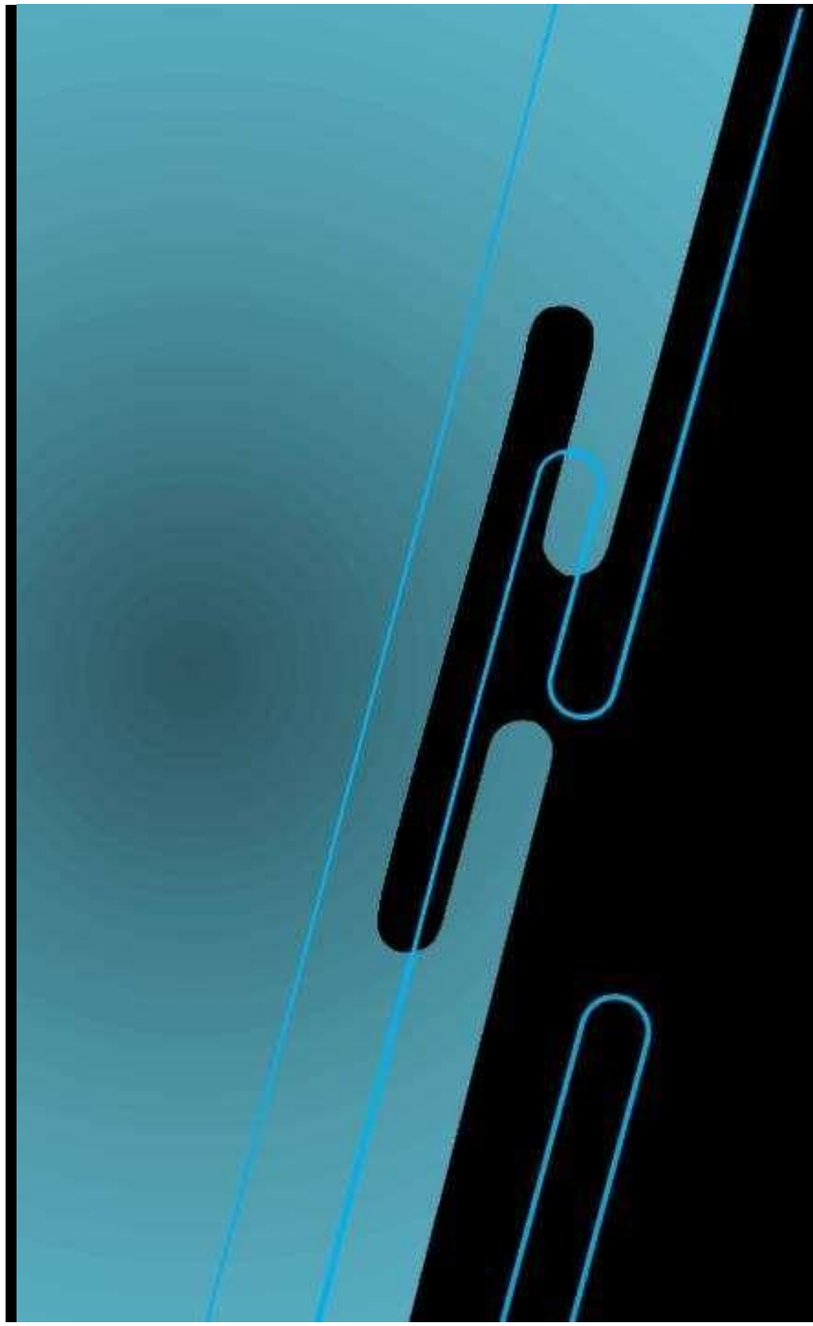
Τεχνητή Νοημοσήνη και κυβερνοασφάλεια: Έρευνα στην Ναυτιλία

