΟΓΑΛΙΑ)



Τεχνητή Νοημοσύνη για την ασφάλεια στον κυβερνοχώρο της ναυτιλίας

Βασικά Στοιχεία

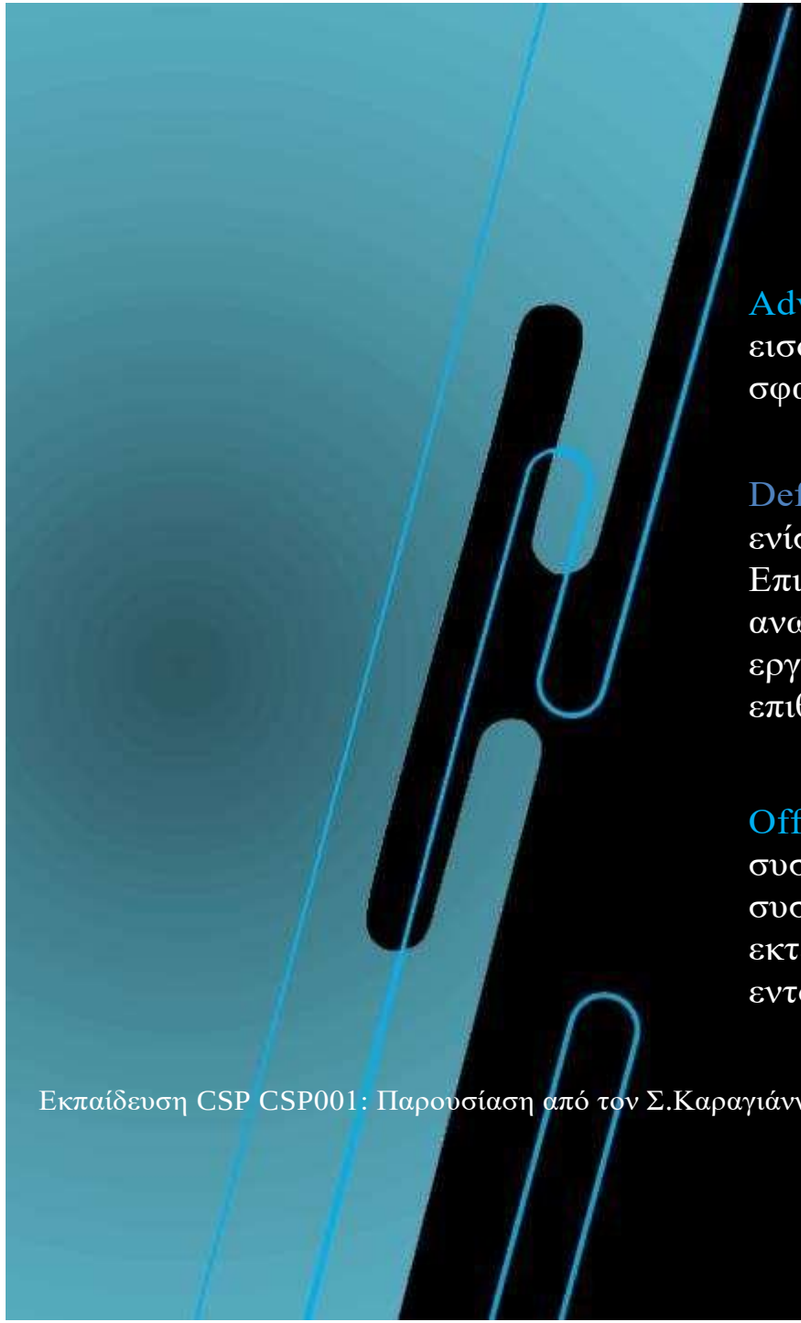
- Η ναυτιλιακή βιομηχανία βασίζεται στις ψηφιακές τεχνολογίες.
- Η ολοκλήρωση της Τεχνητής Νοημοσύνης εισάγει ανησυχίες για την ασφάλεια στον κυβερνοχώρο.

Σημασία της Τεχνητής Νοημοσύνης στη ναυτιλία

- Η Τεχνητή Νοημοσύνη ενισχύει τη λειτουργική αποτελεσματικότητα.
- Ωστόσο, αυξάνει τα τρωτά σημεία της κυβερνοασφάλειας.

Στόχος

- Διερεύνηση της διασταύρωσης Τεχνητής Νοημοσύνης και κυβερνοασφάλειας στη ναυτιλία.
- Προσδιορισμός απειλών και στρατηγικών.



