Definizioni dei concetti di sicurezza e protezione

UE7- A2 Sicurezza informatica: una visione condivisa tra utenti, progettisti di apparecchiature, reti di trasmissione, servizi di gestione dei dati

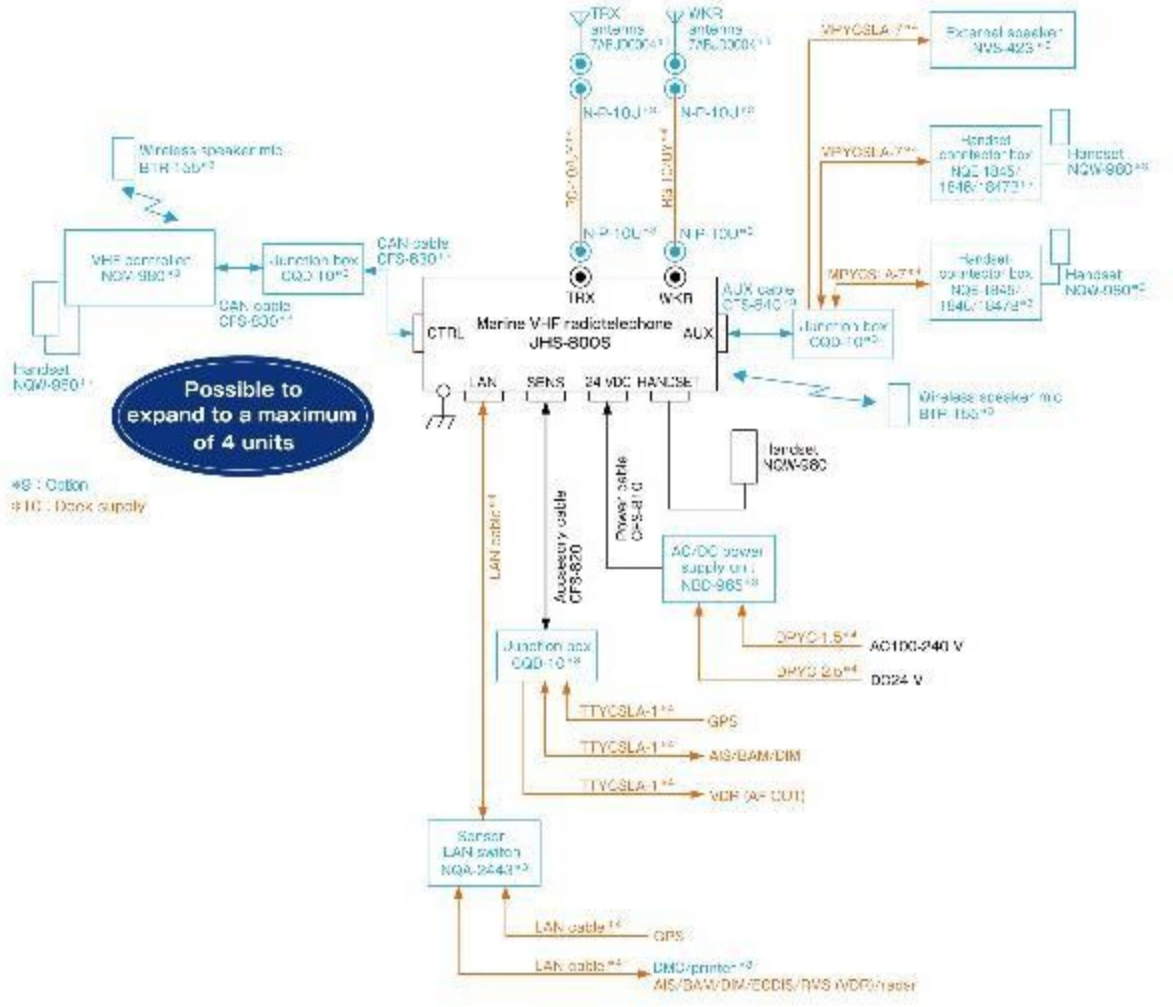
Esempio: AIS / GNSS / ECDIS

Sistemi VMS / Navigazione AIS / GNSS / ECDIS

S 10					
UE 7 - Attuare una politica di sicurezza informatica efficace		**BC 3**	**45**	*6*	**6**
UE7-A - Definizioni dei concetti di sicurezza e protezione			**15**	**2**	**2**
UE7-A-1	Sicurezza e protezione, due ambiti distinti ma di pari importanza				
UE7-A-2	Cybersecurity: una visione condivisa tra utenti, progettisti di apparecchiature, reti di trasmissione, servizi di gestione dati *Esempio: AIS / GNSS / ECDIS*				
UE7-C - Garantire la sicurezza dai rischi legati agli attacchi informatici			**15**	*2*	**2**
UE7-C-1	Identificare i settori funzionali, mapparli e garantirne l' interoperabilità sicura - Esigenze, constatazioni, analisi				
UE7-C-2	Assicurazione per coprire i costi causati dagli attacchi informatici ai sistemi informativi				
UE7-D - Organizzare i processi per garantire la sicurezza informatica dell'azienda e del suo ambiente			**15**	*2*	**2**
UE7-D-1	Le fasi dell'azione: anticipare e monitorare, reagire e combattere, ripristinare				
UE7-D-2	Gestire la comunicazione interna ed esterna verso i collaboratori, i fornitori, i clienti				

SISTEMA DI IDENTIFICAZIONE AUTOMATICA

Cos'è l'AIS?



