Ορισμοί των εννοιών ασφάλειας και προστασίας

Ενότητα 7- Α2 Κυβερνοασφάλεια: μια κοινή οπτική μεταξύ χρηστών, σχεδιαστών εξοπλισμού, δικτύων μετάδοσης, υπηρεσιών διαχείρισης δεδομένων

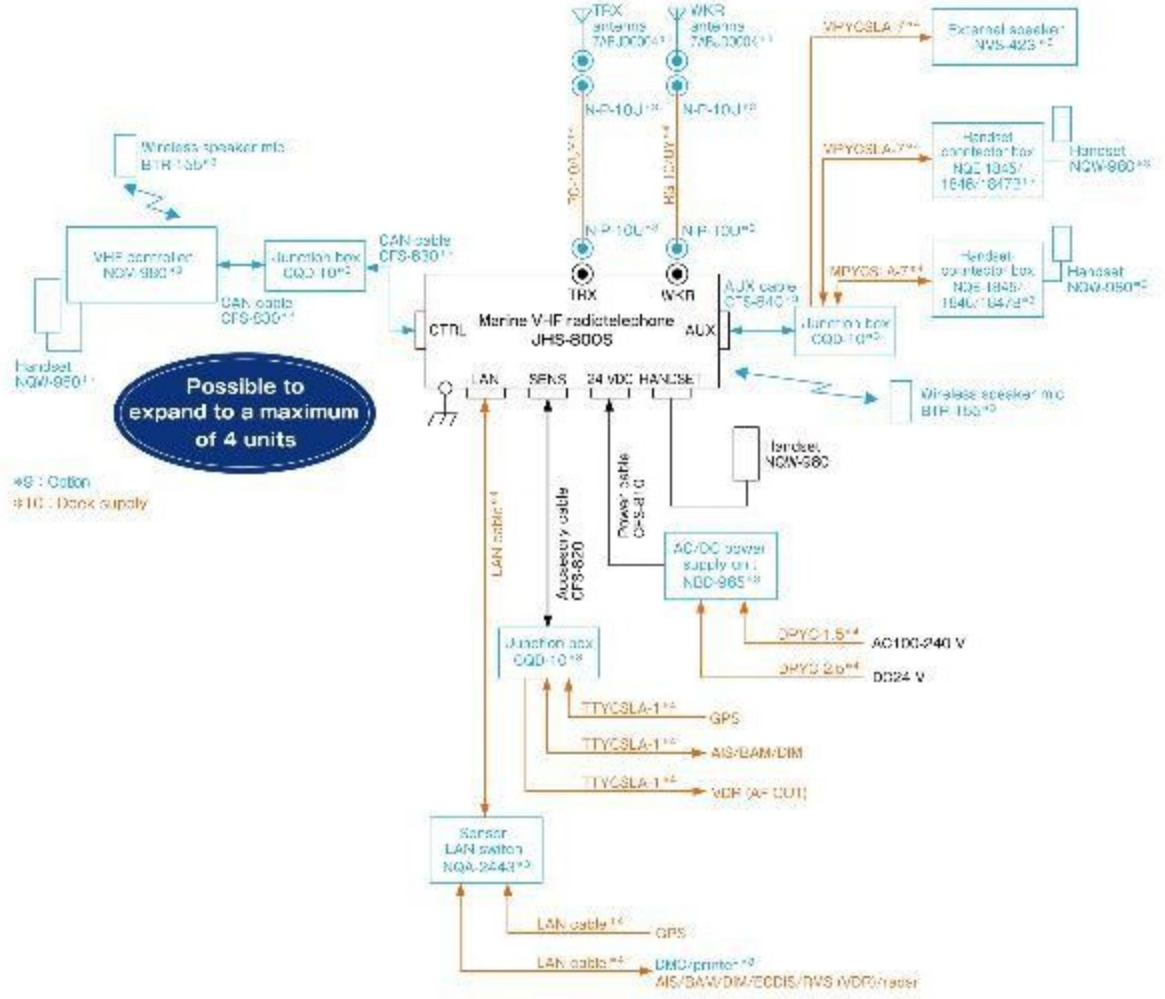
Παράδειγμα: AIS / GNSS / ECDIS

Συστήματα VMS / Πλοήγηση AIS / GNSS / ECDIS

S 10					
Ενότητα 7 - Εφαρμογή μιας αποτελεσματικής πολιτικής κυβερνοασφάλειας		**BC 3**	**45**	*6*	**6**
Ενότητα 7-Α - Ορισμοί των εννοιών ασφάλειας και προστασίας			**15**	**2**	**2**
UE7-A-1	Ασφάλεια και προστασία, δύο ξεχωριστοί αλλά εξίσου σημαντικοί τομείς				
UE7-A-2	Κυβερνοασφάλεια: μια κοινή οπτική μεταξύ χρηστών, σχεδιαστών εξοπλισμού, δικτύων μετάδοσης και υπηρεσιών διαχείρισης δεδομένων *Παράδειγμα: AIS / GNSS / ECDIS*				
UE7-C - Διαχείριση του κινδύνου που συνδέεται με τις κυβερνοεπιθέσεις			**15**	*2*	**2**
UE7-C-1	Προσδιορισμός λειτουργικών τομέων, χαρτογράφησή τους, εξασφάλιση ασφαλή διαλειτουργικότητα - Ανάγκες, διαπιστώσεις, ανάλυση				
UE7-C-2	Ασφάλιση για την κάλυψη των δαπανών που προκύπτουν από κυβερνοεπιθέσεις συστημάτων πληροφοριών				
UE7-D - Οργάνωση των διαδικασιών για τη διασφάλιση της κυβερνοασφάλειας της επιχείρησης και του περιβάλλοντός της			**15**	*2*	**2**
UE7-D-1	Οι φάσεις της δράσης: πρόβλεψη και παρακολούθηση, αντίδραση και καταπολέμηση, αποκατάσταση				
UE7-D-2	Διαχείριση της εσωτερικής και εξωτερικής επικοινωνίας με τους συνεργάτες, τους προμηθευτές, πελάτες				

ΑΥΤΟΜΑΤΟ ΣΥΣΤΗΜΑ ΤΑΥΤΟΠΟΙΗΣΗΣ

Τι είναι το AIS;



JRC – E/R VHF Marine JHS-800S
Με λειτουργία ASN

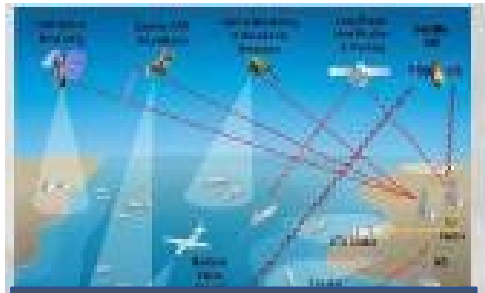
AIS / GNSS – Χρήστες / Χρήσεις

Δημόσιοι φορείς

Δημόσιοι φορείς

Ιδιωτικοί φορείς

Ιδιωτικοί φορείς

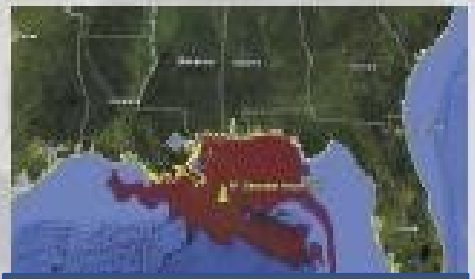


Επιτήρηση και ασφάλεια

SAR

Πληροφορίες

Αντι-πειρατεία



Παρακολούθηση περιβάλλοντος

Έρευνες

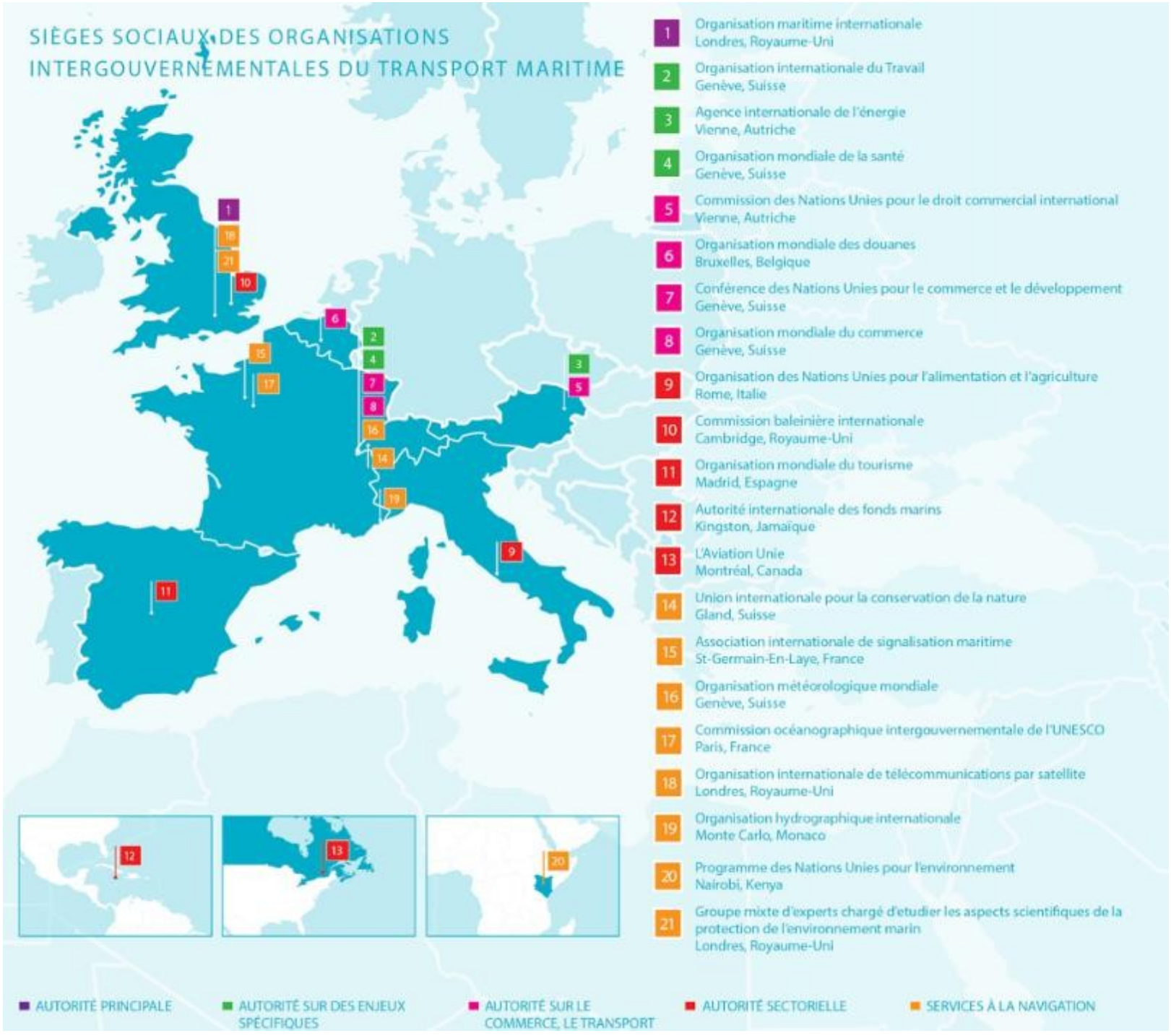
Παρακολούθηση εφοδιαστικής

Παρακολούθηση πετρελαίου / φυσικού αερίου

Παρακολούθηση αλιείας

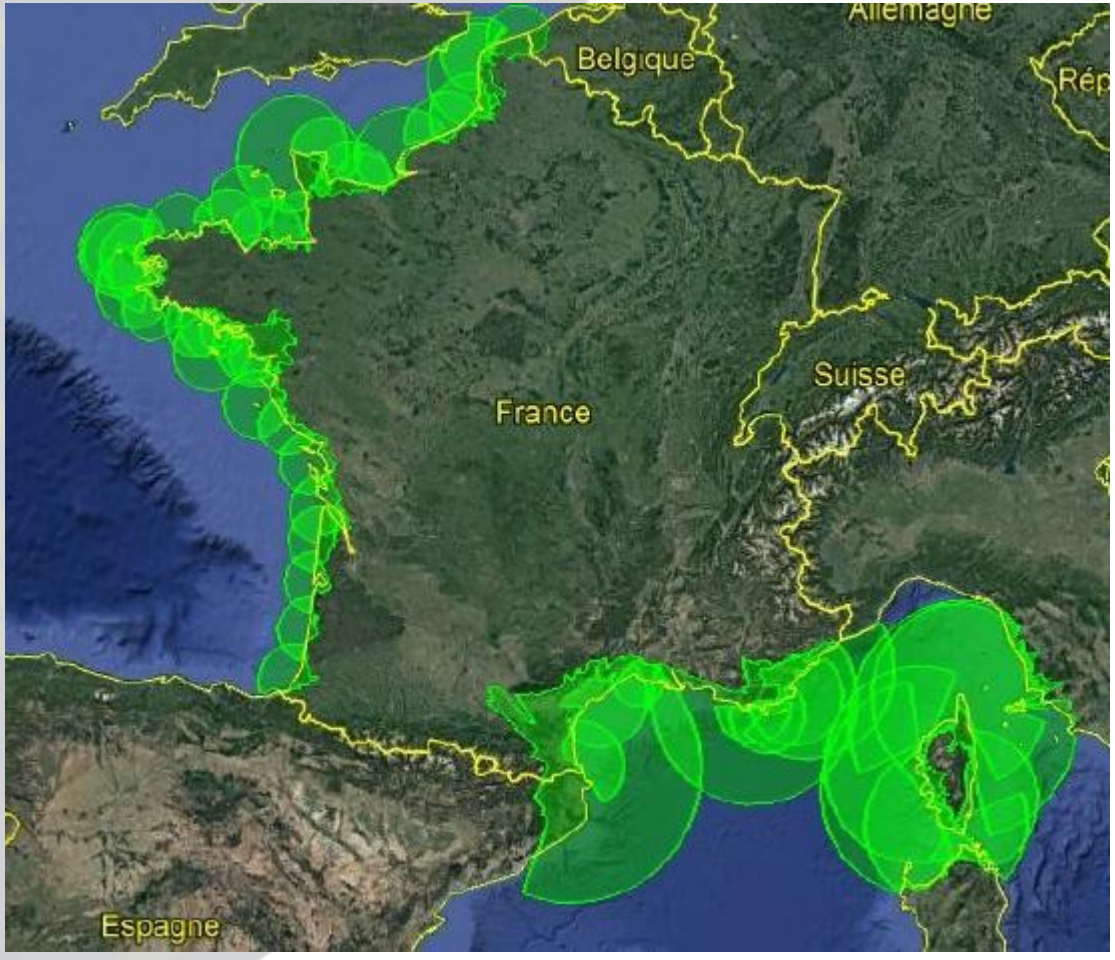
Διακυβέρνηση ναυτιλιακή

(υπενθύμιση)