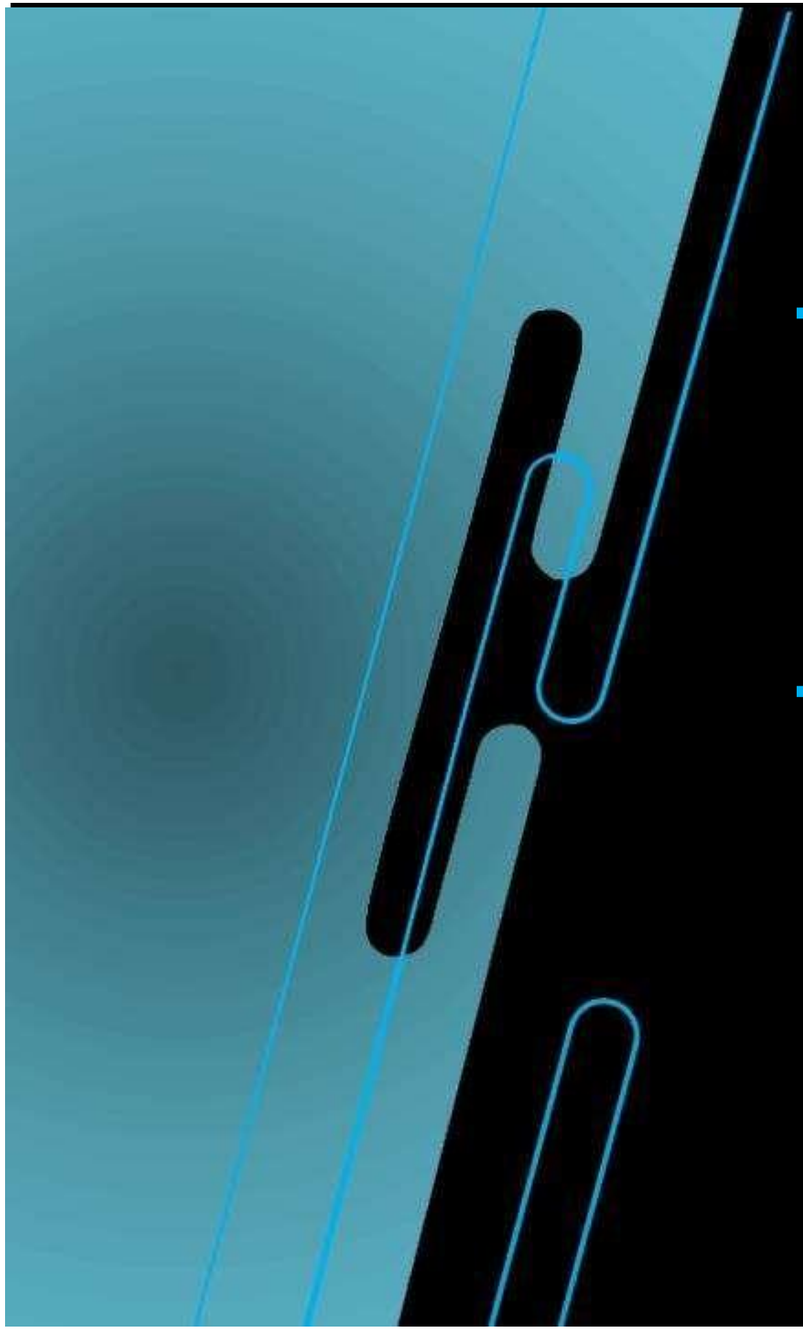
CSP007

PRESENTATION BY: STYLIANOS KARAGIANNIS, (PDMFC, PORTUGAL)