JRC – E/R VHF Marine JHS-800S
Con funzione ASN

AIS / GNSS – Utenti / Usi

Attori pubblici

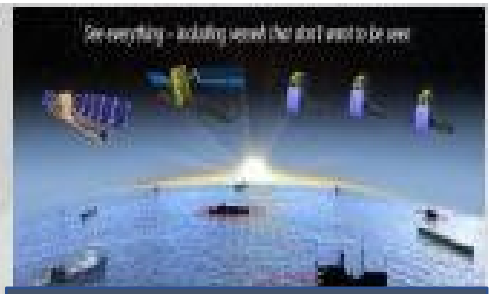
Attori pubblici

Attori privati

Attori privati

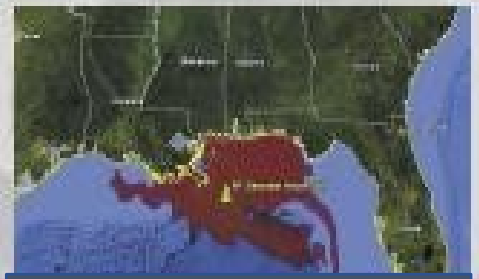
Sorveglianza e sicurezza

SAR



Informazioni

Contro la pirateria



Monitoraggio ambientale

Indagini

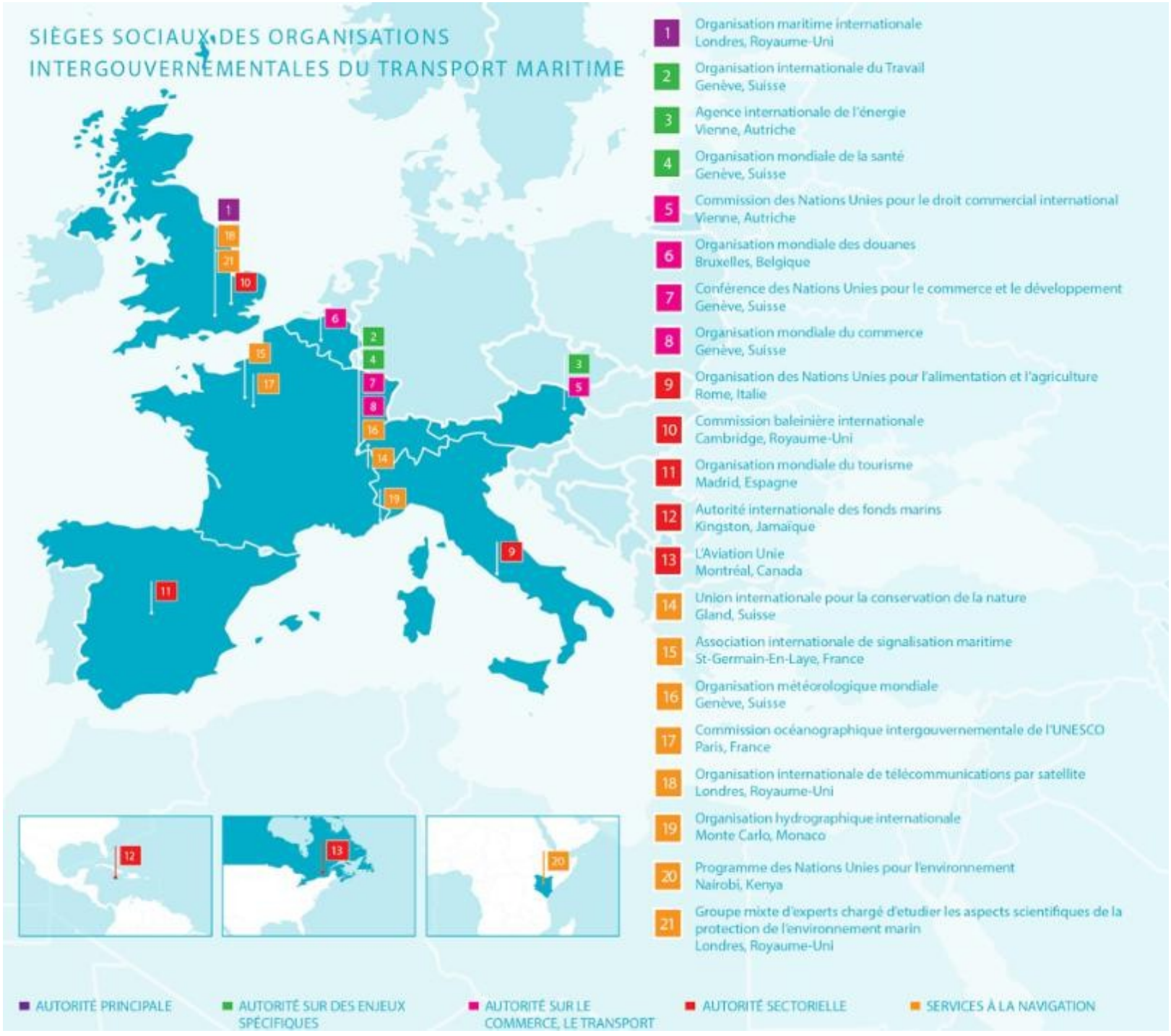
Monitoraggio logistico

Monitoraggio petrolio / gas

Monitoraggio della pesca

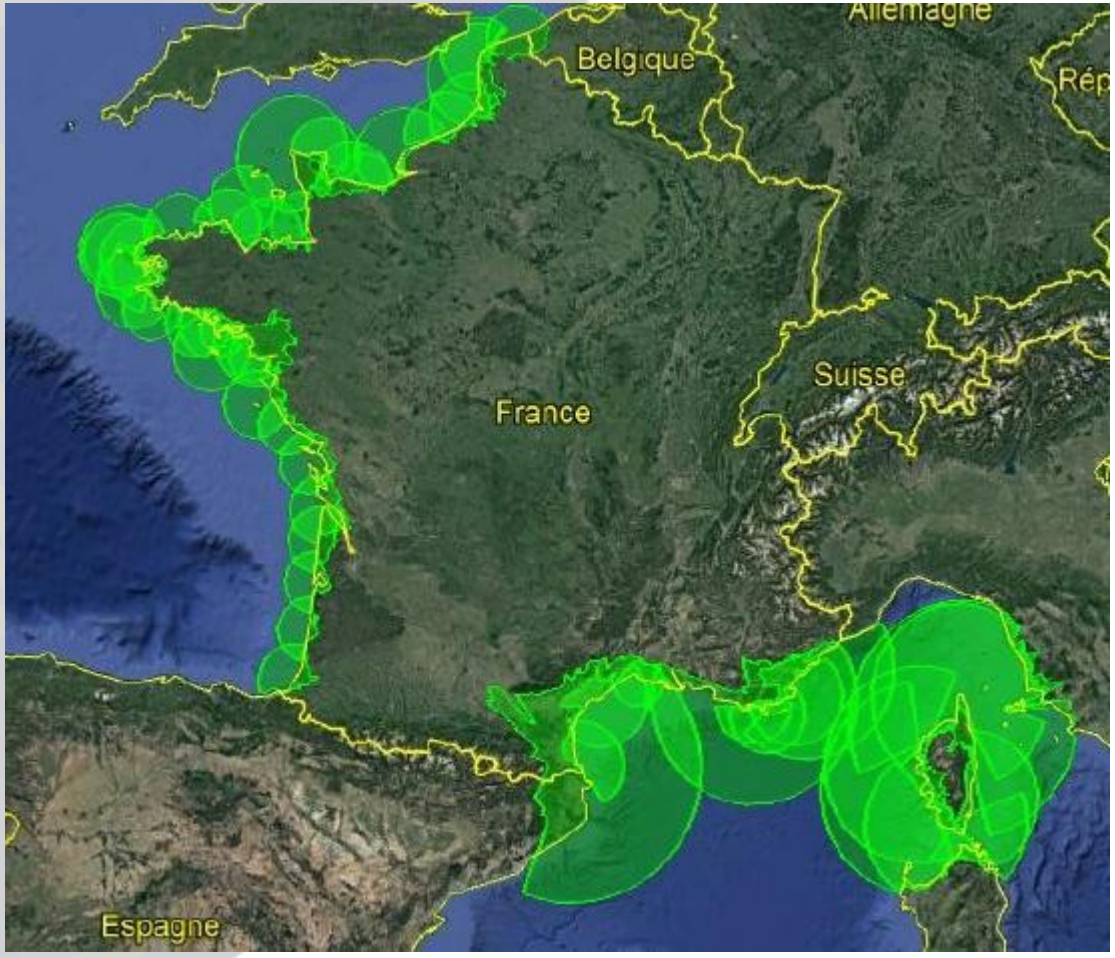
Governance marittima

(promemoria)

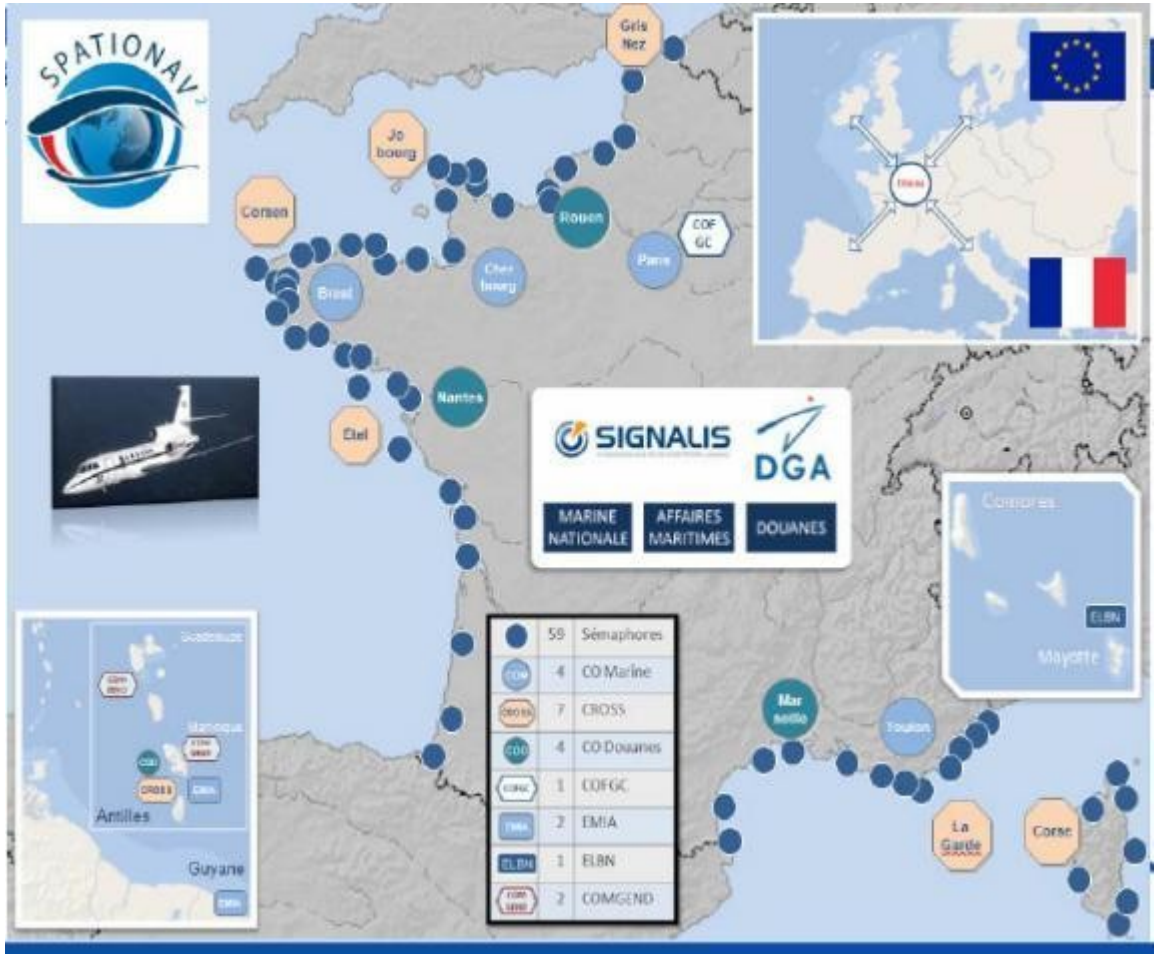


AIS / GNSS – Organizzazione nazionale

Rete AIS costiera "civile" in Francia (40 siti)