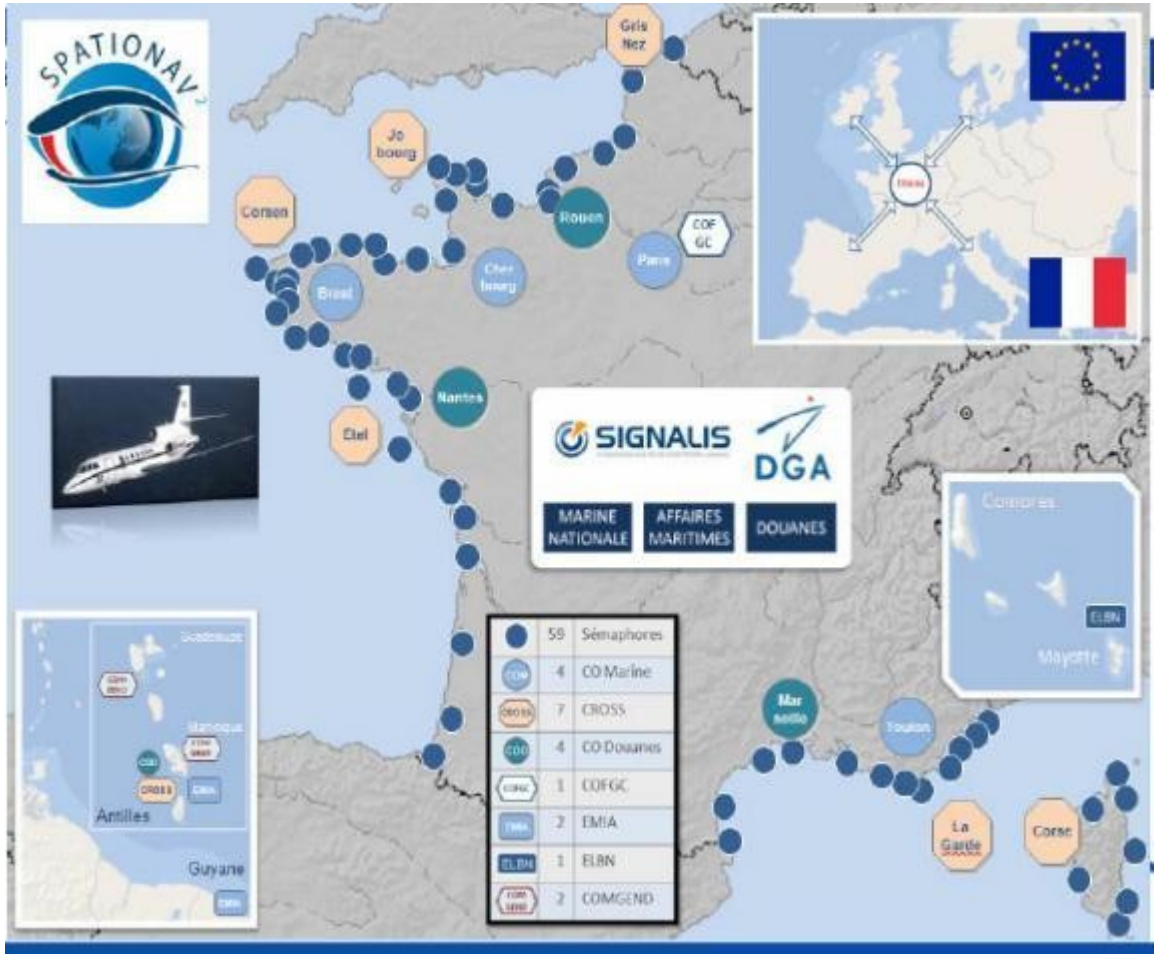


AIS / GNSS – Εθνικός οργανισμός

Δίκτυο AIS «πολιτικής» ακτής στη Γαλλία (40 τοποθεσίες)



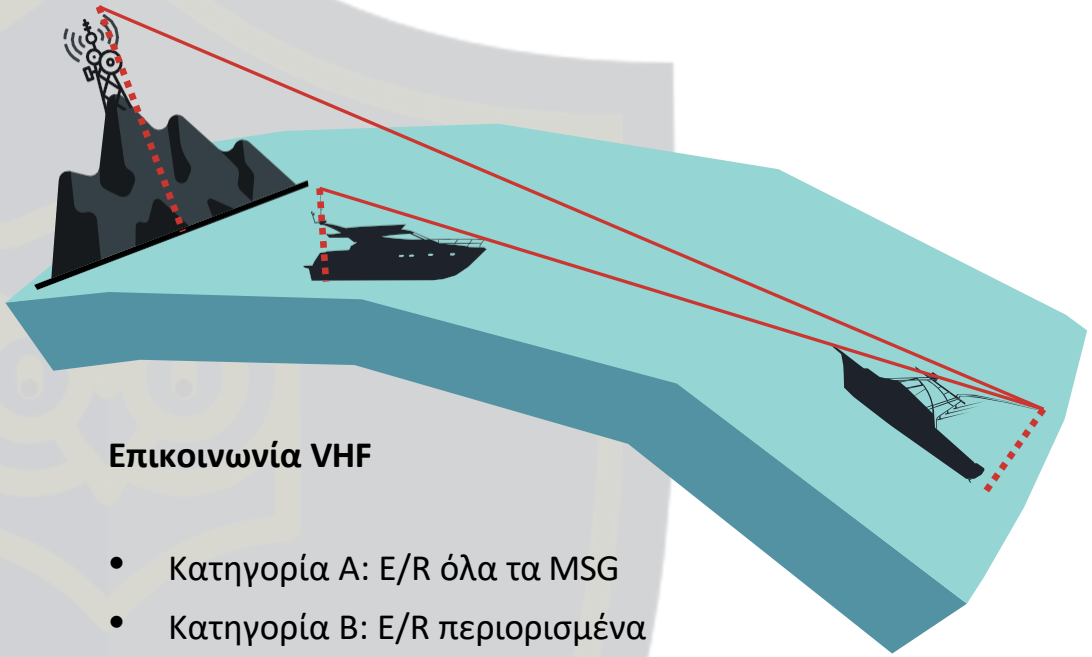
Δίκτυο AIS / «στρατιωτικό» παράκτιο ραντάρ (130 τοποθεσίες)



Λειτουργία του AIS

- Αρχές
- Μηνύματα
- Νομικές υποχρεώσεις
- Πλεονεκτήματα και αδυναμίες
- AIS και κίνδυνος στον κυβερνοχώρο
- Περιπτώσεις

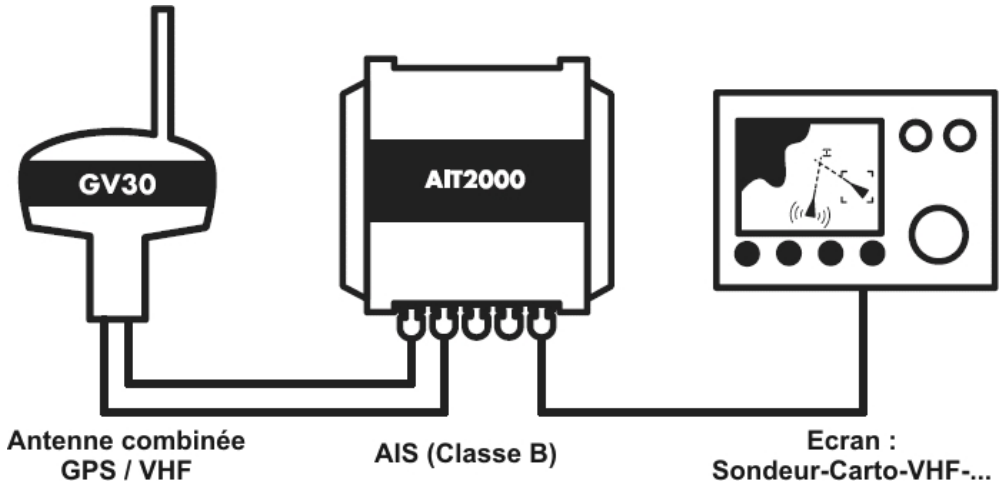
AIS / GNSS – Λειτουργία του συστήματος επικοινωνίας



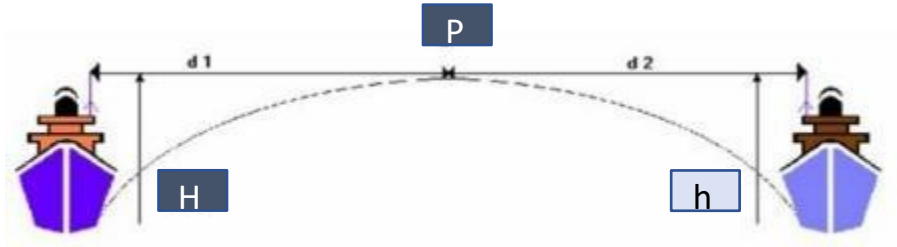
Επικοινωνία VHF

- Κατηγορία A: E/R όλα τα MSG
- Κατηγορία B: E/R περιορισμένα MSG

Αναμεταδότης AIS



Ο τύπος της οπτικής / ραντάρ εμβέλειας



Οπτική εμβέλεια (Nq) = 2,2 ($\sqrt{H(ft)}$ + $\sqrt{h\ (ft\ )}$)

Παράδειγμα:

1 / Σε ποια απόσταση μπορώ να δω ένα πλοίο στη θάλασσα ύψους 20 μέτρων αν βρίσκομαι σε έναν πύργο ύψους 100 μέτρων; 2/ Σε ποια απόσταση μπορώ να δω ένα πλοίο στη θάλασσα ύψους 20 μέτρων αν βρίσκομαι στην παραλία;

1/ 102 km

2/ 34 km

1 ft = 0,305 m

AIS / GNSS – Διασύνδεση με το σύστημα ECDIS

Κεραία GPS

ΚεραίαVHF

Διεπαφή χρήστη
(ECS ή ECDIS)

Αναμεταδότης AIS

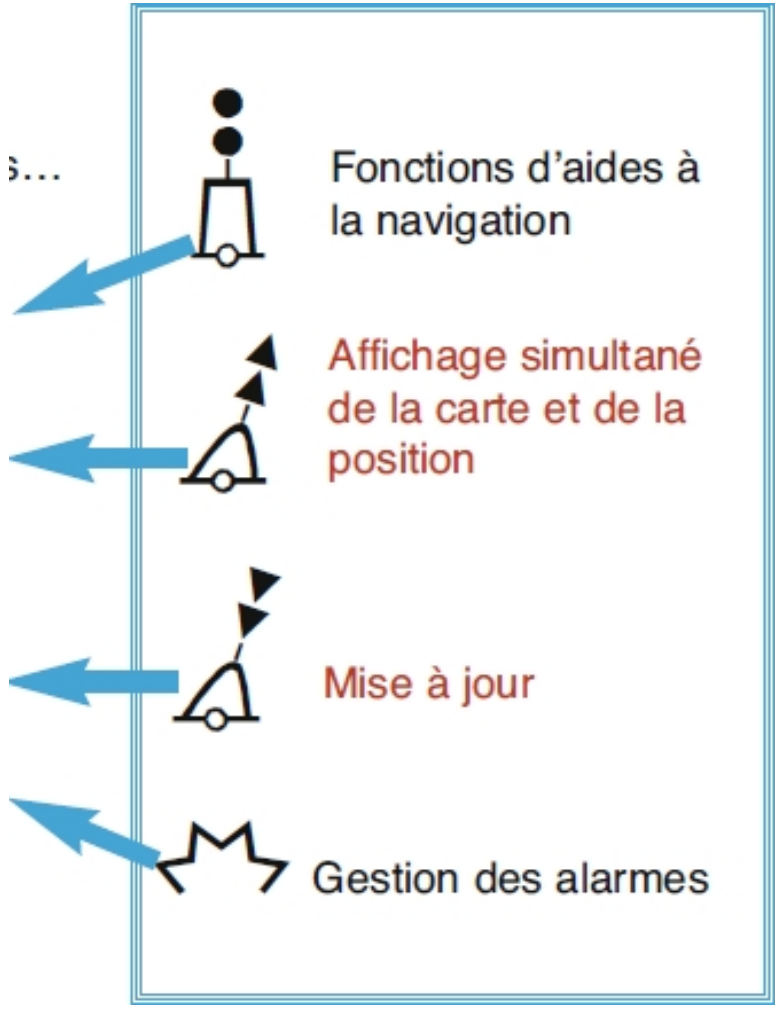
Διεπαφή πιλότου

Λοχ

CCV (Πυξίδα)