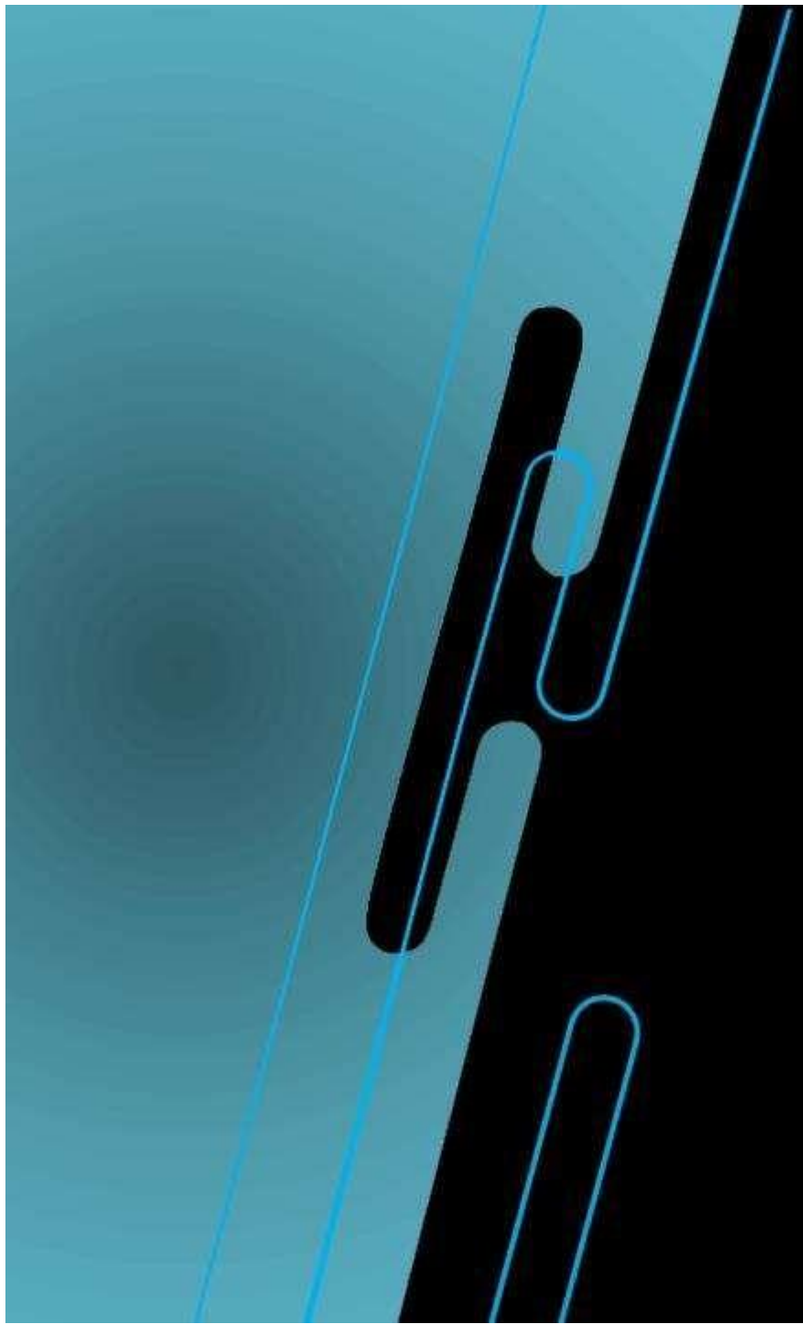
Πρωτόκολλα παρακολούθησης και αναγνώρισης στη ναυτική επικοινωνία

- Σύστημα αυτόματης αναγνώρισης (AIS): Χρησιμοποιείται κυρίως για την παρακολούθηση σκαφών και την αποφυγή συγκρούσεων σε παράκτιες περιοχές και πολυσύχναστες πλωτές οδούς. Λειτουργεί σε συχνότητες VHF και παρέχει πληροφορίες θέσης, πορείας και ταχύτητας σε πραγματικό χρόνο.
- Αναγνώριση και παρακολούθηση μεγάλης εμβέλειας (LRIT): Σχεδιασμένο για αναγνώριση και παρακολούθηση σκαφών μεγάλης εμβέλειας, ιδίως για σκοπούς κανονιστικής συμμόρφωσης και ασφάλειας. Το LRIT λειτουργεί μέσω συστημάτων δορυφορικών επικοινωνιών, επιτρέποντας παγκόσμιες δυνατότητες κάλυψης και παρακολούθησης πέρα από το εύρος του AIS. Παράδειγμα: Τα δεδομένα LRIT διαβιβάζονται μέσω δορυφόρου σε κέντρα δεδομένων LRIT για σκοπούς παρακολούθησης και συμμόρφωσης.