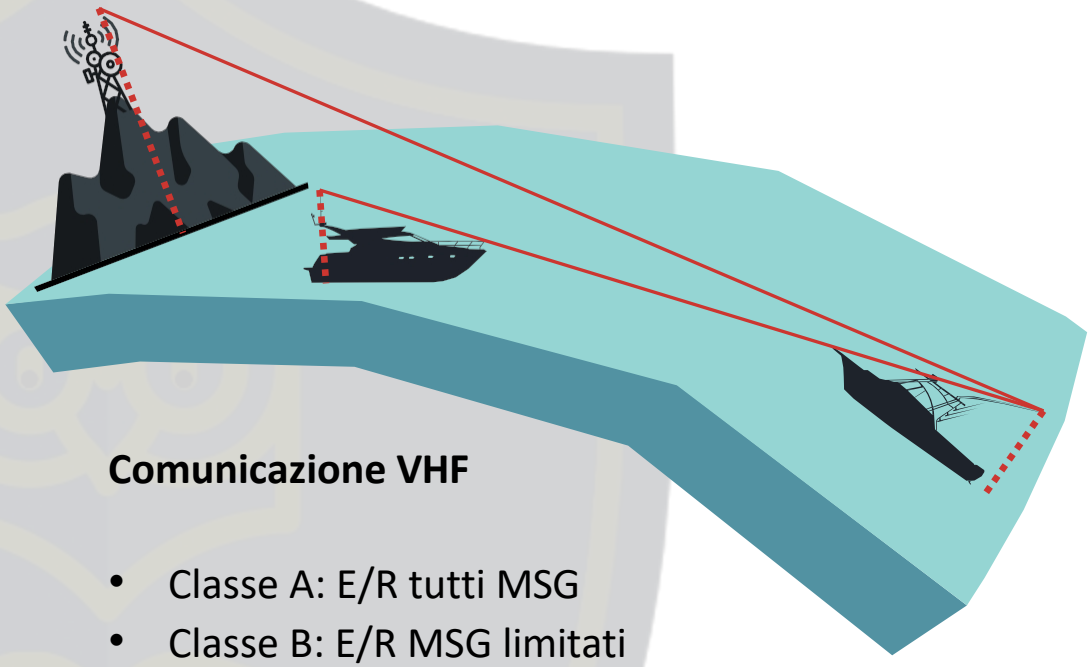
Rete AIS / Radar costiera «militare» (130 siti)



Funzionamento dell'AIS

- Principi
- Messaggi
- Obblighi legali
- Punti di forza e di debolezza
- AIS e rischio informatico
- Caso di studio

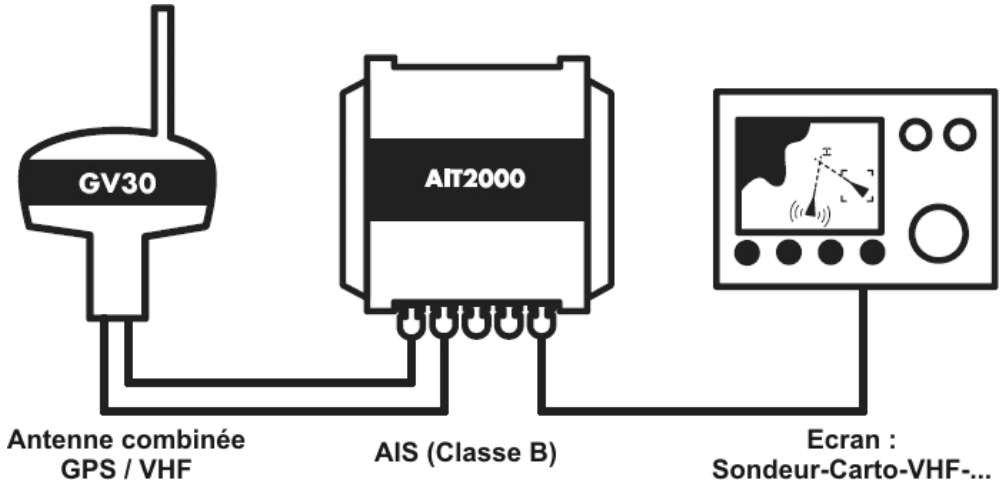
AIS / GNSS – Funzionamento del sistema di comunicazione



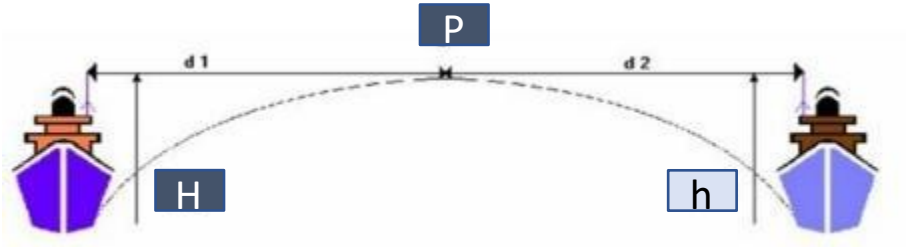
Comunicazione VHF

- Classe A: E/R tutti MSG
- Classe B: E/R MSG limitati

Transponder AIS



La formula della portata ottica / radar



Portata ottica (Nq) = 2,2 ($\sqrt{H(ft)}$ + $\sqrt{h\,(ft\,)}$)

Esempio:

1 / A che distanza posso vedere una nave in mare alta 20 m se mi trovo su una torre alta 100 m? 2/ A che distanza posso vedere una nave in mare alta 20 m se mi trovo sulla spiaggia?

1/ 102 km

2/ 34 km

1 ft = 0,305 m

AIS / GNSS – Interconnessione con il sistema ECDIS

Antenna GPS

AntennaVHF

Interfaccia utente
(ECS o ECDIS)

Transponder
AIS

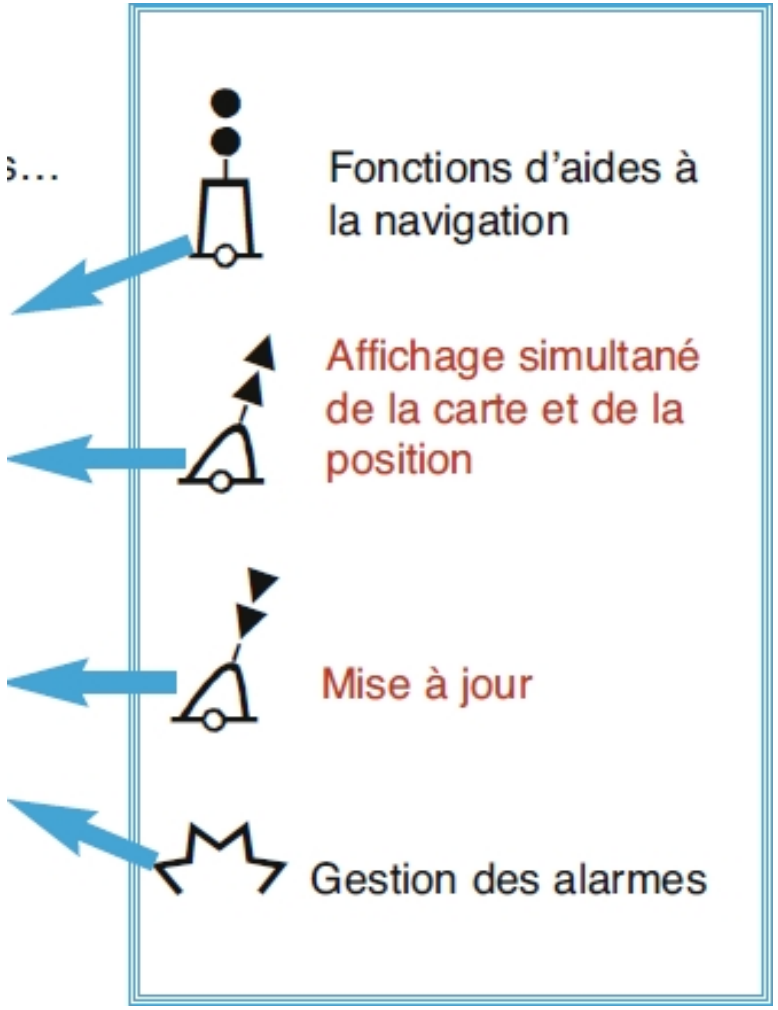
Interfaccia pilota

Loch

CCV (Bussola)