GPS

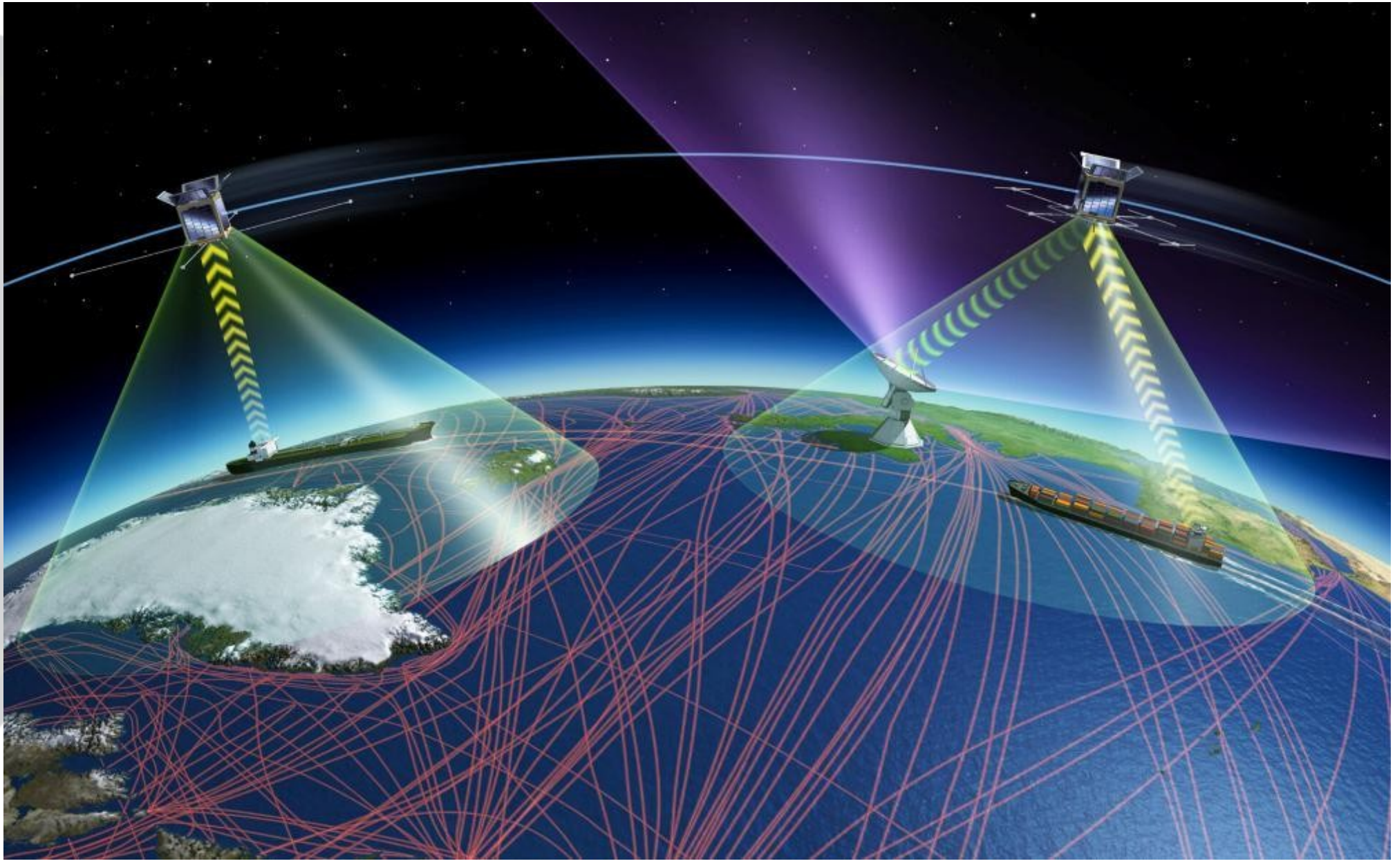
Τροφοδοσία



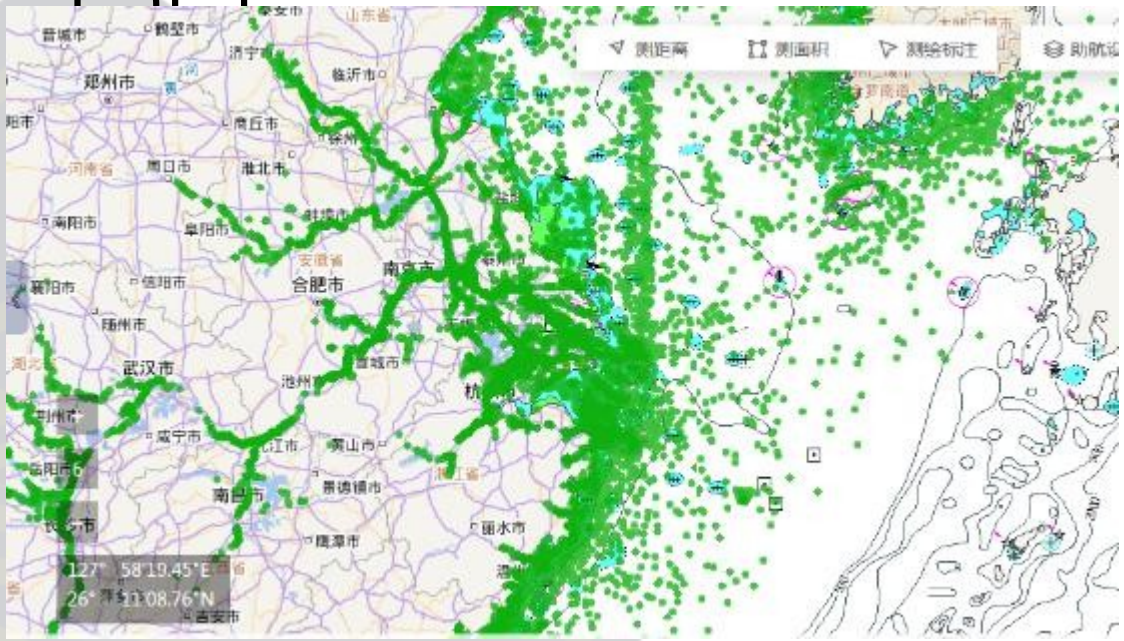
Πληροφορίες που μεταδίδονται από το AIS

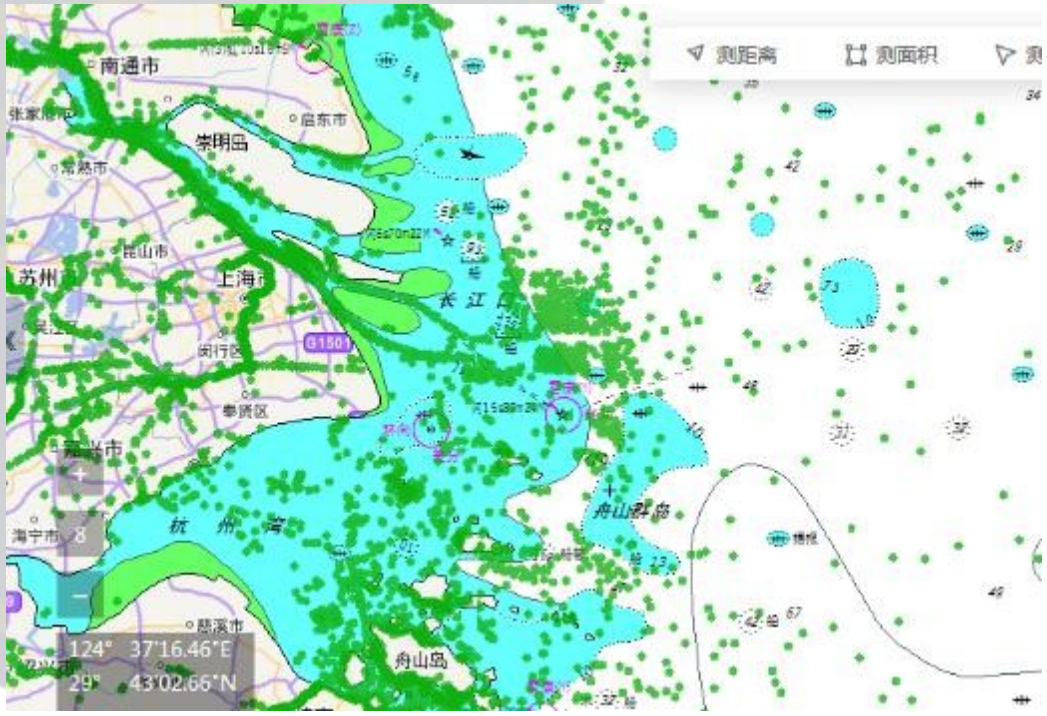
Static information	Dynamic information	Voyage related information
Every 6 minutes and on request by a competent authority	*Dependent on speed and course alteration*	*Every 6 minutes, when data is amended or on request*
MMSI (Maritime Mobile Service Identity)	**Ship's position**	**Ship's draught**
Call sign and **name**	**Position Time stamp** in UTC	**Hazardous** cargo (type)
IMO Number	**Course over ground** (COG)	**Destination** ETA (Estimated Time of Arrival)
Length and beam	**Speed over ground** (SOG)	
Type of ship	**Navigational status** (underway, at anchor, moored...)	
Location of position fixing antenna	Rate of turn (ROT)	

Συλλογή δεδομένων AIS μέσω δορυφόρου

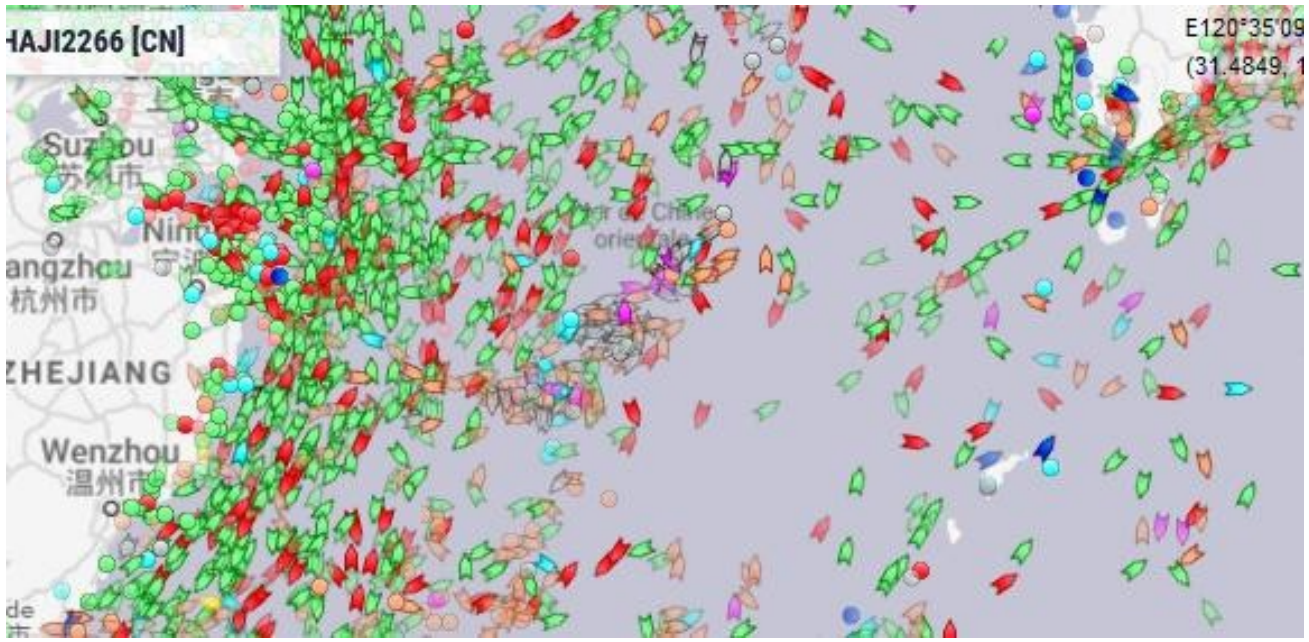


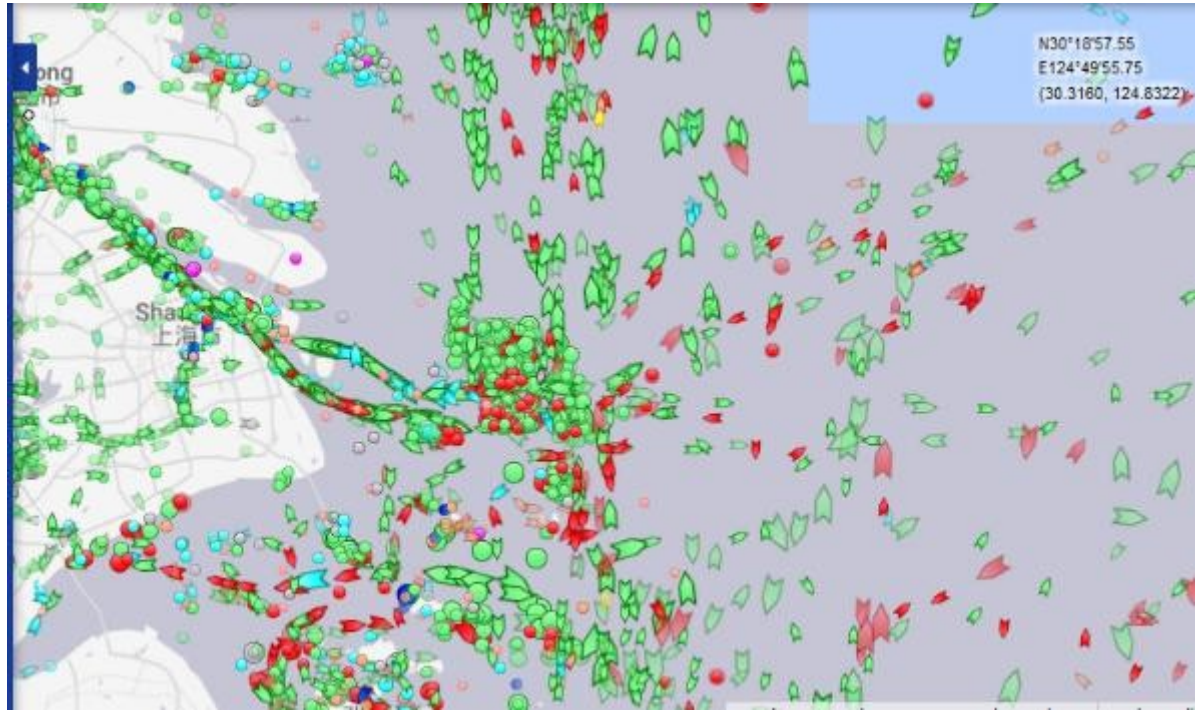
ΧαρτογραφίαAIS





Marinetraffic.com (δορυφόροι)





AIS και CYBER

- Τύποι επιθέσεων
- Παρεμβολές
- Spoofing / Υπεξαίρεση
- Αντιμετώπιση
- Παράδειγμα

Τύπος επιθέσεων

Υποκλοπή ταυτότητας – Τα μηνύματα AIS που μεταδίδονται παρέχουν πληροφορίες σχετικά με την ταυτότητα των πλοίων, τις προηγούμενες, τρέχουσες και μελλοντικές θέσεις τους, καθώς και το φορτίο τους. Η υποκλοπή της θέσης ενός πλοίου μπορεί να οδηγήσει σε περιστατικά ή ακόμη και ατυχήματα.

Υποκλοπή βοηθημάτων πλοήγησης – Ψευδείς πληροφορίες βοηθημάτων πλοήγησης, όπως ένας φάρος που προειδοποιεί για την παρουσία υφάλων, μπορούν να αναγκάσουν ένα πλοίο να αλλάξει την πορεία του. Αυτό μπορεί να γίνει για να αναγκαστεί ένα πλοίο να εισέλθει σε μια περιοχή όπου μπορεί να εκτραπεί.