Έκτακτη ανάγκη κινδύνου και εμπορική Λύσεις Επικοινωνίας στη Θάλασσα

- Global Maritime Distress and Safety System (GMDSS): Ένα διεθνώς αναγνωρισμένο σύστημα επικοινωνιών κινδύνου και ασφάλειας στη θάλασσα. Περιλαμβάνει διάφορες τεχνολογίες επικοινωνίας όπως δορυφορικό, HF, VHF και MF ραδιόφωνο, παρέχοντας εφεδρεία και εξασφαλίζοντας αξιόπιστη επικοινωνία σε καταστάσεις έκτακτης ανάγκης.
- Inmarsat: Ένας εμπορικός πάροχος δορυφορικών δικτύων επικοινωνίας που προσφέρει υπηρεσίες φωνής, δεδομένων και διαδικτύου στη ναυτιλιακή βιομηχανία. Ενώ οι υπηρεσίες Inmarsat μπορούν να χρησιμοποιηθούν για επικοινωνία κινδύνου ως μέρος της συμμόρφωσης με το GMDSS, παρέχουν επίσης λύσεις επικοινωνίας και συνδεσιμότητας μη έκτακτης ανάγκης για τις λειτουργίες των πλοίων και την ευημερία του πληρώματος. Παράδειγμα: Το Inmarsat FleetBroadband παρέχει πρόσβαση στο Internet υψηλής ταχύτητας για email, ενημερώσεις καιρού και επικοινωνίες πληρώματος.



Θέματα ευπάθειας GMDSS (Προμηθευτής: Cobham)

Έλεγχος πρόσβασης υλικολογισμικού Θέματα ευπάθειας

CVE-2019-9534: Η έκδοση υλικολογισμικού 1.07 του Cobham EXPLORER 710 στερείται επικύρωσης, επιτρέποντας σε έναν τοπικό εισβολέα χωρίς έλεγχο ταυτότητας να αποστείλει προσαρμοσμένο υλικολογισμικό, οδηγώντας ενδεχομένως σε διάφορες απειλές ασφαλείας.

CVE-2019-9533: Συγκεκριμένος κωδικός πρόσβασης root σε εκδόσεις υλικολογισμικού έως την έκδοση v1.08, ο οποίος θα μπορούσε να αντιστραφεί από εισβολείς για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση.

CVE-2019-9530: Ο ριζικός κατάλογος web της έκδοσης firmware 1.07 του Cobham EXPLORER 710 επιτρέπει στους τοπικούς εισβολείς χωρίς έλεγχο ταυτότητας να έχουν πρόσβαση και να κατεβάζουν οποιοδήποτε αρχείο χωρίς περιορισμούς.

CVE-2019-9532: Η πύλη εφαρμογών web της έκδοσης υλικολογισμικού 1.07 του Cobham EXPLORER 710 μεταδίδει κωδικούς πρόσβασης σύνδεσης σε απλό κείμενο, διευκολύνοντας την υποκλοπή από τοπικούς εισβολείς χωρίς έλεγχο ταυτότητας.

, Πορτογαλία

Ευπάθειες του Inmarsat

Δορυφορικές Επικοινωνίες

CVE-2017-3221: Η φόρμα σύνδεσης Inmarsat AmosConnect 8 είναι ευάλωτη σε Τυφλή έγχυση SQL, επιτρέποντας σε απομακρυσμένους εισβολείς να έχουν πρόσβαση σε ονόματα χρήστη

και κωδικούς πρόσβασης.

CVE-2013-6035: Το υλικολογισμικό σε διάφορα δορυφορικά τερματικά επιτρέπει την απομακρυσμένους εισβολείς για την εκτέλεση αυθαίρετου κώδικα μέσω της θύρας TCP 1827 χωρίς

έλεγχο ταυτότητας.

CVE-2013-6034: Το υλικολογισμικό σε δορυφορικά τερματικά περιέχει ενσωματωμένο κώδικα διαπιστευτήρια, διευκολύνοντας τους εισβολείς να αποκτήσουν μη εξουσιοδοτημένη σύνδεση

πρόσβαση.

Σας ευχαριστώ

Οργανισμός: PDMFC

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