GPS

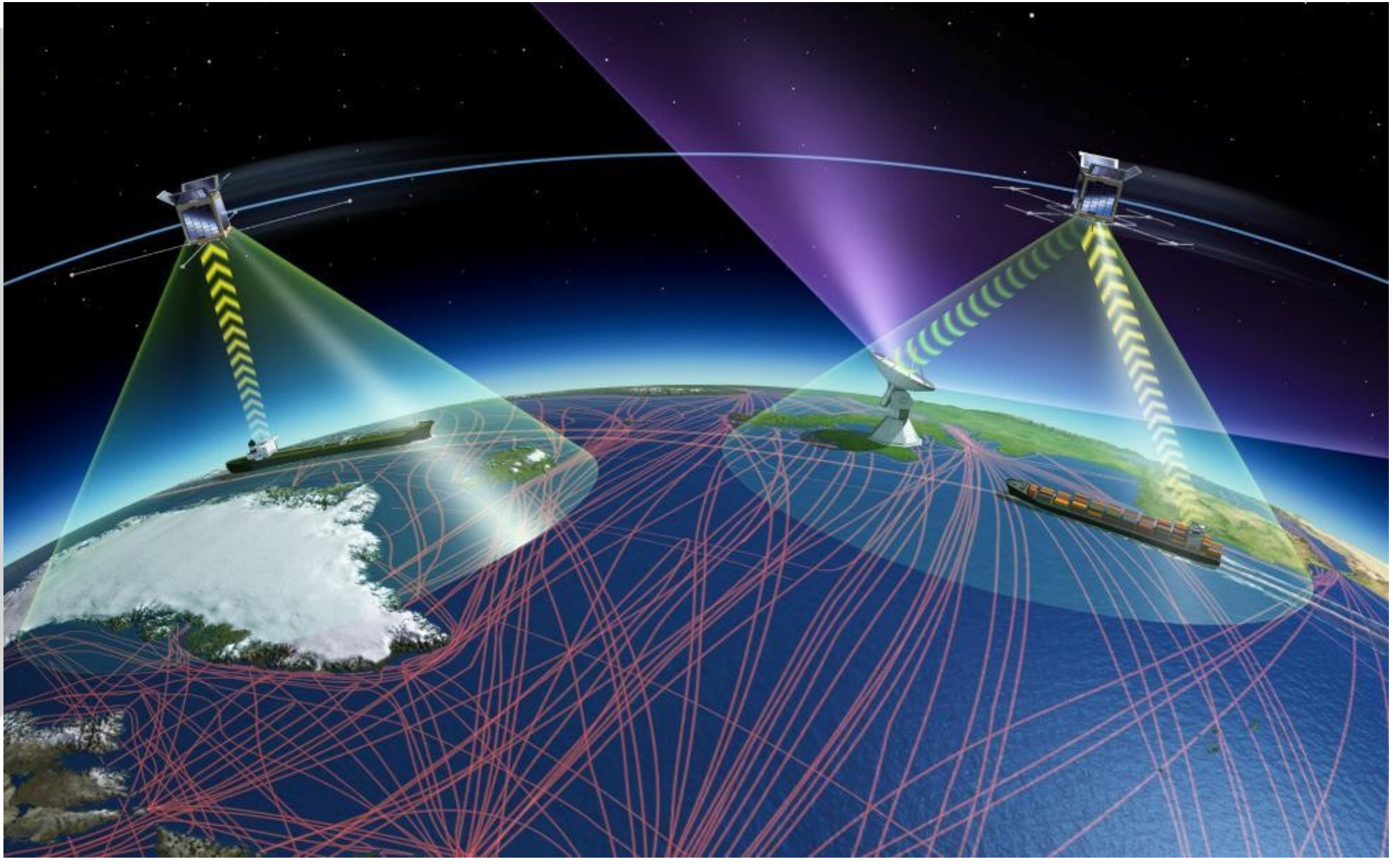
Alimentazione



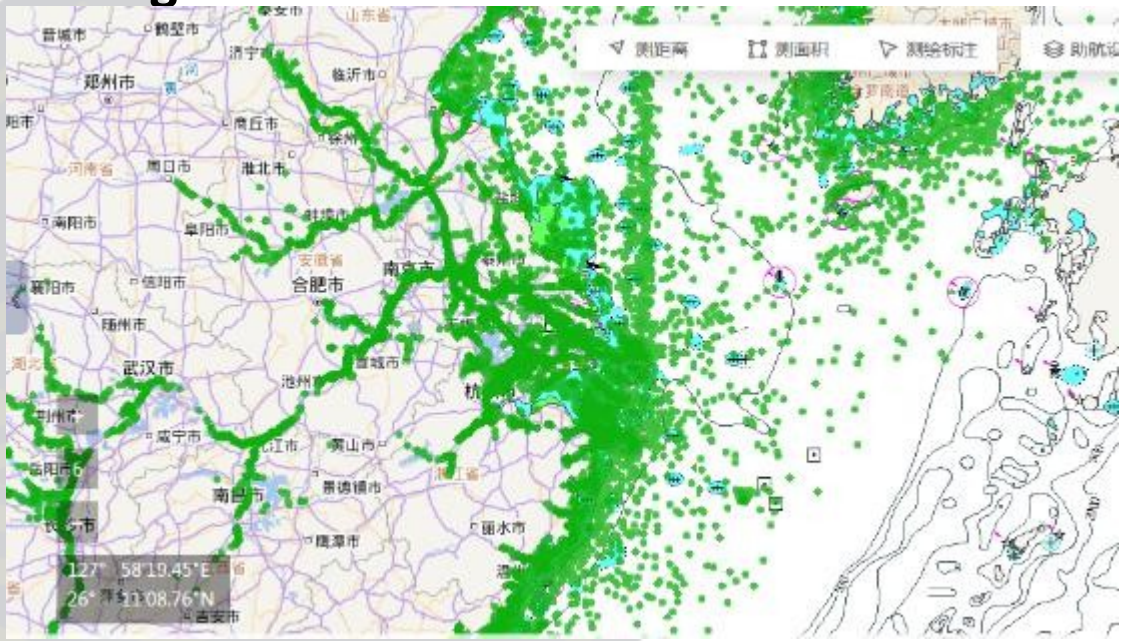
Informazioni trasmesse dall'AIS

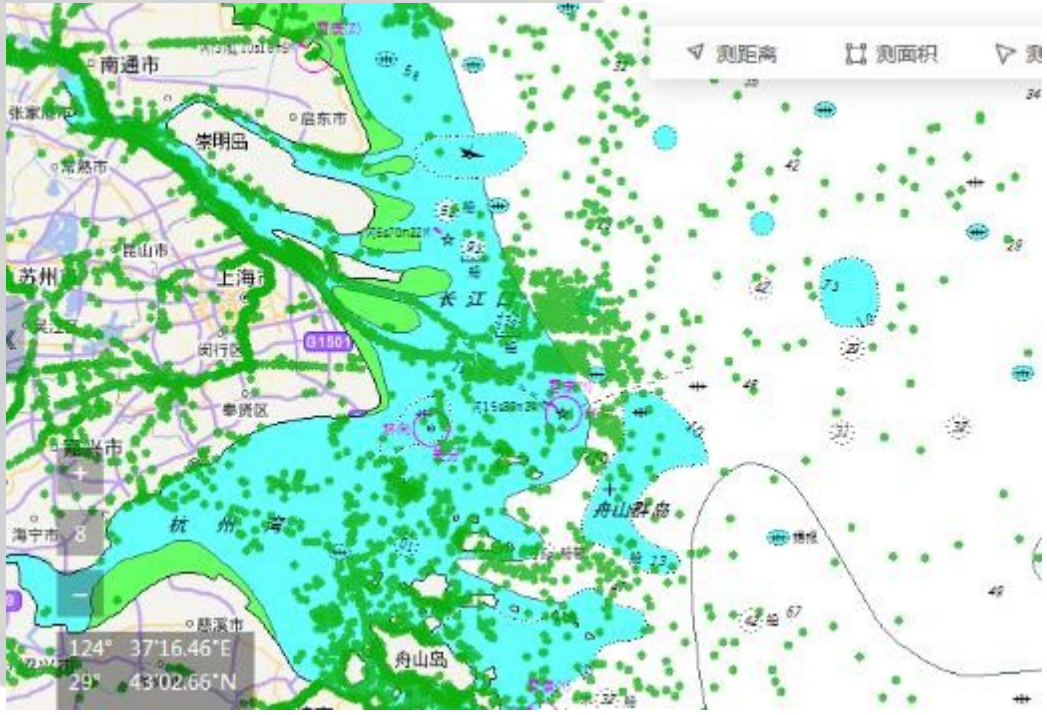
Static information	Dynamic information	Voyage related information
Every 6 minutes and on request by a competent authority	*Dependent on speed and course alteration*	*Every 6 minutes, when data is amended or on request*
MMSI (Maritime Mobile Service Identity)	**Ship's position**	**Ship's draught**
Call 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)	