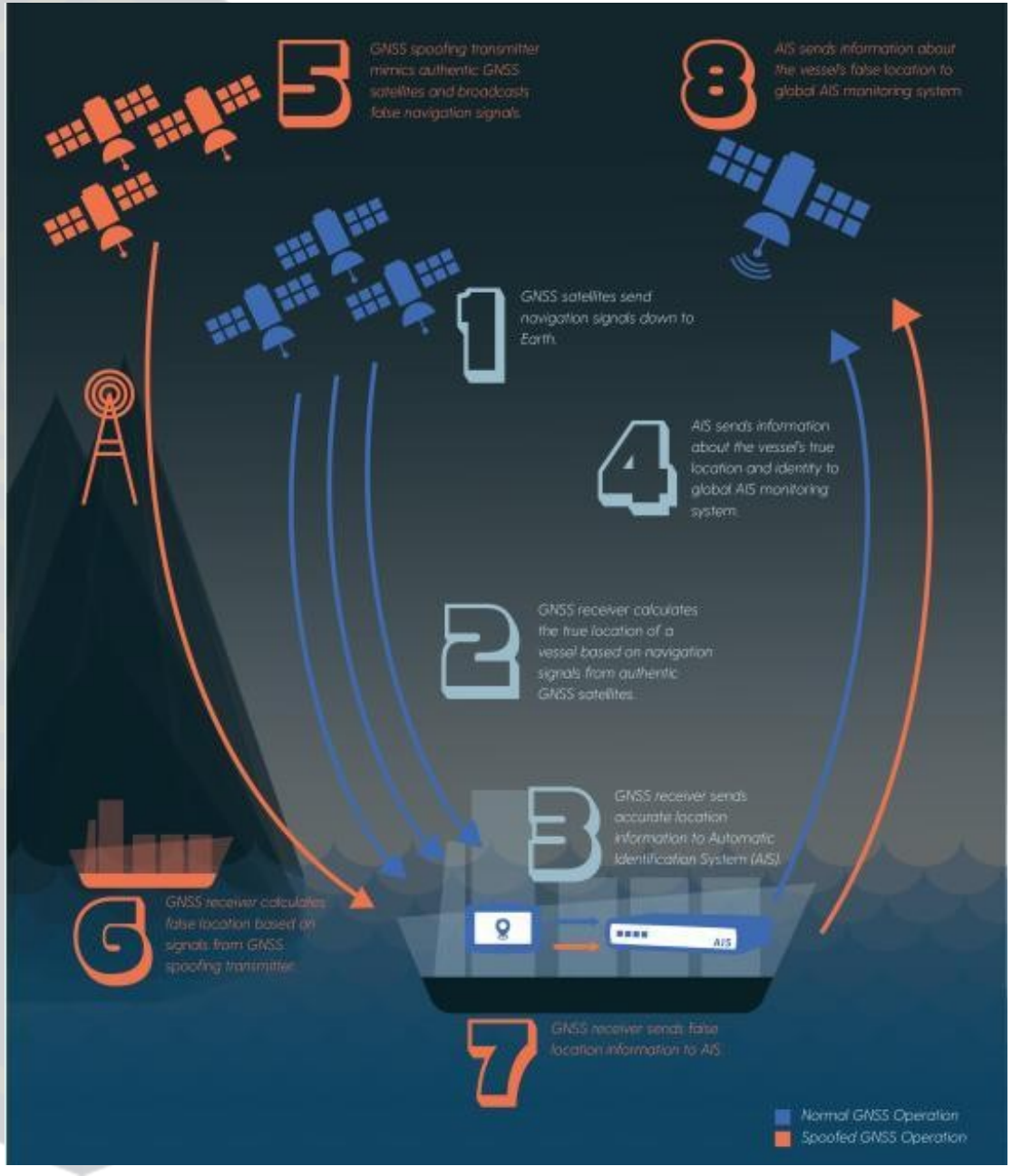
Υποκλοπή / σύγκρουση – Η αποφυγή συγκρούσεων είναι μία από τις κύριες χρήσεις του AIS. Παρέχοντας πλαστά στοιχεία ενός πλοίου που βρίσκεται σε πορεία σύγκρουσης, ένας εισβολέας μπορεί να αναγκάσει ένα πλοίο να αλλάξει πορεία για να αποφύγει τη σύγκρουση. Αυτό θα μπορούσε, για παράδειγμα, να χρησιμοποιηθεί για να οδηγήσει το πλοίο σε προσάραξη.

Παραβίαση AIS-SART – Η έρευνα και διάσωση είναι μια άλλη χρήση του AIS. Αυτή η επίθεση δημιουργεί ένα ψεύτικο σήμα SART (Transponder Search and Rescue), το οποίο περιγράφει μια κατάσταση έκτακτης ανάγκης. Τα πλοία που λαμβάνουν το σήμα SART είναι νομικά υποχρεωμένα να βοηθήσουν στις επιχειρήσεις διάσωσης, οπότε η πλαστογράφηση SART μπορεί να χρησιμοποιηθεί για να προσελκύσει πλοία σε ένα σημείο όπου μπορούν να δεχθούν επίθεση.

Παραποίηση μετεωρολογικών προγνώσεων – Το AIS μπορεί να χρησιμοποιηθεί για τη μετάδοση πληροφοριών σχετικά με τις καιρικές συνθήκες. Μια ψευδής πρόγνωση, ειδικά μια που προβλέπει καλές συνθήκες ενώ πλησιάζει καταιγίδα, θα μπορούσε να χρησιμοποιηθεί για να βάλει ένα πλοίο σε κίνδυνο.

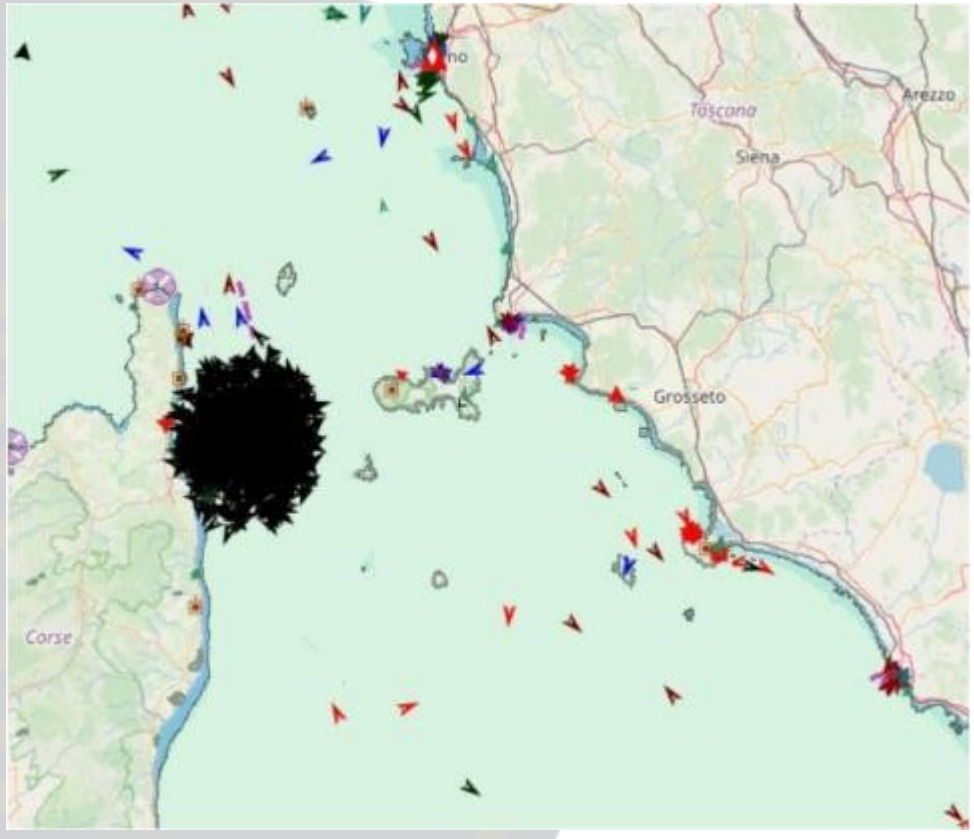
Παραβίαση AIS – Είναι δυνατό να αντικατασταθούν τα σήματα που στέλνουν τα πλοία, εκπέμποντας ένα σήμα μεγαλύτερης ισχύος την ίδια στιγμή και στην ίδια συχνότητα. Ο εισβολέας μπορεί τότε να τροποποιήσει ορισμένες λεπτομέρειες του αρχικού μηνύματος, για παράδειγμα για να υποδείξει ότι το πλοίο μεταφέρει επικίνδυνο φορτίο σε μια ζώνη όπου τέτοια φορτία είναι παράνομα.

Πώς μπορεί να παραποιηθεί το AIS;



1. Οι δορυφόροι GPS στέλνουν σήματα στο πλοίο.
2. Ο δέκτης GPS υπολογίζει τη θέση του πλοίου με βάση τα σήματα που προέρχονται από αυθεντικούς δορυφόρους GPS.
3. Ο δέκτης GPS στέλνει ακριβείς πληροφορίες θέσης στο AIS.
4. Το AIS στέλνει πληροφορίες σχετικά με την πραγματική θέση του πλοίου και το αναγνωρίζει στο παγκόσμιο σύστημα παρακολούθησης του AIS.
5. Ο πλαστός πομπός GNSS μιμείται το αυθεντικό σήμα των δορυφόρων GNSS και εκπέμπει ψευδή σήματα πλοήγησης.
6. Ο δέκτης GNSS υπολογίζει την ψευδή θέση με βάση τα σήματα του πλαστού πομπού GNSS.
7. Ο δέκτης GNSS στέλνει ψευδείς πληροφορίες ψευδείς τοποθεσίας στο AIS.
8. Το AIS στέλνει πληροφορίες σχετικά με την ψευδή θέση του πλοίου στο παγκόσμιο σύστημα παρακολούθησης του AIS.

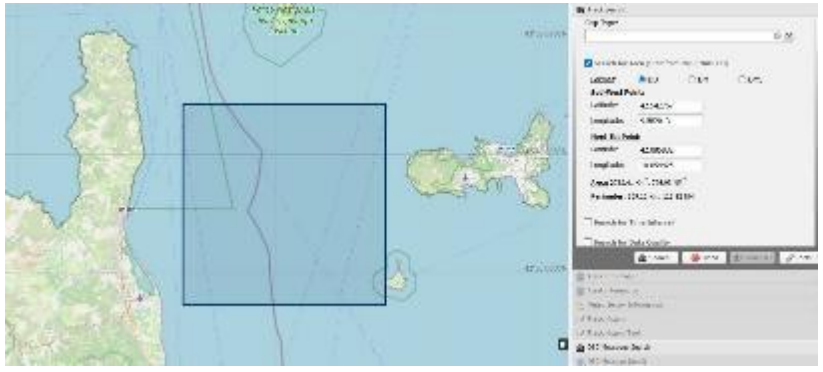
Επίθεση με Spoofing



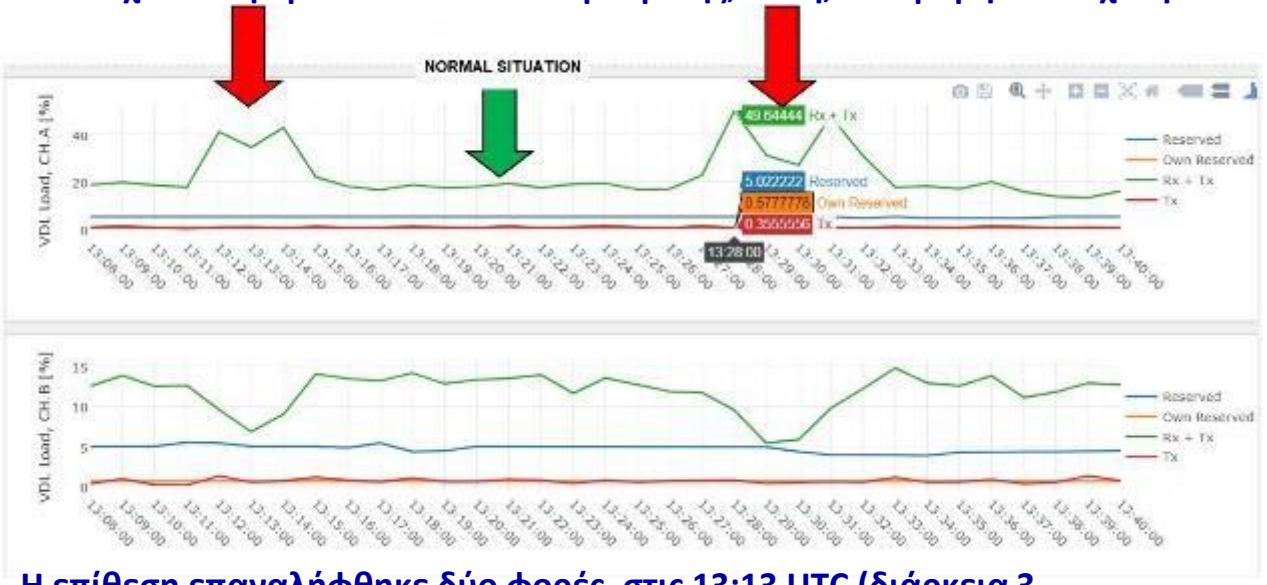
Αυτές οι πληροφορίες είχαν κατακλύσει πλήρως μια κυκλική θαλάσσια περιοχή με ακτίνα περίπου 15 Nm. Η περιοχή που επηρεάστηκε από την επίθεση κατακλύστηκε με την εισαγωγή πάνω από 850 ψευδών στόχων.

ΥΠΟΥΡΓΕΙΟ ΒΙΩΣΙΜΩΝ ΥΠΟΔΟΜΩΝ ΚΑΙ ΚΙΝΗΤΙΚΟΤΗΤΑΣ

ΙΤΑΛΙΚΗ ΑΚΤΟΦΥΛΑΚΗ



Στις 3/12/19, μεταξύ του νησιού Έλβα και της Κορσικής, ελήφθησαν εκατοντάδες πληροφορίες AIS από ναυτικές μονάδες με ολλανδική σημαία, οι οποίες είχαν δημιουργηθεί τεχνητά και είχαν διαφορετικό κωδικό αναγνώρισης, θέση, διαδρομή και ταχύτητα.



Η επίθεση επαναλήφθηκε δύο φορές, στις 13:13 UTC (διάρκεια 3 λεπτών) και στις 13:28 (διάρκεια 4 λεπτά).