Επιθετική Τεχνητή Νοημοσύνη vs. Αμυντική Τεχνητή Νοημοσύνη στην Κυβερνοασφάλεια

Adversarial AI (Εχθρική Τεχνητή Νοημοσύνη):Στοχευμένες προσπάθειες χειραγώγησης των εισόδων προς τα μοντέλα ΤΝ και αλλοίωσης των συνόλων δεδομένων, με σκοπό την πρόκληση σφαλμάτων ή λανθασμένων ταξινομήσεων.

Defensive AI (Αμυντική Τεχνητή Νοημοσύνη):Στοχεύει στην αντιμετώπιση ευπαθειών και στην ενίσχυση της αξιοπιστίας των συστημάτων ΤΝ για την άμυνα έναντι κυβερνοαπειλών. Επικεντρώνεται στην ενίσχυση μέτρων ασφαλείας, όπως ανίχνευση εισβολών, εντοπισμός ανωμαλιών και ανάλυση απειλών, ώστε να προστατεύει από εχθρικές επιθέσεις. Επιπλέον, εργάζεται προς την ενίσχυση της ανθεκτικότητας των συστημάτων ΤΝ, ώστε να αντέχουν επιθέσεις και να διατηρούν τη λειτουργικότητά τους.

Offensive AI (Επιθετική Τεχνητή Νοημοσύνη): Υπερβαίνει τη στοχοποίηση αποκλειστικά των συστημάτων ΤΝ και μπορεί να περιλαμβάνει ευρύτερα θύματα, όπως παραδοσιακή υποδομή IT ή συσκευές IoT. Επικεντρώνεται στην ανάπτυξη και ανάπτυξη τεχνικών με χρήση ΤΝ για την εκτέλεση κυβερνοεπιθέσεων — π.χ. αυτοματοποιημένο penetration testing, τεχνικές αποφυγής εντοπισμού ή δημιουργία κακόβουλου λογισμικού.

Εχθρική Τεχνητή Νοημοσύνη

- Ορισμός: Χρησιμοποιεί τεχνικές Τεχνητής Νοημοσύνης για την εκμετάλλευση ευπαθειών ή την εξαπάτηση συστημάτων Τεχνητής Νοημοσύνης.

- Στόχος:Η παραβίαση ή υπονόμευση συστημάτων Τεχνητής Νοημοσύνης για κακόβουλους σκοπούς.

- Παραδείγματα:Εχθρικές επιθέσεις, όπως δηλητηρίαση, παράκαμψη ή χειραγώγηση δεδομένων.

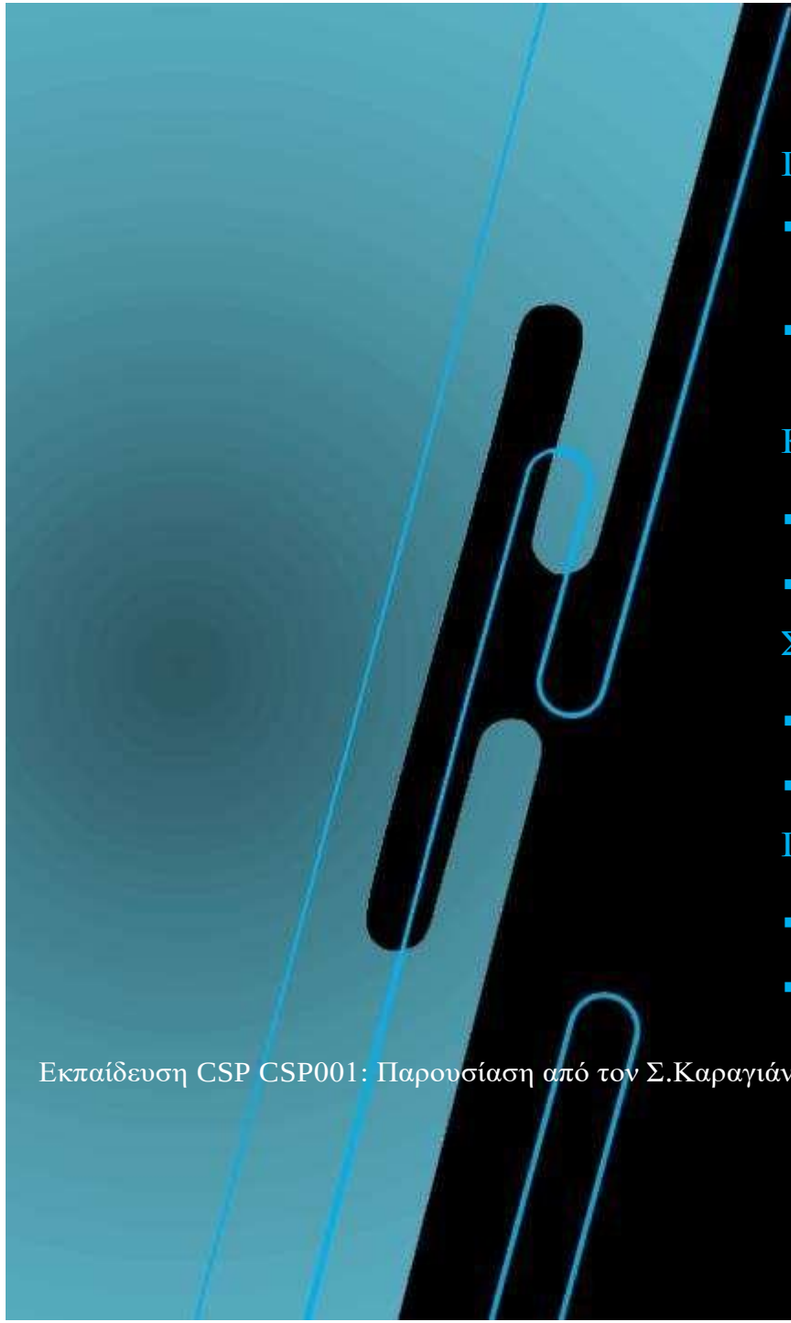
- Εστίαση:Στοχεύει στην εκμετάλλευση αδυναμιών και στην υπονόμευση της ακεραιότητας των μοντέλων και συστημάτων Τεχνητής Νοημοσύνης.