Raccolta dei dati AIS via satellite

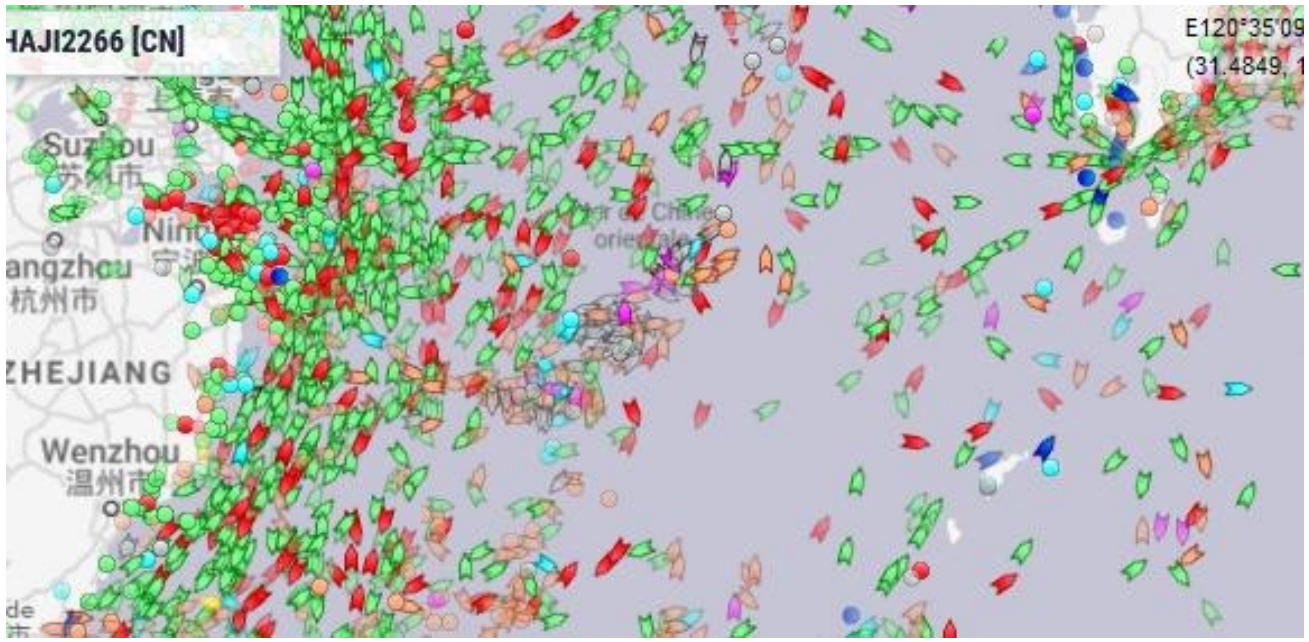


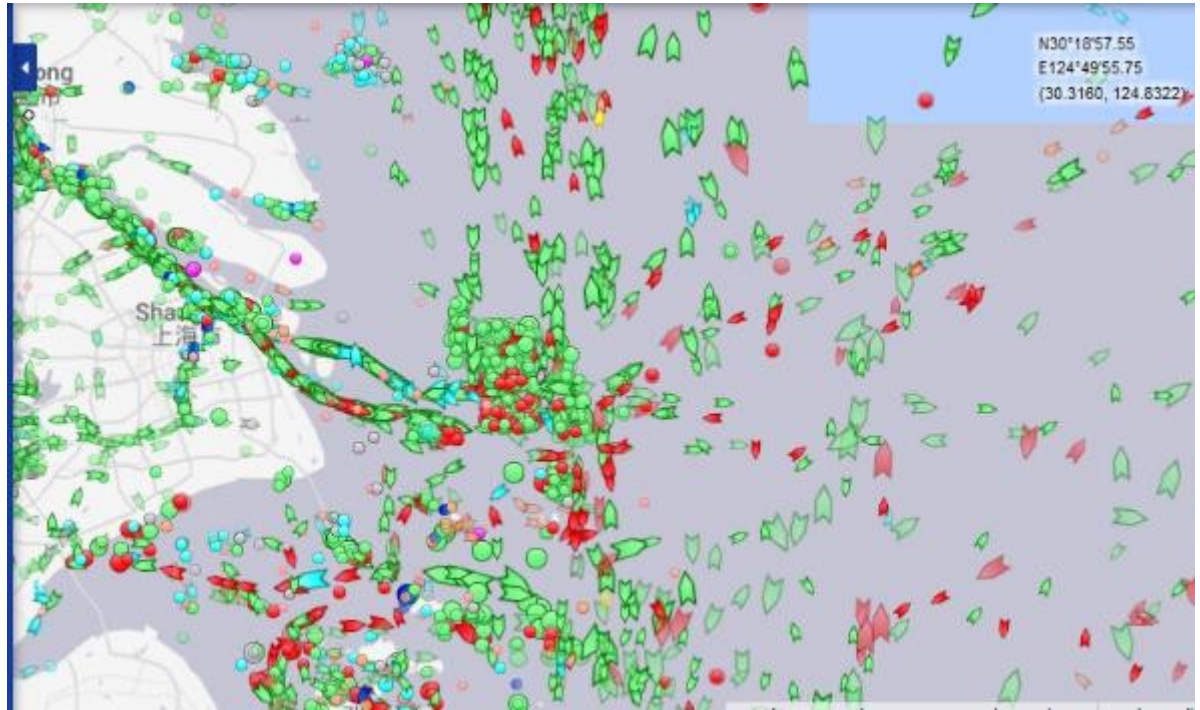
CartografiaAIS





Marinetraffic.com (satelliti)





AIS e CYBER

- Tipi di attacchi
- Interferenza
- Spoofing / Usurpazione
- Rimedi
- Esempio

Tipo di attacchi

Usurpazione di identità – I messaggi AIS trasmessi forniscono informazioni sull'identità delle navi, sulle posizioni passate, presenti e future e sul carico. L'usurpazione della posizione di una nave può causare incidenti o persino collisioni.

Usurpazione dell'ausilio alla navigazione – Informazioni false sull'ausilio alla navigazione, come un segnale che avverte della presenza di secche, possono costringere una nave a modificare la propria rotta. Ciò può essere fatto per costringere una nave ad entrare in una zona dove può essere dirottata.

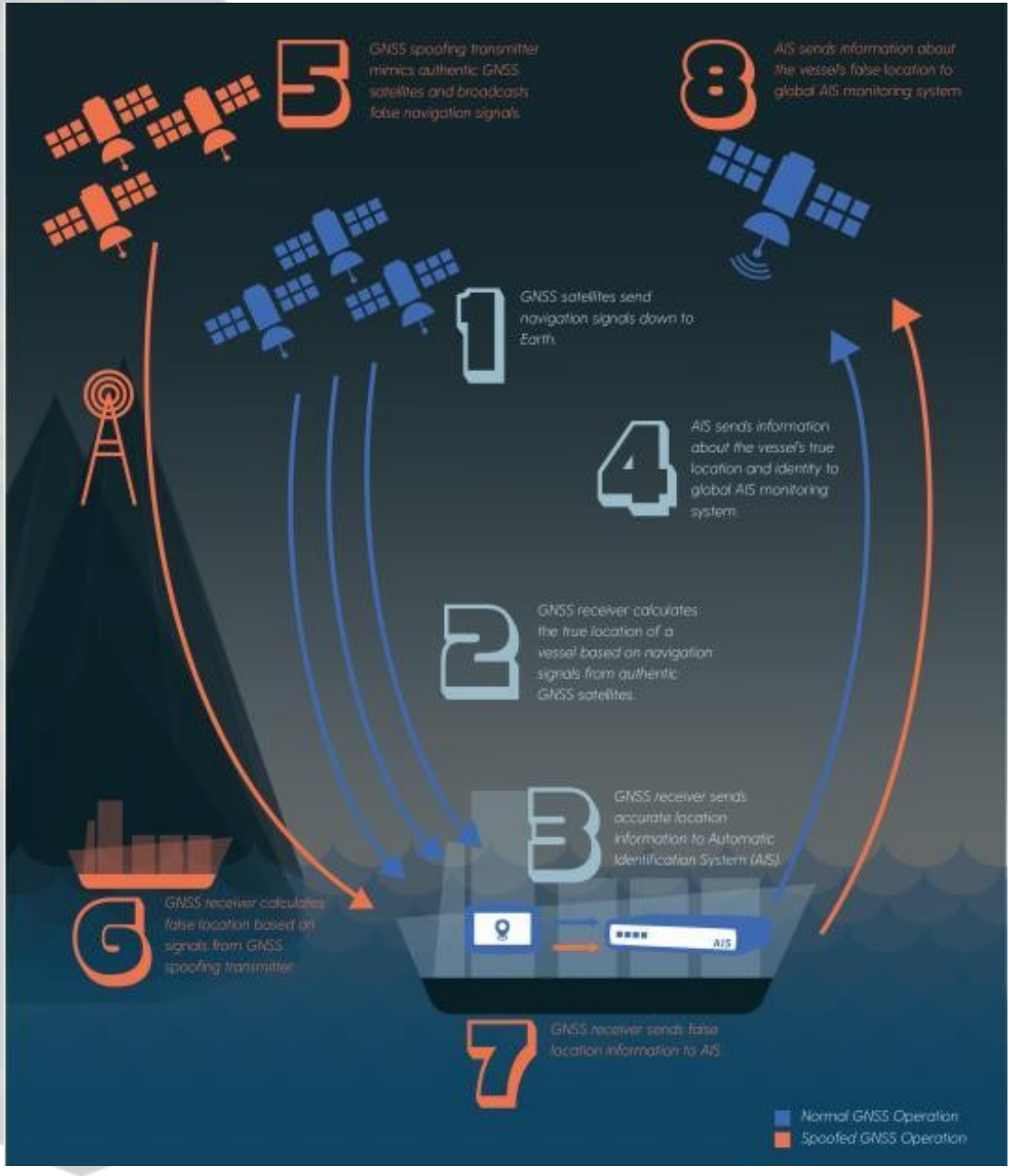
Usurpazione/collisione – La prevenzione delle collisioni è uno degli usi principali dell'AIS. Fornendo dettagli usurpati di una nave su una traiettoria di collisione, un aggressore può costringere una nave a cambiare rotta per evitare la collisione. Ciò potrebbe, ad esempio, essere utilizzato per dirigere la nave verso un incagliamento.