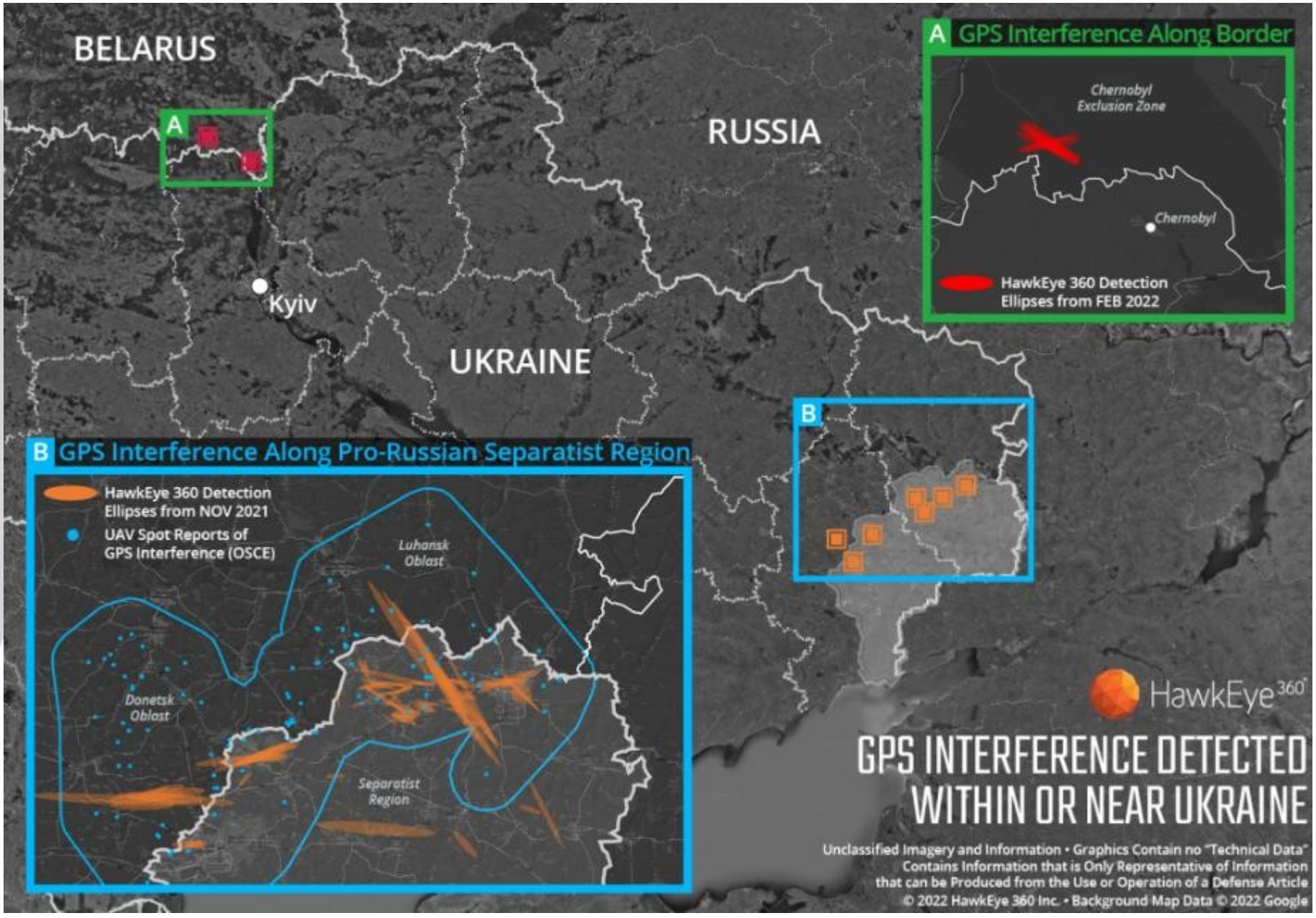
Η παρεμβολή

ANFR
AGENCE NATIONALE DES FRÉQUENCES

Brouillage en zone portuaire, en Martinique.

l'ANFR
(L'agence Nationale
des Fréquences)
mène l'enquête.