.

Αμυντική Τεχνητή Νοημοσύνη (Τεχνητή Νοημοσύνη στην Κυβερνοασφάλεια)

Τεχνητή Νοημοσύνη στην άμυνα της κυβερνοασφάλειας

- Ορισμός:Χρησιμοποιεί τεχνικές Τεχνητής Νοημοσύνης για την ενίσχυση των μέτρων κυβερνοασφάλειας και την άμυνα κατά των απειλών.
- Στόχος: Η προστασία των συστημάτων, των δικτύων και των δεδομένων από απειλές στον κυβερνοχώρο.
- Παραδείγματα:Ανίχνευση εισβολών, εντοπισμός ανωμαλιών, ανάλυση κακόβουλου λογισμικού και συλλογή πληροφοριών απειλών.
- Εστίαση: Προληπτική αναγνώριση και αντιμετώπιση απειλών, ενίσχυση της ανθεκτικότητας και της ασφάλειας των συστημάτων.



Τεχνητή Νοημοσύνη στη ναυτιλία

Πλοήγηση και βελτιστοποίηση διαδρομής

- Η Τεχνητή Νοημοσύνη αναλύει προηγούμενες συμπεριφορές για να πλοηγεί τα σκάφη αυτόνομα ή με ελάχιστο πλήρωμα.
- Παρέχει βελτιστοποιημένες διαδρομές με βάση τη χρήση καυσίμων, τη κίνηση και τις καιρικές συνθήκες.

Κατανάλωση καυσίμου

- Παρακολουθεί την κατανάλωση καυσίμων και προτείνει στρατηγικές μείωσης.
- Προσφέρει υποδείξεις σε αναποτελεσματικές διαδικασίες για την βελτιωμένη διαχείριση των πόρων.

Συντήρηση εξοπλισμού και σκαφών

- Χρησιμοποιεί αισθητήρες για την ανίχνευση προβλημάτων επίδοσης του εξοπλισμού.
- Ειδοποιεί τα συνεργεία για έγκαιρη συντήρηση, αυξάνοντας την αποδοτικότητα και την ασφάλεια.

Πυκνότητα λιμένων και κίνηση

- Αναλύει δεδομένα ραντάρ, και GPS για την ασφαλή πλοήγηση στην κίνηση.
- Βοηθά στην αποφυγή περιοχών με μεγάλη κυκλοφορία, **μείωση των κινδύνων σύγκρουσης**.

Σας ευχαριστώ

Οργανισμός: PDMFC

Παρακαλούμε στείλτε όλες τις ερωτήσεις στη διεύθυνση:
stylianos.karagiannis@pdmfc.com