Usurpazione AIS-SART – La ricerca e il soccorso sono un altro utilizzo dell'AIS. Questo attacco genera un falso segnale SART (Transponder di ricerca e soccorso), che segnala una situazione di emergenza. Le navi che ricevono il segnale SART sono tenute per legge a prestare soccorso, quindi la spoofing SART può essere utilizzata per attirare le navi in un luogo dove possono essere attaccate.

Usurpazione delle previsioni meteorologiche – L'AIS può essere utilizzato per trasmettere informazioni sulle condizioni meteorologiche. Una previsione falsa, in particolare quella che prevede condizioni favorevoli quando è in arrivo una tempesta, potrebbe essere utilizzata per mettere in difficoltà una nave.

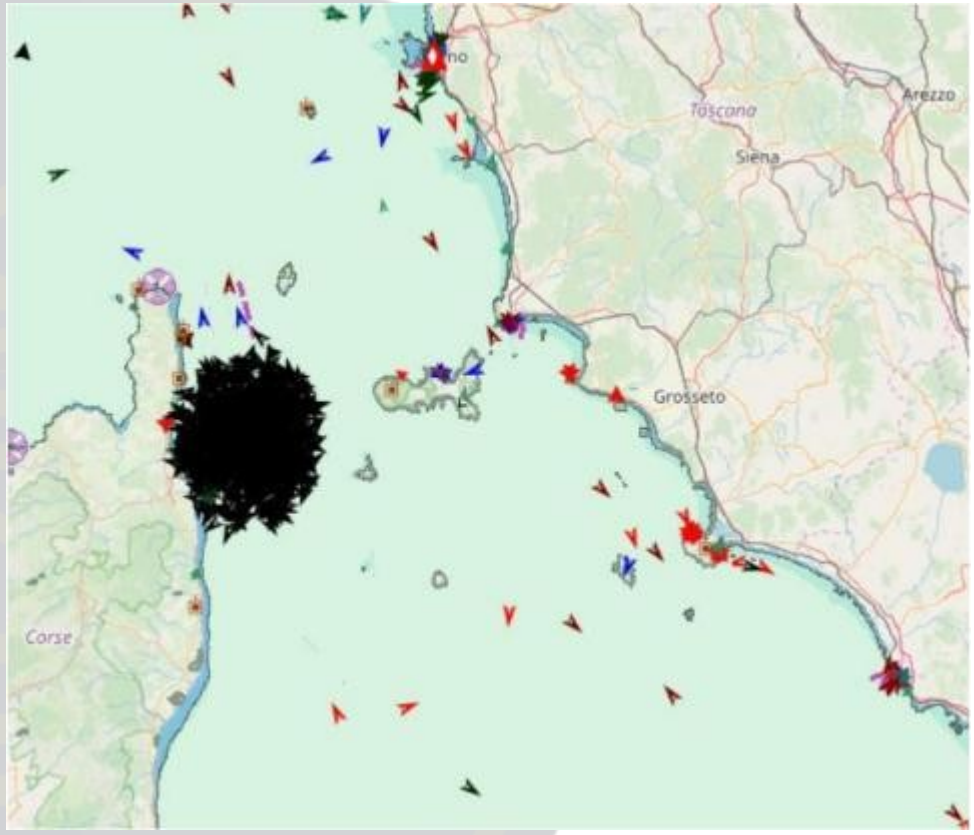
Dirottamento AIS – È possibile sostituire i segnali inviati dalle navi trasmettendo un segnale di potenza superiore nello stesso momento e alla stessa frequenza. L'aggressore può quindi modificare alcuni dettagli del messaggio originale, ad esempio per suggerire che la nave trasporta un carico pericoloso in una zona in cui tali carichi sono illegali.

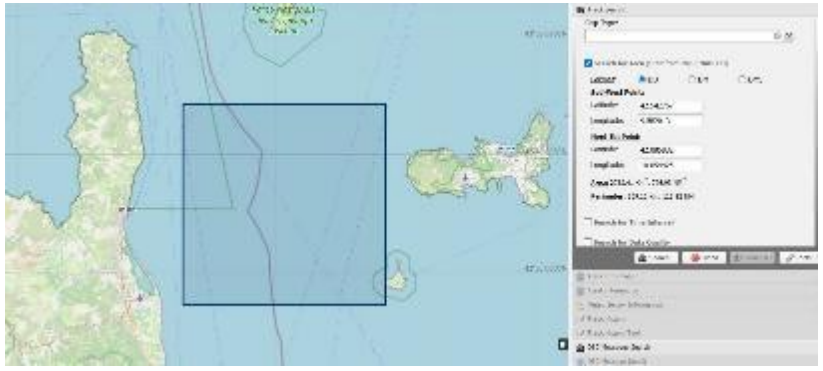
Come si può spoofare l'AIS?



1. I satelliti GPS inviano segnali alla nave;
2. Il ricevitore GPS calcola la posizione della nave in base ai segnali provenienti da satelliti GPS autentici;
3. Il ricevitore GPS invia informazioni precise sulla posizione all'AIS;
4. L'AIS invia informazioni sulla posizione reale della nave e la identifica al sistema globale di monitoraggio dell'AIS;
5. Il trasmettitore GNSS usurpatore imita il segnale satellitare GNSS autentico e diffonde falsi segnali di navigazione;
6. Il ricevitore GNSS calcola la posizione errata in base ai segnali del trasmettitore GNSS usurpatore;
7. Il ricevitore GNSS invia di informazioni informazionidi localizzazione all'AIS;
8. L'AIS invia informazioni sulla posizione falsa della nave al sistema di monitoraggio globale dell'AIS.

Attacco tramite spoofing





Il 3/12/19 tra l'isola d'Elba e la Corsica sono state ricevute centinaia di informazioni AIS da unità navali battenti bandiera olandese, create artificialmente, con codice di identificazione, posizione, rotta e velocità diversi.

Queste informazioni hanno completamente saturato un'area marittima circolare con un raggio di circa 15 Nm. L'area colpita dall'attacco è stata saturata con l'inserimento di oltre 850 bersagli falsi.

L'attacco è stato ripetuto due volte, alle 13:13 UTC (durata 3 minuti) e alle 13:28 (durata 4 minuti).