Παρεμβολή περιοχής

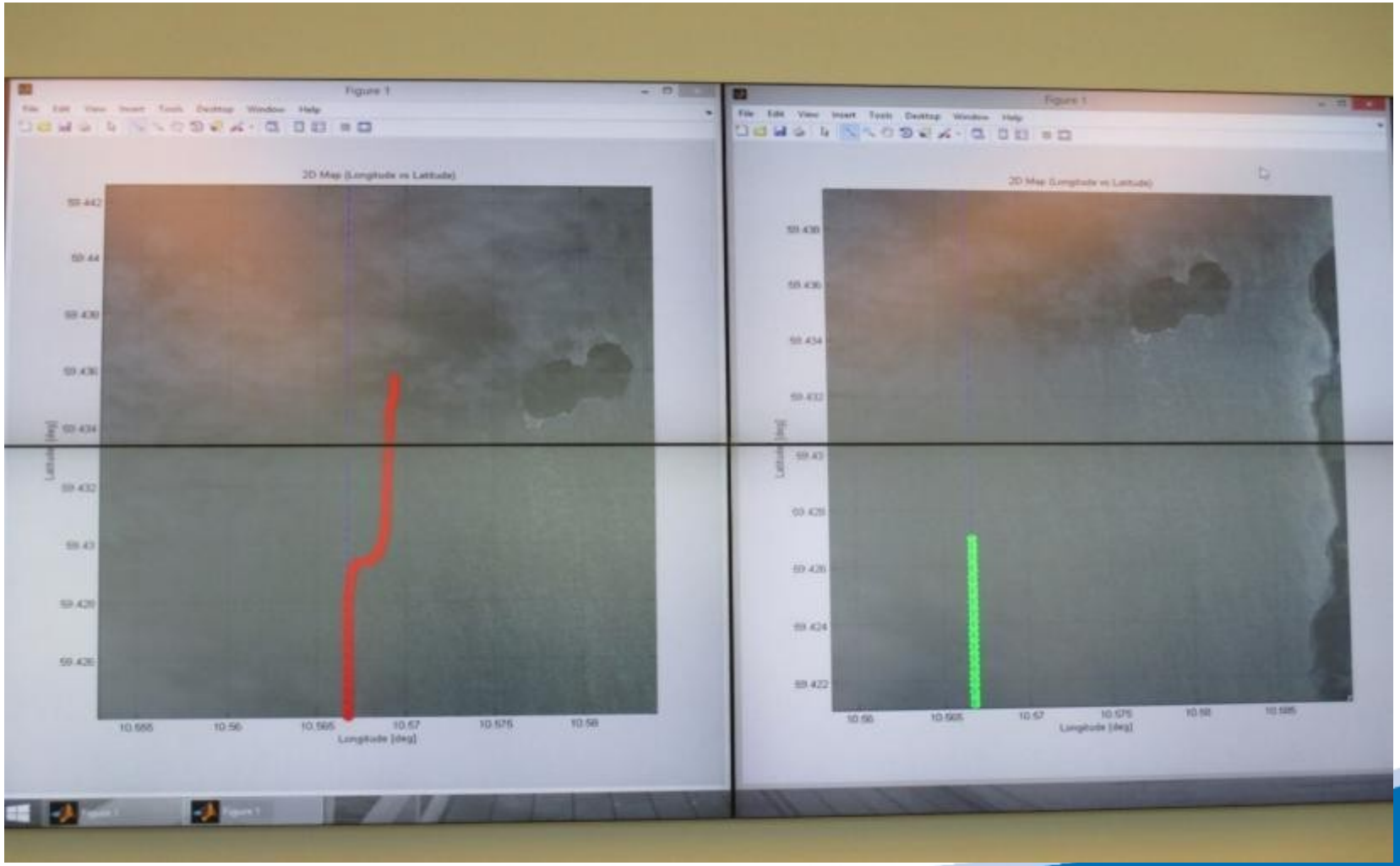


Federal Police

Spoofing AIS / GNSS

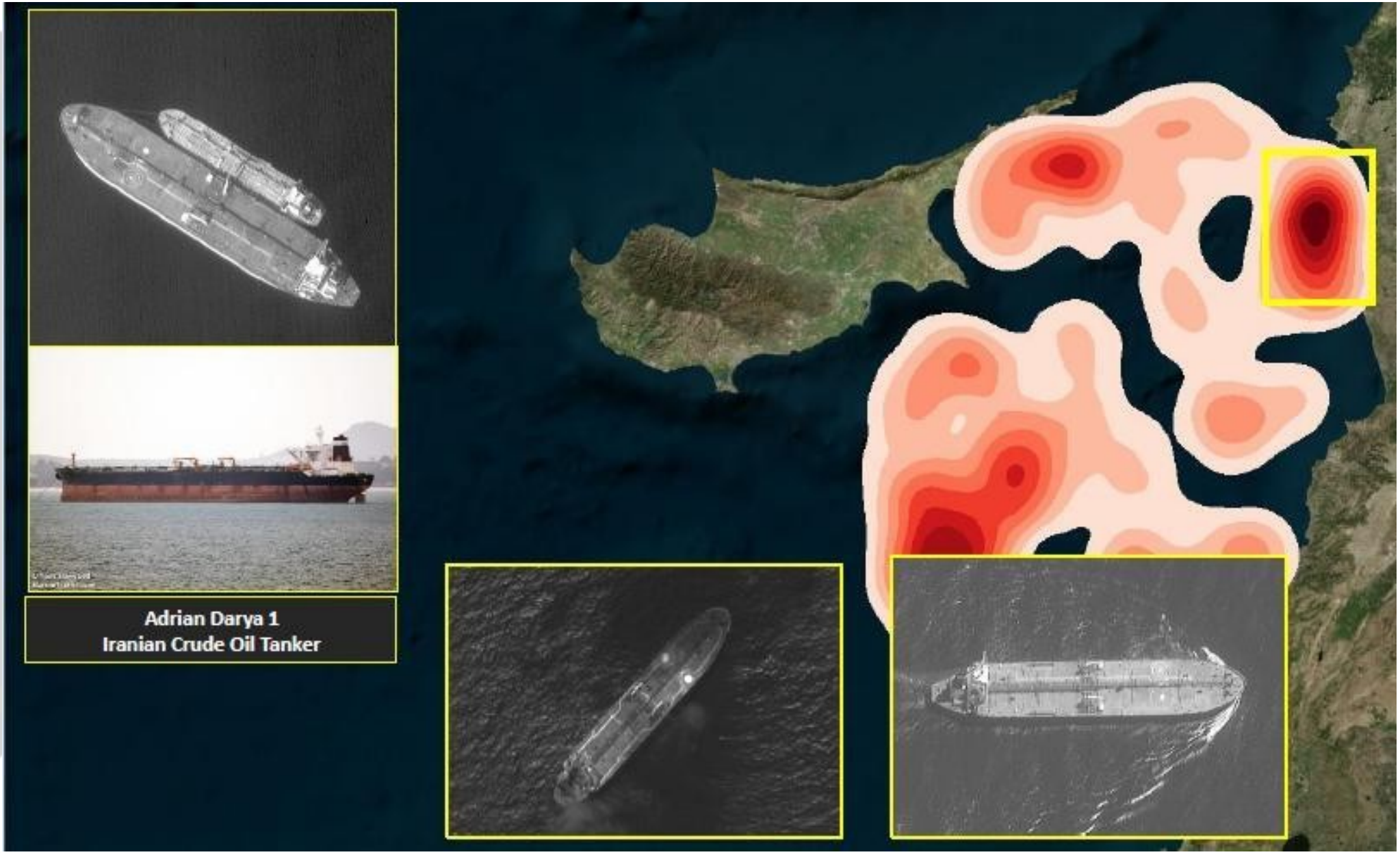
Πηγή: Γερμανική Θαλάσσια Αστυνομία

Παραποίηση θέσης

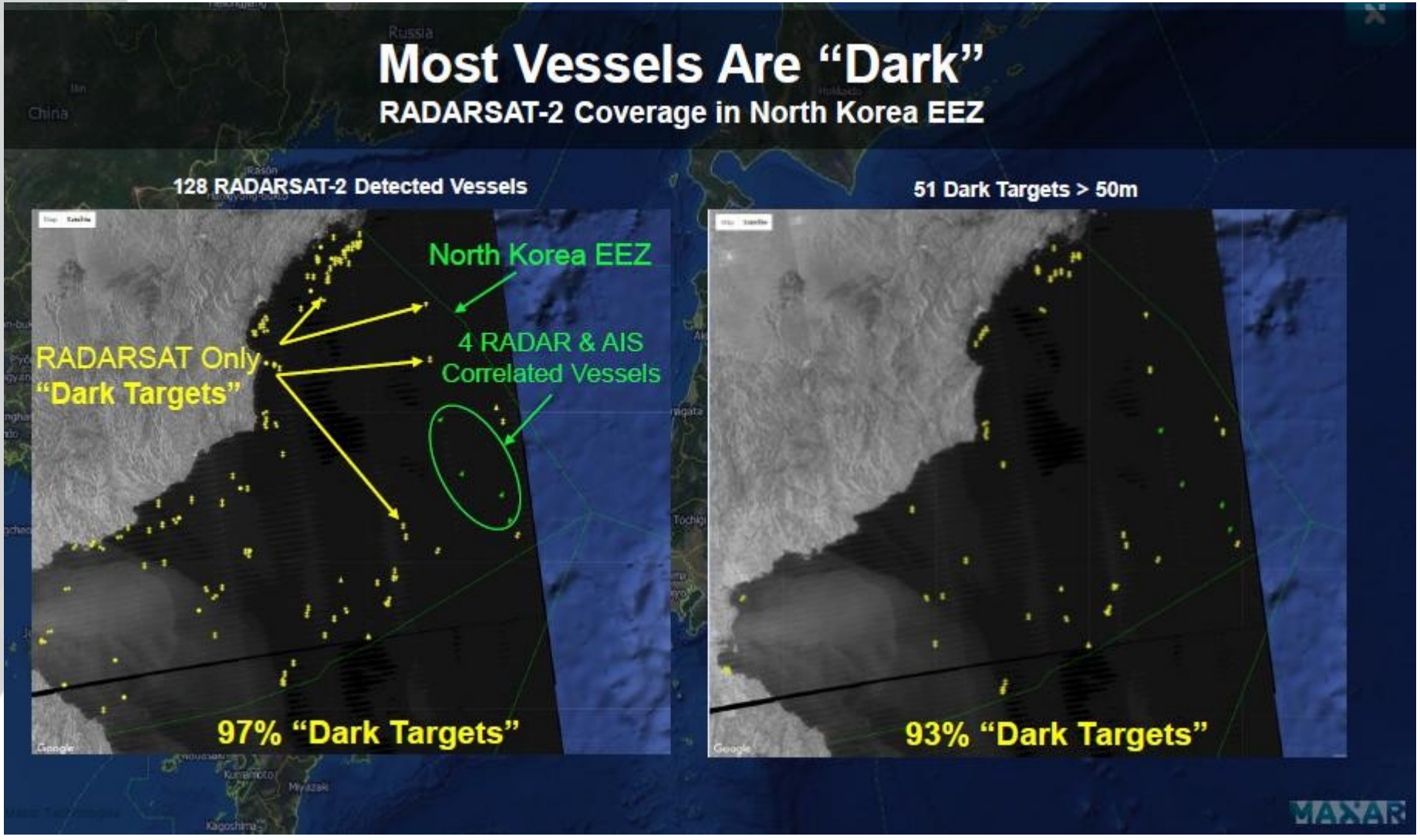


Πραγματική θέση

Παράνομη χρήση του AIS - Οι φάντασμα στόλοι



Παράνομη χρήση του AIS - Οι φάντασμα στόλοι



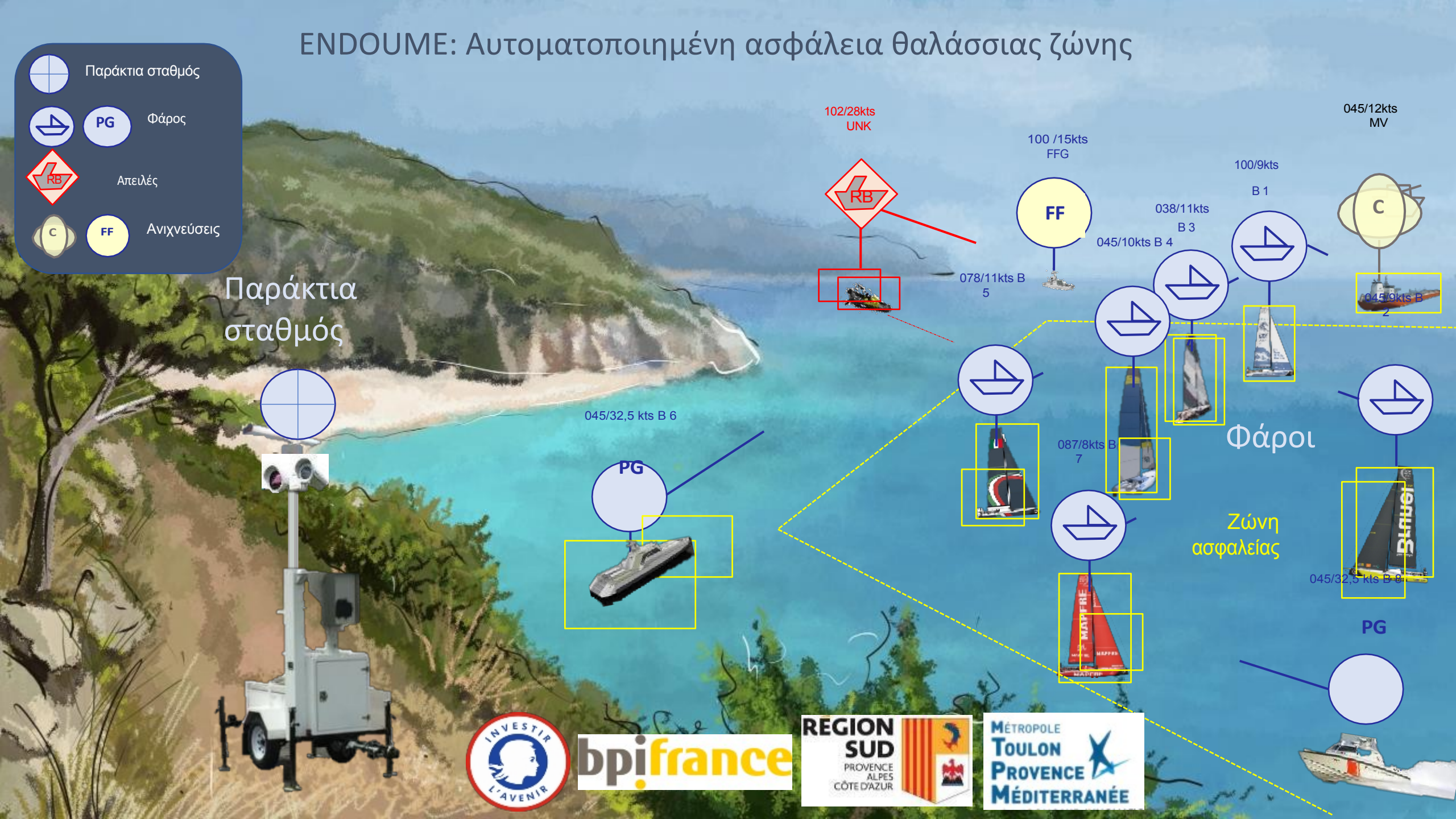
Μελέτη ασφάλειας AIS

Έργο ENDOUME

Ολυμπιακοί Αγώνες 2024 - Παρίσι

- Μοντέλο ANSSI
- EBIOS

ENDOUME: Αυτοματοποιημένη ασφάλεια θαλάσσιας ζώνης



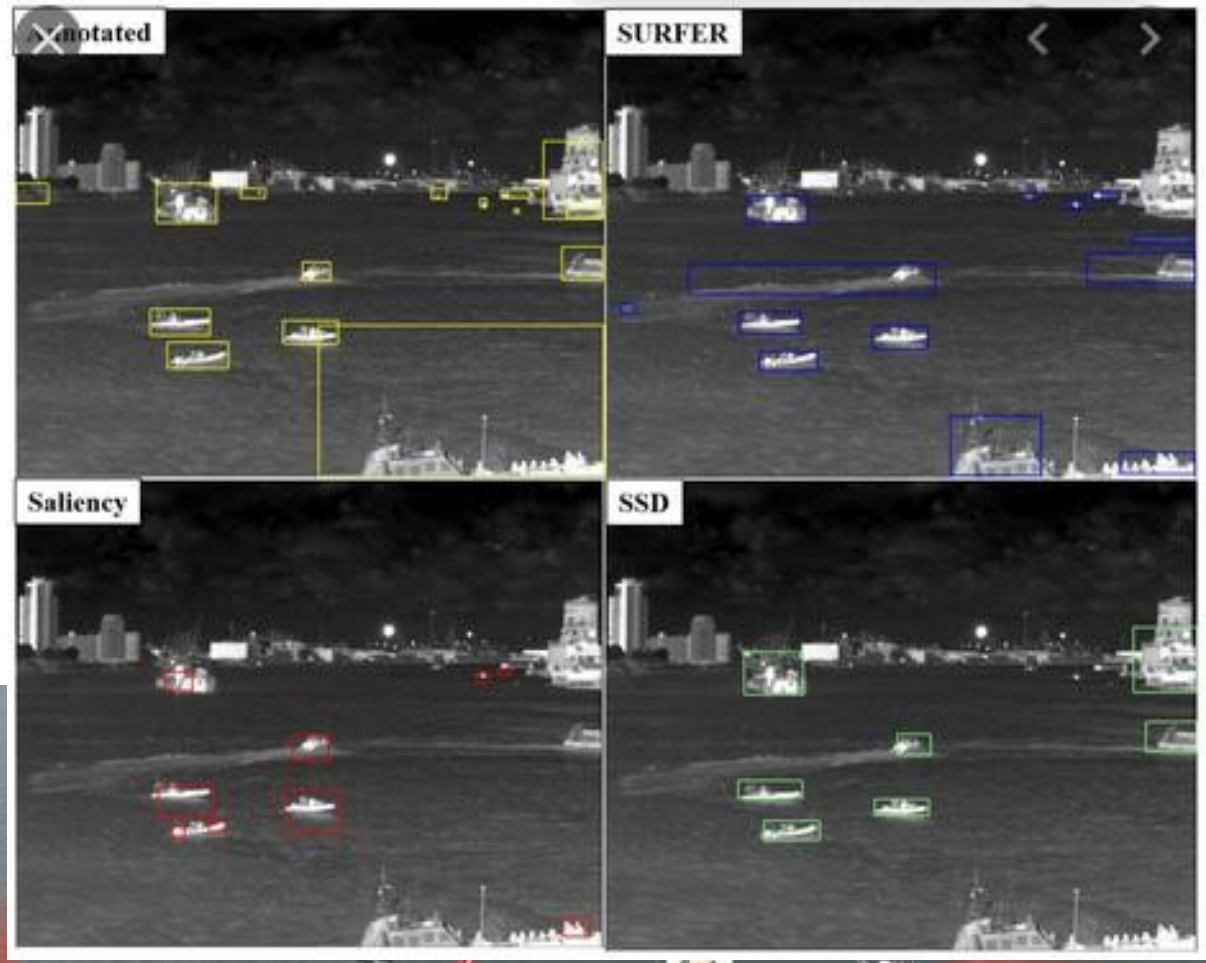
Ορισμός σεναρίων και αλγορίθμων

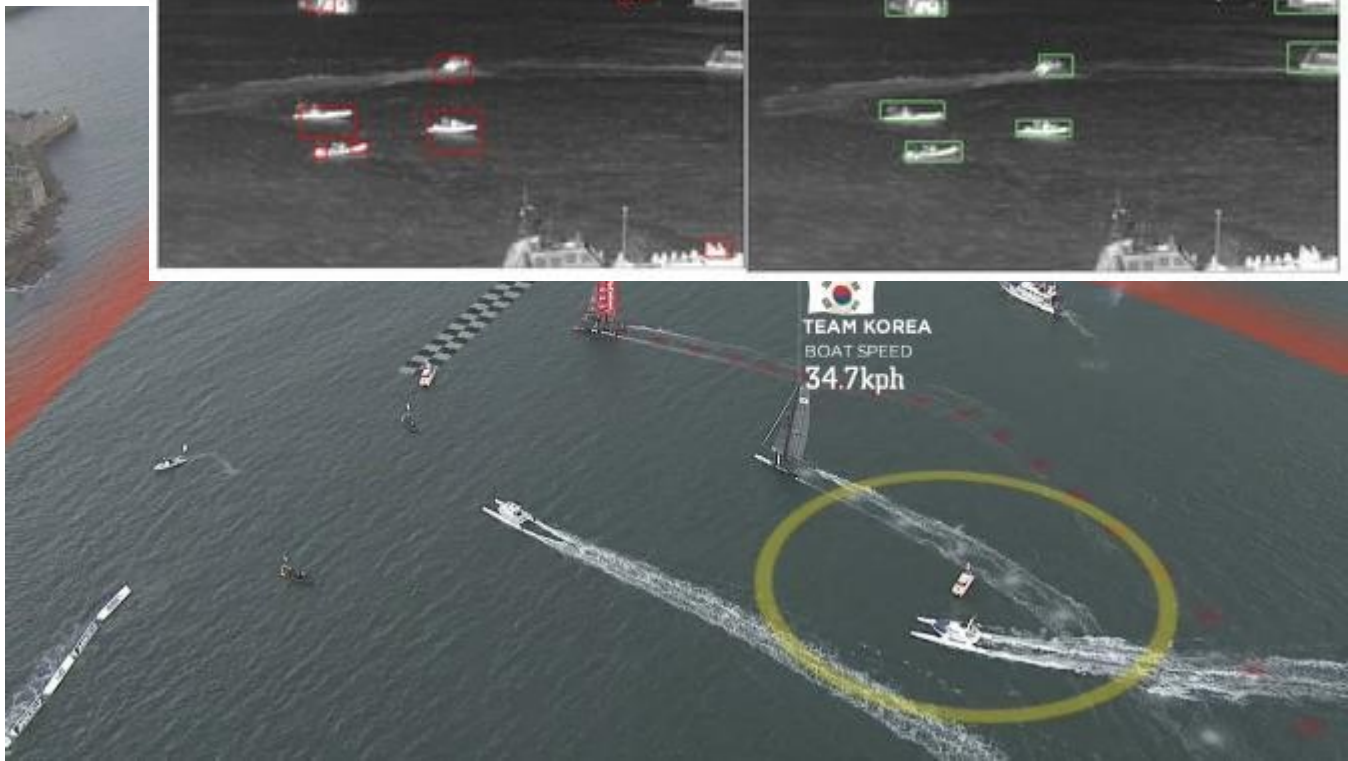
Δημιουργία βάσης δεδομένων Εικόνες αφιερωμένες στη μάθηση μέσω του συστήματος

Στόχος: Εκμάθηση του περιβάλλοντος, των παραγόντων και των συμπεριφορών του


OUDY BAY
97


CHINA TEAM
ETNZ
ARTEMIS
OR SPITHILL
ENERGY TEAM

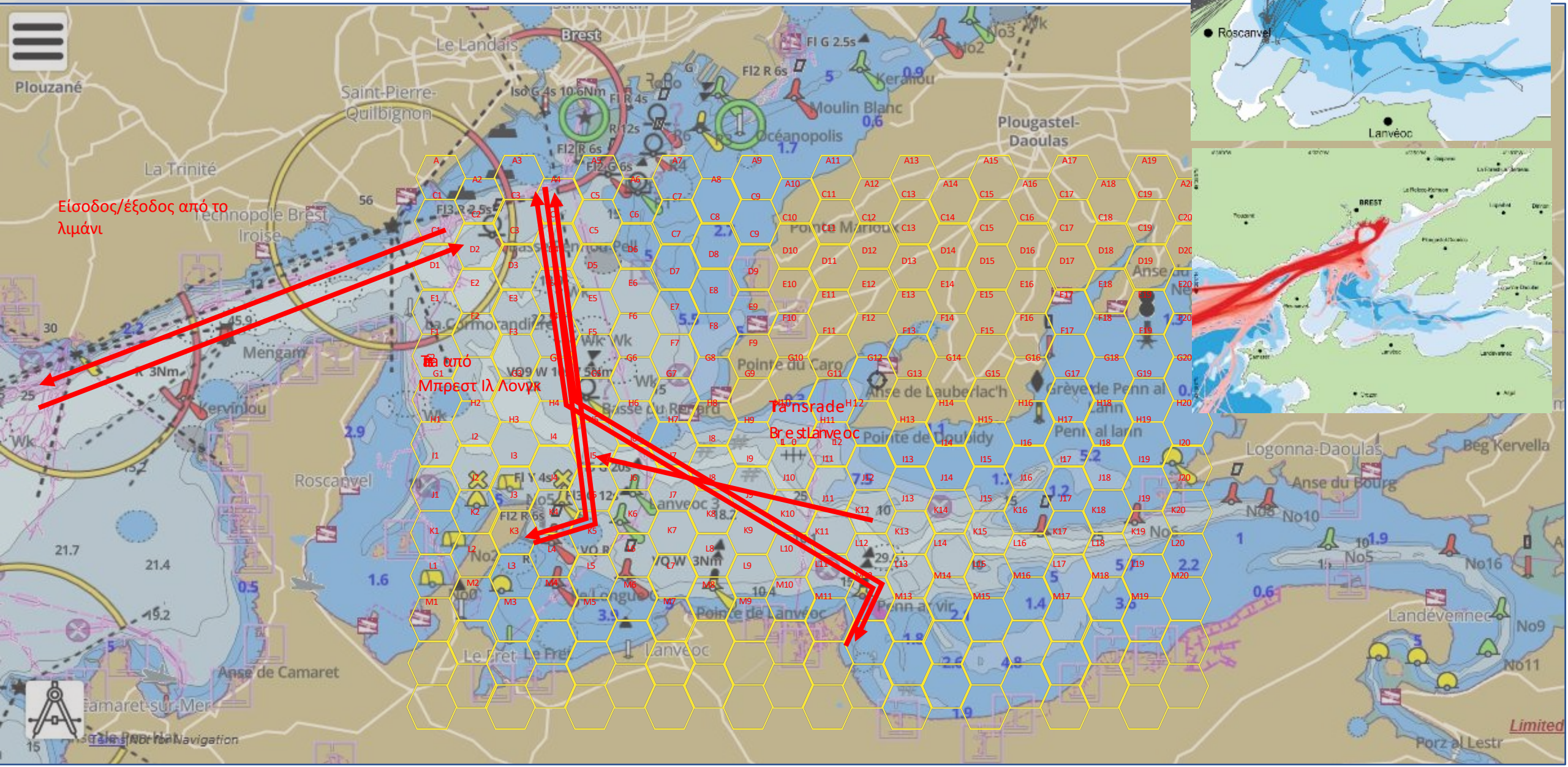

notated
SURFER
Saliency
SSD


TEAM KOREA
BOAT SPEED
34.7kph

Σενάρια

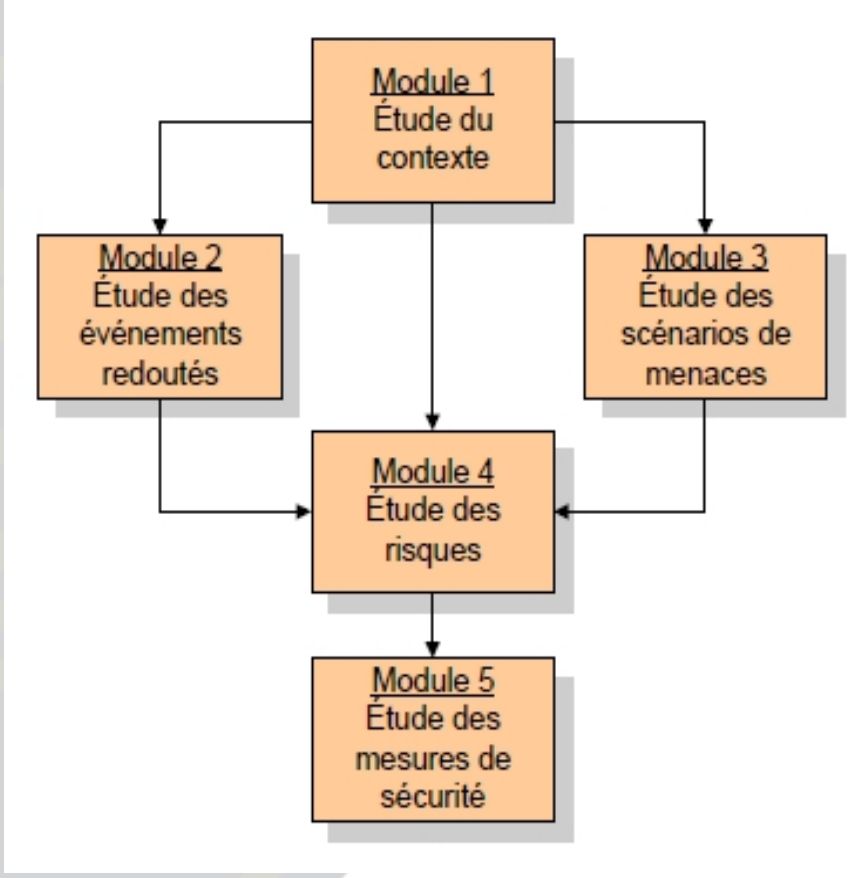
Σενάρια 1 - Μεγάλο βραβείο της Ναυτικής Ακαδημίας

Μοντελοποίηση των συνηθισμένων προτύπων



Μελέτη ασφάλειας (Φάρους ασφαλείας)

Μεθοδολογία



Ενότητα 1 – Μελέτη του πλαισίου

Καθορισμός του πλαισίου διαχείρισης κινδύνων, των μετρήσεων και του πεδίου εφαρμογής της μελέτης. Προσδιορίζονται τα βασικά περιουσιακά στοιχεία, τα υποστηρικτικά περιουσιακά στοιχεία στα οποία βασίζονται και οι παράμετροι που πρέπει να ληφθούν υπόψη κατά την αντιμετώπιση των κινδύνων.

Ενότητα 2 – Μελέτη των ανεπιθύμητων συμβάντων

Αξιολόγηση των κινδύνων. Προσδιορισμός και εκτίμηση των αναγκών ασφάλειας των βασικών περιουσιακών στοιχείων (όσον αφορά τη διαθεσιμότητα, την ακεραιότητα, την εμπιστευτικότητα κ.λπ.), καθώς και όλων των επιπτώσεων (στις αποστολές, στην ασφάλεια των προσώπων, στις οικονομικές και νομικές πτυχές, στην εικόνα, στο περιβάλλον, σε τρίτους και άλλα) σε περίπτωση μη τήρησης των εν λόγω αναγκών και των πηγών απειλών (ανθρώπινες, περιβαλλοντικές, εσωτερικές, εξωτερικές, τυχαίων, σκόπιμων κ.λπ.) που ενδέχεται να τις προκαλέσουν, γεγονός που επιτρέπει τη διατύπωση των φοβερών γεγονότων.

Ενότητα 3 – Μελέτη σεναρίων απειλών

Προσδιορισμός και εκτίμηση των σεναρίων που μπορούν να προκαλέσουν τα φοβερά γεγονότα και, ως εκ τούτου, να συνθέσουν κινδύνους. Για το σκοπό αυτό, μελετώνται οι απειλές που μπορούν να προκαλέσουν οι πηγές απειλών και οι ευπάθειες που μπορούν να εκμεταλλευτούν

Ενότητα 4 – Μελέτη των κινδύνων

Κίνδυνοι που βαρύνουν τον οργανισμό, αντιπαραθέτοντας τα φοβερά γεγονότα με τα σενάρια απειλών. Το κεφάλαιο περιγράφει επίσης τον τρόπο εκτίμησης και αξιολόγησης αυτών των κινδύνων και, τέλος, τον τρόπο προσδιορισμού των στόχων ασφάλειας που πρέπει να επιτευχθούν για την αντιμετώπισή τους.

Ενότητα 5 – Μελέτη των μέτρων ασφαλείας

Αντιμετώπιση κινδύνων. Αυτή η ενότητα εξηγεί πώς να καθορίσετε τα μέτρα ασφαλείας που πρέπει να εφαρμοστούν, πώς να προγραμματίσετε τα μέτρα και πώς να επικυρώσετε την αντιμετώπιση των κινδύνων και των υπολειπόμενων κινδύνων.

Ανάγκη ασφάλειας του συστήματος ENDOUME

Ερώτηση αριθ. 1: Είναι το ENDOUME σημαντικό για την εκπλήρωση των καθηκόντων σας;

1	Όχι, το σύστημα είναι δευτερεύον για την εκπλήρωση των καθηκόντων	Ναι, οι αποστολές θα διαταραχθούν σοβαρά από δυσλειτουργία του πληροφοριακού συστήματος.	Ναι, οι αποστολές εξαρτώνται πλήρως από το πληροφοριακό σύστημα	Δεν ξέρω
		2		

Ερώτηση αριθ. 2: Εάν ένα ατύχημα πλήξει την ENDOUME, προκαλώντας δυσλειτουργία ή απώλεια δεδομένων,

2	Όχι, οι εσωτερικές συνέπειες μιας καταστροφής θα ήταν αμελητέες	Ναι, οι εσωτερικές συνέπειες ενός καταστροφής θα ήταν σημαντικές	Ναι, οι εσωτερικές συνέπειες ενός θα ήταν σοβαρές, voire καταστροφικές	Δεν ξέρω
		1		

Ερώτηση 3: Εάν ένα ατύχημα επηρεάσει την ασφάλεια του ENDOUME (δεν λειτουργεί πλέον ή δεν λειτουργεί σωστά, κλοπή πληροφοριών κ.λπ.), οι συνέπειες για το εξωτερικό περιβάλλον (για τους χρήστες, τους διοικητικούς υπαλλήλους κ.λπ.) θα ήταν σοβαρές;

3	Όχι, οι συνέπειες ενός συμβάντος για το εξωτερικό περιβάλλον θα ήταν αμελητέες	Ναι, οι συνέπειες ενός συμβάντος για το εξωτερικό περιβάλλον θα ήταν σημαντικές	Ναι, οι συνέπειες ενός συμβάντος για το εξωτερικό περιβάλλον θα ήταν σοβαρές, ή ακόμη και καταστροφικές	Δεν ξέρω
		2		

Σοβαρότητα των πιθανών συνεπειών (αναφέρετε εδώ τη μέγιστη τιμή των απαντήσεων στις ερωτήσεις 1 έως 3) **2**

Ερώτηση αριθ. 4: Είναι σοβαρό το γεγονός ότι τα δεδομένα του ENDOUME είναι απρόσιτα; Π.χ.: δεν μπορείτε να έχετε πρόσβαση στα δεδομένα λόγω βλάβης του εξοπλισμού.

4	Όχι, το γεγονός ότι δεν είναι προσβάσιμα δεν εμποδίζει σχεδόν καθόλου τη δραστηριότητα	Ναι, το γεγονός ότι δεν είναι πρόσβαση θα διαταράξει σημαντικά τη δραστηριότητα σημαντικά	Ναι, το γεγονός ότι δεν είναι προσβάσιμο μπορεί να είναι καταστροφικό για την επιχείρηση	Δεν ξέρω
		2		

Ερώτηση αριθ. 5: Είναι σοβαρό το γεγονός ότι τα δεδομένα έχουν αλλοιωθεί; Π.χ.: ένας ιός έχει τροποποιήσει τις τιμές σε μια βάση δεδομένων, επαναφέροντάς τις όλες στο 0.

5	Όχι, το γεγονός ότι τα δεδομένα είναι αλλοιωμένα δεν επηρεάζει σχεδόν καθόλου στη δραστηριότητα	Ναι, το γεγονός ότι τα δεδομένα είναι αλλοιωμένα θα διαταράξει σημαντικά τη δραστηριότητα σημαντικά	Ναι, το γεγονός ότι τα δεδομένα είναι αλλοιωμένα μπορεί να είναι καταστροφικό για στη δραστηριότητα	Δεν ξέρω
		2		

Ερώτηση αριθ. 6: Είναι σοβαρό το γεγονός ότι τα δεδομένα της ENDOUME δεν είναι ή δεν είναι πλέον εμπιστευτικά; Παράδειγμα: η λίστα των δικαιούχων κοινωνικών υπηρεσιών έχει δημοσιοποιηθεί.

6	Όχι, η έλλειψη εμπιστευτικότητας δεν επηρεάζει σχεδόν καθόλου τη δραστηριότητα	Ναι, η έλλειψη εμπιστευτικότητας θα διαταράξει σημαντικά τη δραστηριότητα σημαντικό	Ναι, η έλλειψη εμπιστευτικότητας μπορεί να είναι καταστροφική για τη δραστηριότητα	Δεν ξέρω
		1		

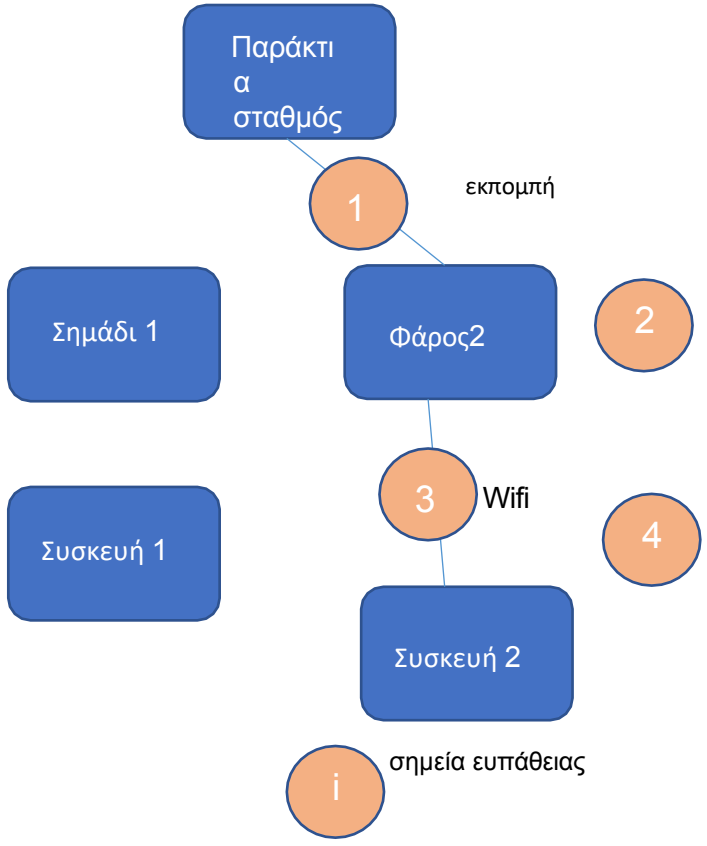
Ευαισθησία των δεδομένων του συστήματος (αναφέρετε εδώ τη μέγιστη τιμή των απαντήσεων στις ερωτήσεις 4 έως 6) **2**

Ενότητα 1 – Μελέτη του πλαισίου

- Το σύστημα αποτελείται από τρεις τύπους οντοτήτων:
    - Μια παράκτια σταθμός (SC)
    - Φάροι
    - Πελάτες / Συσκευές
- Οι αλληλεπιδράσεις μεταξύ αυτών των οντοτήτων:
    - Ανταλλαγές μεταξύ του SC και των φάρων
    - Ανταλλαγές μεταξύ των φάρων και των συσκευών
- Το πλαίσιο διαχείρισης κινδύνων:
    - Η S.C είναι ασφαλής (δεν μπορεί να παραβιαστεί φυσικά)
    - Οι ανταλλαγές μεταξύ της SC και των πομπών γίνονται μέσω εκπομπής, σε «ιδιόκτητες συχνότητες»
    - Οι ανταλλαγές μεταξύ των ραδιοφάρων και των νομισμάτων γίνονται μέσω wifi.
    - Κάθε πομπός διαθέτει μια ιστοσελίδα που εμφανίζει την τακτική κατάσταση (SITAC) που λαμβάνεται από την SC

Ενότητα 2 – Μελέτη των φοβερών γεγονότων

- Μη εξουσιοδοτημένη πρόσβαση στο SITAC **(α)**
- Τροποποίηση της τοποθεσίας **(β)**
- Διάδοση ψευδών sitac / ψευδών μηνυμάτων **(γ)**



Ενότητα 3 – Μελέτη σεναρίων απειλών

Τα σημεία **1** έως **4** στο σχήμα δεξιά αντιπροσωπεύουν τα σημεία ευπάθειας μέσω των οποίων μπορούν να συμβούν τα φοβούμενα γεγονότα.