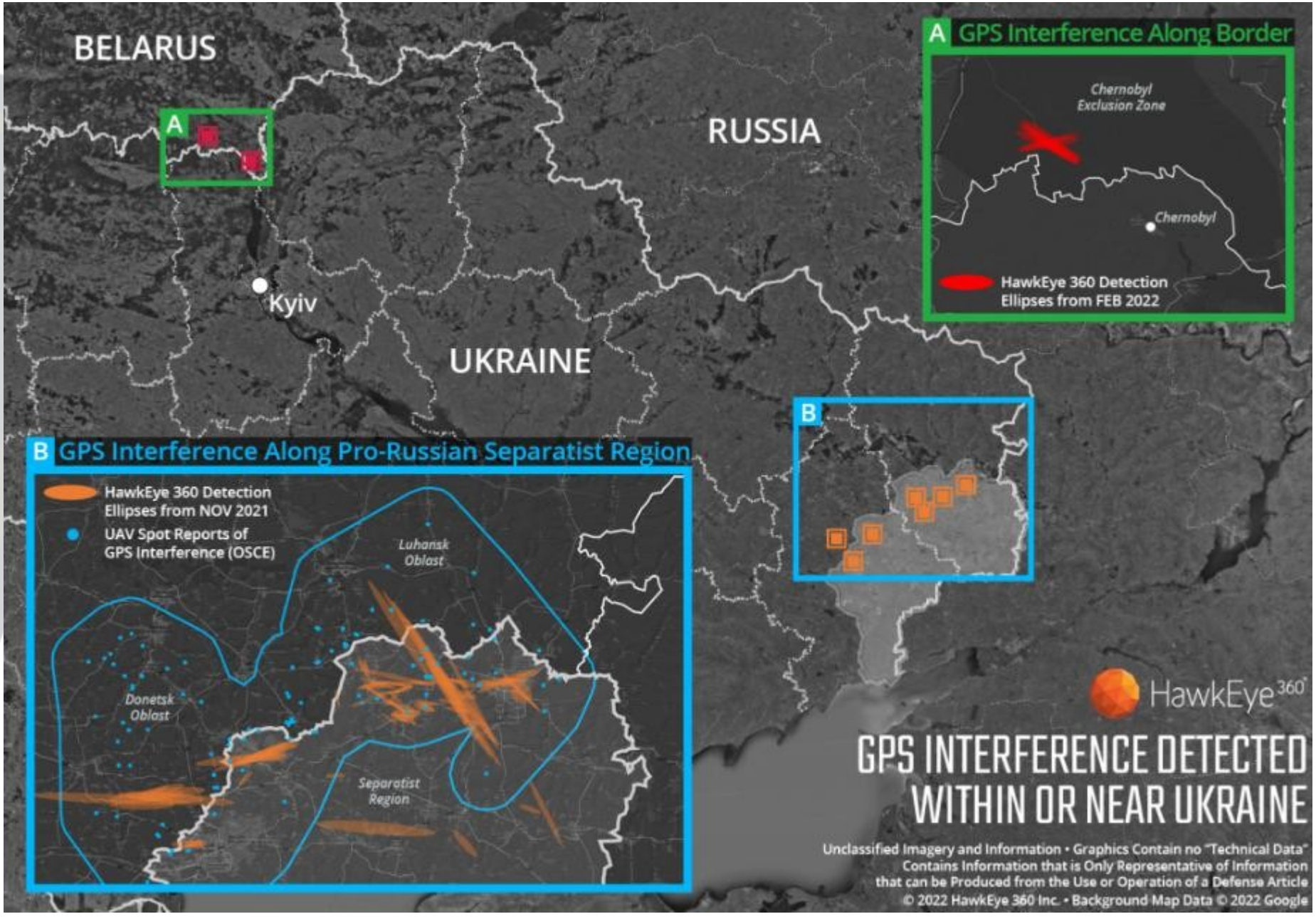
Il Brouillage

ANFR
AGENCE NATIONALE DES FRÉQUENCES

Brouillage en zone portuaire, en Martinique.