Σενάρια:

- Κατάληψη του παράκτιου σταθμού (επανάληψη: από άτομο που βρίσκεται κοντά) **(1)** ⇒ **(c)** (και **(β)** έμμεσα)
- Παρεμβολή συχνοτήτων **(1)** ⇒ **(c)** (και **(β)** έμμεσα)
- Κλοπή ενός ραδιοφάρου **(2)** ⇒ **(α)** (και **(β)** έμμεσα)
- Ανεπιθύμητη πρόσβαση κοντά σε έναν πομπό **(3)** ⇒ **(α)**
- Παράνομη σύνδεση μιας συσκευής σε έναν πομπό **(4)** ⇒ **(α)**

⇒ : συνεπάγεται το φοβούμενο συμβάν

Ενότητα 4 Προσδιορισμός απειλών (ανάγκη ασφάλειας του συστήματος)

Ερώτηση αριθ. 1: Είναι το ENDOUME σημαντικό για την εκπλήρωση των καθηκόντων σας;

1	Όχι, το σύστημα είναι δευτερεύον για την εκπλήρωση των αποστολών	Ναι, οι αποστολές θα επηρεάζονταν σημαντικά διαταραχές λόγω δυσλειτουργίας του πληροφοριακού συστήματος.	Ναι, οι αποστολές εξαρτώνται πλήρως από το SI	Δεν ξέρω
		2		

Ερώτηση αριθ. 2: Εάν ένα ατύχημα πλήξει την ENDOUME, προκαλώντας δυσλειτουργία ή απώλεια δεδομένων, 2

Όχι, οι εσωτερικές συνέπειες μιας καταστροφής θα ήταν αμελητέες	Ναι, οι εσωτερικές συνέπειες μιας καταστροφής θα ήταν σημαντικές	Ναι, οι εσωτερικές συνέπειες μιας καταστροφής θα ήταν σοβαρές, ακόμη και θανατηφόρες	Δεν ξέρω
1			

Ερώτηση αριθ. 3: Εάν ένα ατύχημα επηρεάσει την ασφάλεια του ENDOUME (δεν λειτουργεί πλέον ή δεν λειτουργεί σωστά, κλοπή πληροφοριών κλπ.), οι συνέπειες για το εξωτερικό περιβάλλον (για τους χρήστες, τους διοικητικούς υπαλλήλους κ.λπ.) θα ήταν σοβαρές;

3	Όχι, οι συνέπειες ενός ατυχήματος για το εξωτερικό θα ήταν αμελητέες	Ναι, οι συνέπειες ενός ατυχήματος για το εξωτερικό θα ήταν σημαντικές	Ναι, οι συνέπειες ενός ατυχήματος για το εξωτερικό θα ήταν σοβαρές, ακόμη και θανατηφόρες	Δεν ξέρω
		2		

Σοβαρότητα των πιθανών συνεπειών (αναφέρετε εδώ τη μέγιστη τιμή των απαντήσεων στις ερωτήσεις 1 έως 3) **2**

Ερώτηση αριθ. 4: Είναι σοβαρό το γεγονός ότι τα δεδομένα του ENDOUME είναι απρόσιτα; Π.χ.: δεν μπορείτε να έχετε πρόσβαση στα δεδομένα λόγω βλάβης του εξοπλισμού.

4	Όχι, το γεγονός ότι δεν είναι προσβάσιμα δεν επηρεάζει σχεδόν καθόλου τη δραστηριότητα	Ναι, το γεγονός ότι δεν είναι προσβάσιμα θα διαταράξει σημαντικά τη δραστηριότητα σημαντικό	Ναι, το γεγονός ότι δεν είναι είναι προσβάσιμα μπορεί να είναι καταστροφικό για τη δραστηριότητα	Δεν ξέρω
	1			

Ερώτηση αριθ. 5: Είναι σοβαρό το γεγονός ότι τα δεδομένα έχουν αλλοιωθεί; Π.χ.: ένας ιός έχει τροποποιήσει τις τιμές σε μια βάση δεδομένων, επαναφέροντάς τις όλες στο 0.

5	Όχι, το γεγονός ότι τα δεδομένα είναι αλλοιωμένα δεν επηρεάζει σχεδόν καθόλου τη δραστηριότητα	Ναι, το γεγονός ότι τα δεδομένα είναι αλλοιωμένα θα διαταράξει τη δραστηριότητα σημαντικά	Ναι, το γεγονός ότι τα δεδομένα είναι παραποιημένα μπορεί να είναι καταστροφικό για τη δραστηριότητα	Δεν ξέρω
		2		

Ερώτηση αριθ. 6: Είναι σοβαρό το γεγονός ότι τα δεδομένα της ENDOUME δεν είναι ή δεν είναι πλέον εμπιστευτικά; Παράδειγμα: η λίστα των δικαιούχων της κοινωνικής υπηρεσίας αποκαλύπτεται.

6	Όχι, η έλλειψη εμπιστευτικότητας δεν επηρεάζει σχεδόν καθόλου τη δραστηριότητα	Ναι, η έλλειψη εμπιστευτικότητας θα διαταράξει σημαντικά τη δραστηριότητα σημαντικό	Ναι, η έλλειψη εμπιστευτικότητας μπορεί να είναι καταστροφική για τη δραστηριότητα	Δεν ξέρω
	1			

Ευαισθησία των δεδομένων του συστήματος (αναφέρετε εδώ τη μέγιστη τιμή των απαντήσεων στις ερωτήσεις 4 έως 6) **2**

Ερώτηση αριθ. 7: Ποιο είναι το μέγιστο επίπεδο ικανότητας που μπορεί να έχει ο εισβολέας ή η ομάδα εισβολέων που ενδέχεται να βλάψουν το σύστημα;

7	Μεμονωμένο άτομο με βασικό επίπεδο ικανότητας	Απομονωμένο άτομο με προχωρημένο επίπεδο δεξιοτήτων	Ομάδα οργανωμένων ατόμων, με χαμηλό έως μέτριο επίπεδο δεξιοτήτων, ή μεμονωμένο άτομο με εξειδικευμένες δεξιότητες	Ομάδα οργανωμένων ατόμων με σχεδόν απεριόριστους πόρους
				1

Ερώτηση αριθ. 8: Πόσο ακριβείς είναι οι πιθανές επιθέσεις κατά του πληροφοριακού συστήματος;

8	«Τυχαίες» επιθέσεις στον κυβερνοχώρο	Επιθέσεις που στοχεύουν την ευρωπαϊκή ήπειρο ή τη Γαλλία	Επιθέσεις που στοχεύουν μια ομάδα θυμάτων με κοινά χαρακτηριστικά κοινά χαρακτηριστικά	Επιθέσεις που στοχεύουν συγκεκριμένα το σύστημα
				1

Ερώτηση αριθ. 9: Ποιο είναι το επίπεδο πολυπλοκότητας των πιθανών επιθέσεων κατά του πληροφοριακού συστήματος;

9	Απλά εργαλεία επίθεσης (λογισμικό σάρωσης θυρών, γνωστοί ιοί κ.λπ.)	Εξελιγμένα γενικά εργαλεία έτοιμα χρήσης (μισθωμένα δίκτυα botnet, γνωστές ευπάθειες κενά ασφαλείας κ.λπ.)	Εξελιγμένα εργαλεία, προσαρμοσμένα για το SI (zero-day κ.λπ.)	Πολύ εξελιγμένη εργαλειοθήκη.
				1

Ερώτηση αριθ. 10: Ποια είναι η ορατότητα των πιθανών επιθέσεων κατά του πληροφοριακού συστήματος;

10	Ανακοινωμένη επίθεση (αξιώσεις «χακτιβιστών», λύτρα κ.λπ.)	Επίθεση που διαπιστώνεται αμέσως από τις επιπτώσεις της στο πληροφοριακό σύστημα	Διακριτική επίθεση, που αφήνει ίχνη στα αρχεία καταγραφής συμβάντων, αλλά δεν διαταράσσει τη λειτουργία του πληροφοριακού συστήματος	Αόρατη επίθεση, που πραγματοποιείται αφήνοντας ελάχιστα ίχνη
				1

Ερώτηση αριθ. 11: Ποια είναι η συχνότητα και η διάρκεια των πιθανών επιθέσεων κατά του πληροφοριακού συστήματος;

11	Μόνιμη.	Επαναλαμβανόμενη: επίθεση με διαδοχικές σημαντικές κυμάτων	Σποραδικές: η επίθεση συμβαίνει πολλές φορές χωρίς τακτική συχνότητα (μπορεί να σχετίζεται με την επικαιρότητα).	Μοναδική: η επίθεση πραγματοποιείται στο στόχο μόνο μία μία φορά
				1

Βάση εκτίμησης του δυναμικού των κυβερνοεπιθέσεων (αναφέρετε εδώ τη μέγιστη τιμή των απαντήσεων στις ερωτήσεις 7 έως 11)

1

Ερώτηση αριθ. 12: Ποιο είναι το επίπεδο ετερογένειας του συστήματος; Παράδειγμα: διάφορα λογισμικά, υλικά ή δίκτυα για το ίδιο σύστημα.

12	Το σύστημα θεωρείται ομοιογενές	Το σύστημα θεωρείται ελαφρώς ετερογενές	Το σύστημα θεωρείται ως έντονα ετερογενές	Δεν ξέρω
		2		

Ερώτηση αριθ. 13: Ποιος είναι ο βαθμός ανοιχτότητας/διασύνδεσης του συστήματος; Παράδειγμα: Διαδίκτυο, άλλο εσωτερικό ή εξωτερικό σύστημα (από πάροχο, άλλη διοικητικής αρχής κ.λπ.)

13	Το πληροφοριακό σύστημα δεν είναι ανοιχτό	Το πληροφοριακό σύστημα είναι ανοιχτό μόνο σε ελεγχόμενα εσωτερικά συστήματα	Το σύστημα είναι ανοιχτό σε εσωτερικά που δεν ελέγχονται ή σε εξωτερικά συστήματα	Δεν γνωρίζω
		2		

Ερώτηση αριθ. 14: Το περιβάλλον στο οποίο λειτουργεί το πληροφοριακό σύστημα και τα συστατικά του στοιχεία (υλικό, λογισμικό, δίκτυα) εξελίσσεται τακτικά;

14	Το πληροφοριακό σύστημα και το περιβάλλον του θεωρούνται σταθερά	Το πληροφοριακό σύστημα και το περιβάλλον του αλλάζουν συχνά	Το πληροφοριακό σύστημα και το περιβάλλον του εξελίσσονται συνεχώς	Δεν ξέρω
		2		

Ερώτηση αριθ. 15: Τα στοιχεία του πληροφοριακού συστήματος ενημερώνονται τακτικά;

15	Όλα τα στοιχεία του πληροφοριακού συστήματος ενημερώνονται συνεχώς	Μέρος των στοιχείων του πληροφοριακού συστήματος ενημερώνεται τακτικά	Οι ενημερώσεις γίνονται σε ακανόνιστα χρονικά διαστήματα	Δεν γνωρίζω
		2		

Έκθεση και ευπάθειες (αναφέρετε εδώ τη μέγιστη τιμή των απαντήσεων στις ερωτήσεις 12 έως 15)

Σύνολο:	**2**
	7

Άθροισμα των τεσσάρων τιμών	Ανάγκη ασφάλειας του συστήματος
Από 4 έως 6	1 - Χαμηλή
Από 7 έως 9	2 - Μέτρια
Από 10 έως 16	3 - Υψηλό

Ενότητα 5 – Μελέτη των μέτρων ασφαλείας

- Ασφάλεια του σημείου **(1)**:

  - Κρυπτογράφηση των ανταλλαγών με AES 128 bit · ένα κοινό κλειδί για όλους τους πομπούς και το SC
  - Η ανταλλαγή και η διαχείριση αυτού του κλειδιού θα γίνεται με ένα σύστημα κρυπτογράφησης με δημόσιο κλειδί (RSA 3072 bits). Για το σκοπό αυτό, κάθε πομπός θα έχει το δημόσιο κλειδί του αποθηκευμένο στην SC.
  - Ο κωδικός AES πρέπει να ανανεώνεται σε κάθε ανάπτυξη του συστήματος. Μπορεί επίσης να ανανεώνεται περιοδικά (π.χ. κάθε μέρα).
  - Μέτρα κατά της υποκλοπής SC (επανάληψη) που πρέπει να εξεταστούν ξεχωριστά.

- Ασφάλεια του σημείου **(2)**:

  - Σε περίπτωση κλοπής ενός πομπού (υποτιθέμενη κλοπή που μπορεί να ανιχνευθεί αποτελεσματικά), η SC ενεργοποιεί τη διαδικασία ανανέωσης του κλειδιού AES με τους πομπούς που δεν έχουν παραβιαστεί.

- Ασφάλεια του σημείου **(3)**:

  - Μια συσκευή συνδέεται μέσω Wi-Fi, μέσω ενός προγράμματος περιήγησης ιστού, στον διακομιστή ενός πομπού για να λάβει το SITAC. Αυτή η σύνδεση θα προστατεύεται με το πρωτόκολλο HTTPS (ή WSS).

Ενότητα 5 – Μελέτη των μέτρων ασφαλείας (συνέχεια)

Ασφάλεια του σημείου **(4)**:

- **Μετά** την ασφάλεια του σημείου **(3)**, ο στόχος εδώ είναι να διασφαλιστεί ότι η συσκευή έχει το δικαίωμα πρόσβασης στο SITAC. Υπάρχουν διάφορες πιθανές επιλογές.
- Λύση με κωδικό PIN / ετικέτα:
  - Θεωρούμε μια συνάρτηση κατακερματισμού H (SHA-256 για παράδειγμα)
  - Για κάθε ετικέτα *bi:*
    - δημιουργούμε έναν κωδικό PIN ***pi*** και επιλέγουμε ένα κείμενο *ti.*
    - υπολογίζουμε: *hi* = H(*ti, rand_seed*), *ki* = Epsilon(*pi*) = H(*pi, no_seed*) και *ci* = **ENC_AES_256**(*ki*, *hi*)
    - αποθηκεύουμε στο *bi* το ζεύγος **(*hi*, *ci*)**

- Αυθεντικοποίηση του κωδικού στη *βιομετρική* ετικέτα για πρόσβαση στο sitac: (μετά την εξασφάλιση του σημείου **(3)**)
  - *bi* στέλνει ***ci*** στο *d*
  - *d* υπολογίζει: *ki* = Epsilon(***pi***) = H(***pi***, *no_seed*), στη συνέχεια *m* = ***DEC_AES_256****(ki, hi)* και στέλνει *m* στο *bi*
  - *Το bi* ελέγχει αν *m* = ***hi***. Αν ναι, η πιστοποίηση είναι έγκυρη. Αν όχι, επαναλαμβάνεται.
  - Θα επιτρέπονται έως 5 (?) προσπάθειες στο devise, μετά θα γίνεται μπλοκάρισμα.
- Κάθε κωδικός PIN ***pi*** πρέπει να ανανεώνεται σε κάθε ανάπτυξη του συστήματος και επίσης περιοδικά (για παράδειγμα, κάθε μέρα). Επίσης, κάθε ζεύγος ***(hi, ci)*** σε κάθε μία από τις ετικέτες.

ΕΡΩΤΗΣΕΙΣ;