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

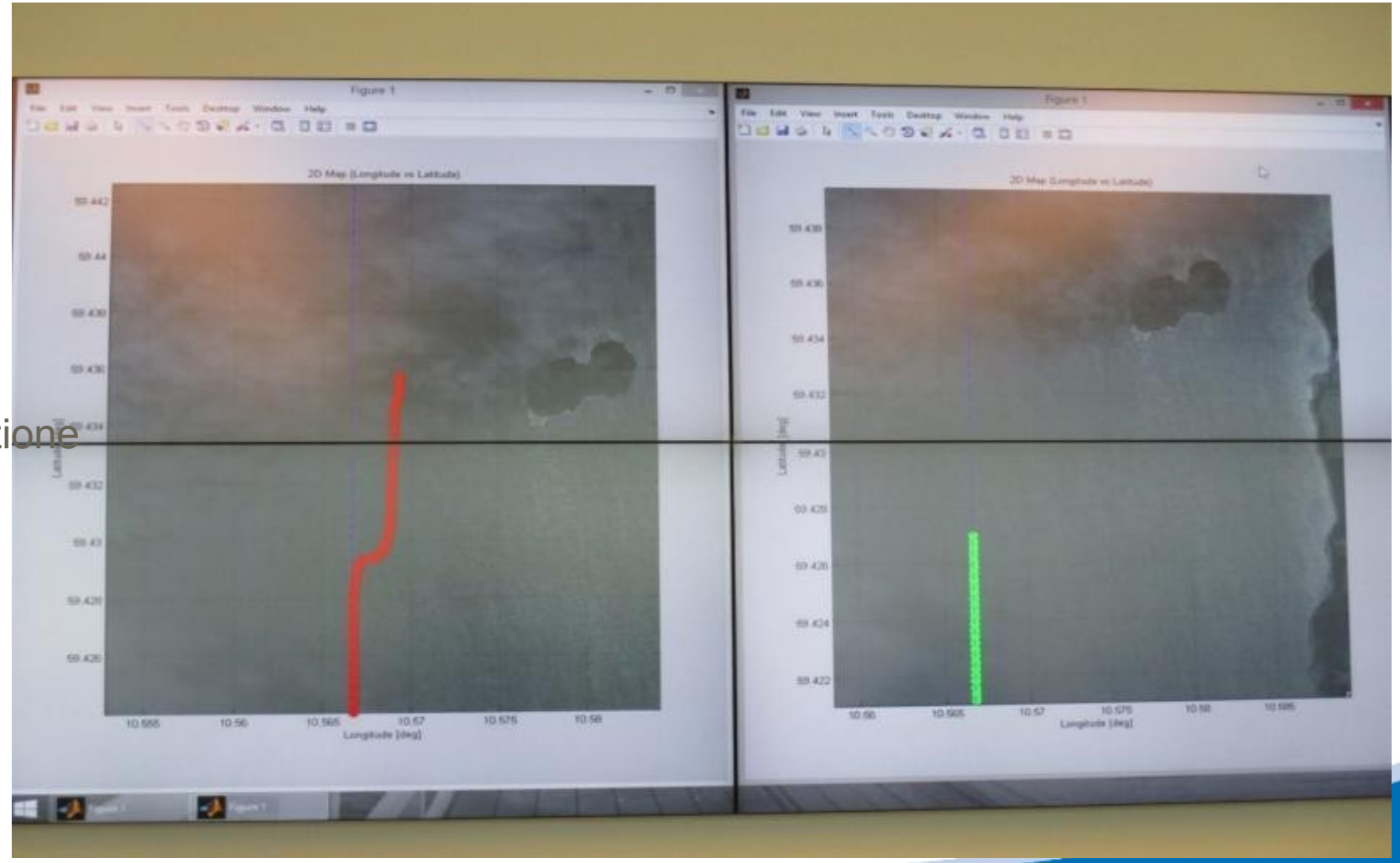
Disturbo di zona



Federal Police

Spoofing AIS / GNSS

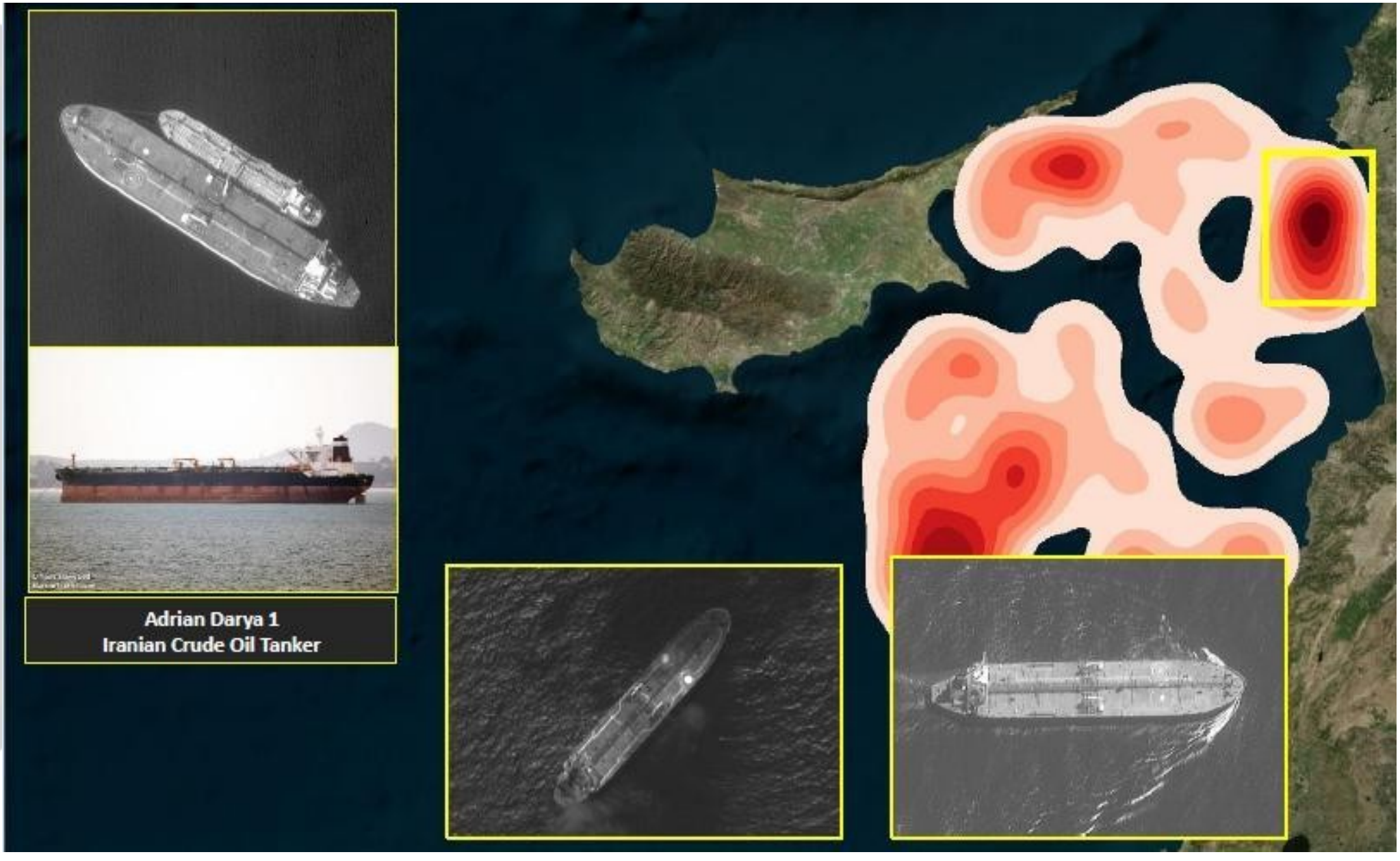
Fonte: Polizia marittima tedesca



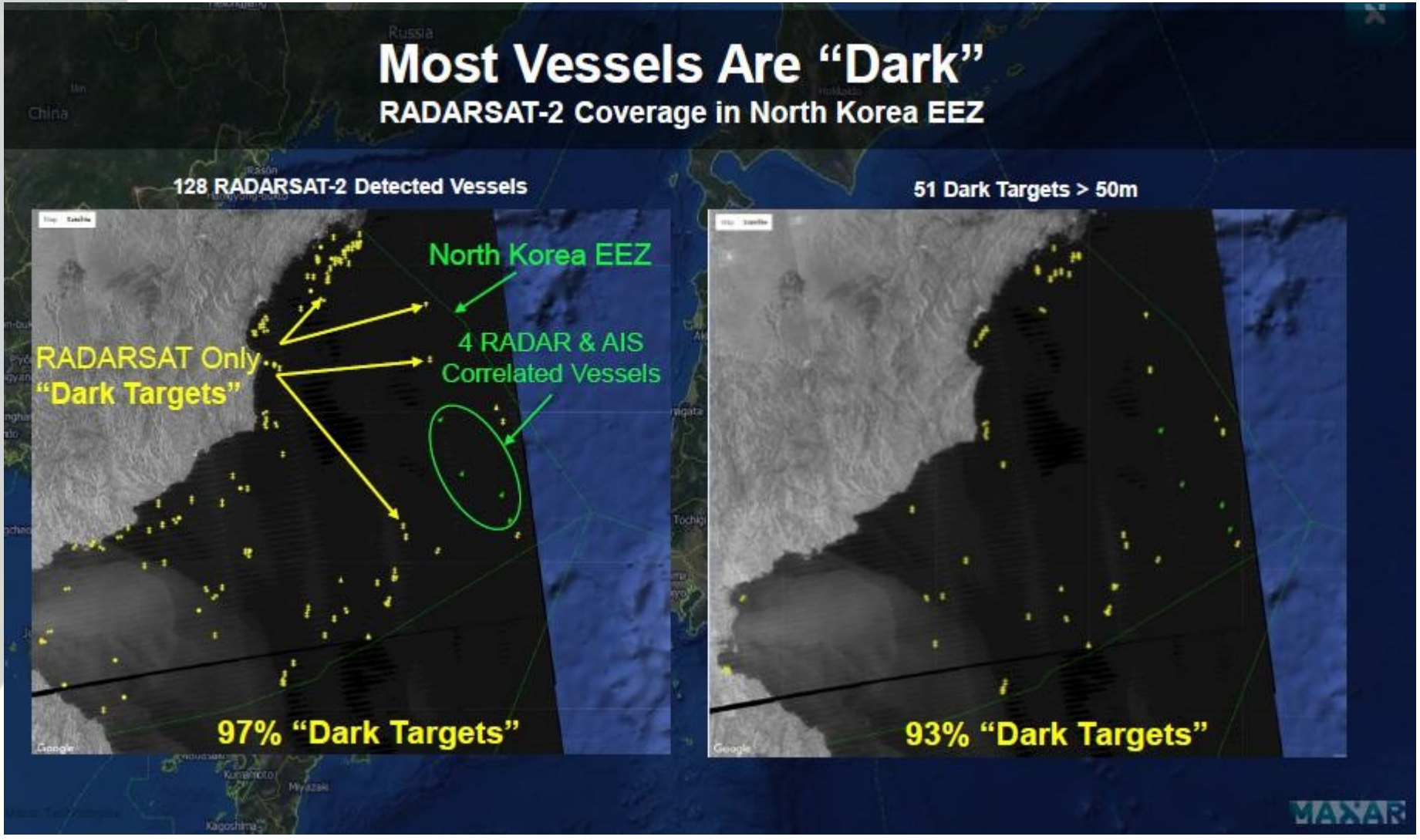
Spoofing della posizione

Posizione reale

Uso illegale dell'AIS - Le flotte fantasma



Uso illegale dell'AIS - Le flotte fantasma



Studio sulla sicurezza AIS

Progetto ENDOUME

Giochi Olimpici 2024 - Parigi

- Modello ANSSI
- EBIOS

ENDOUME: Sicurezza automatizzata delle zone marittime

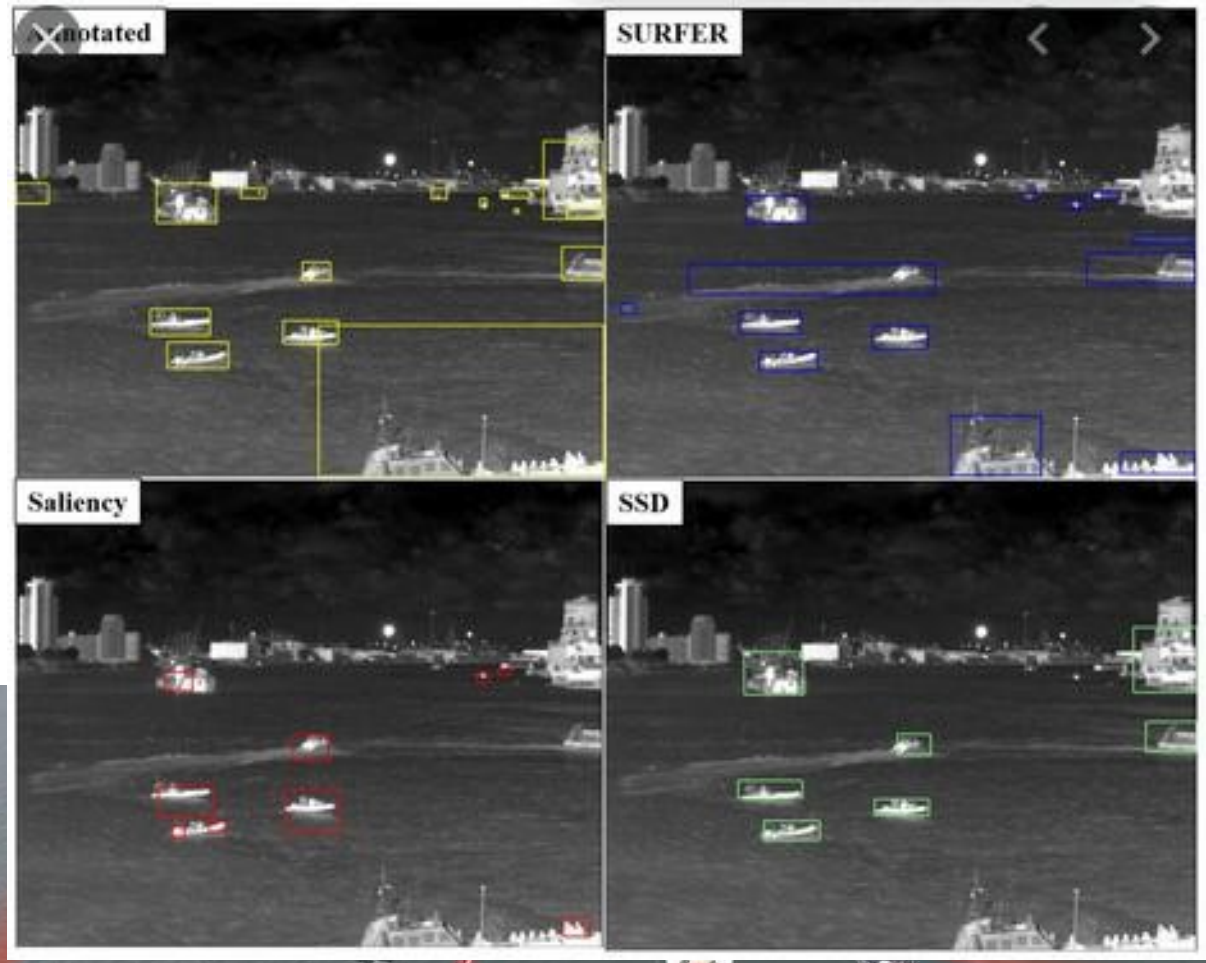
Definizione degli scenari e degli algoritmi

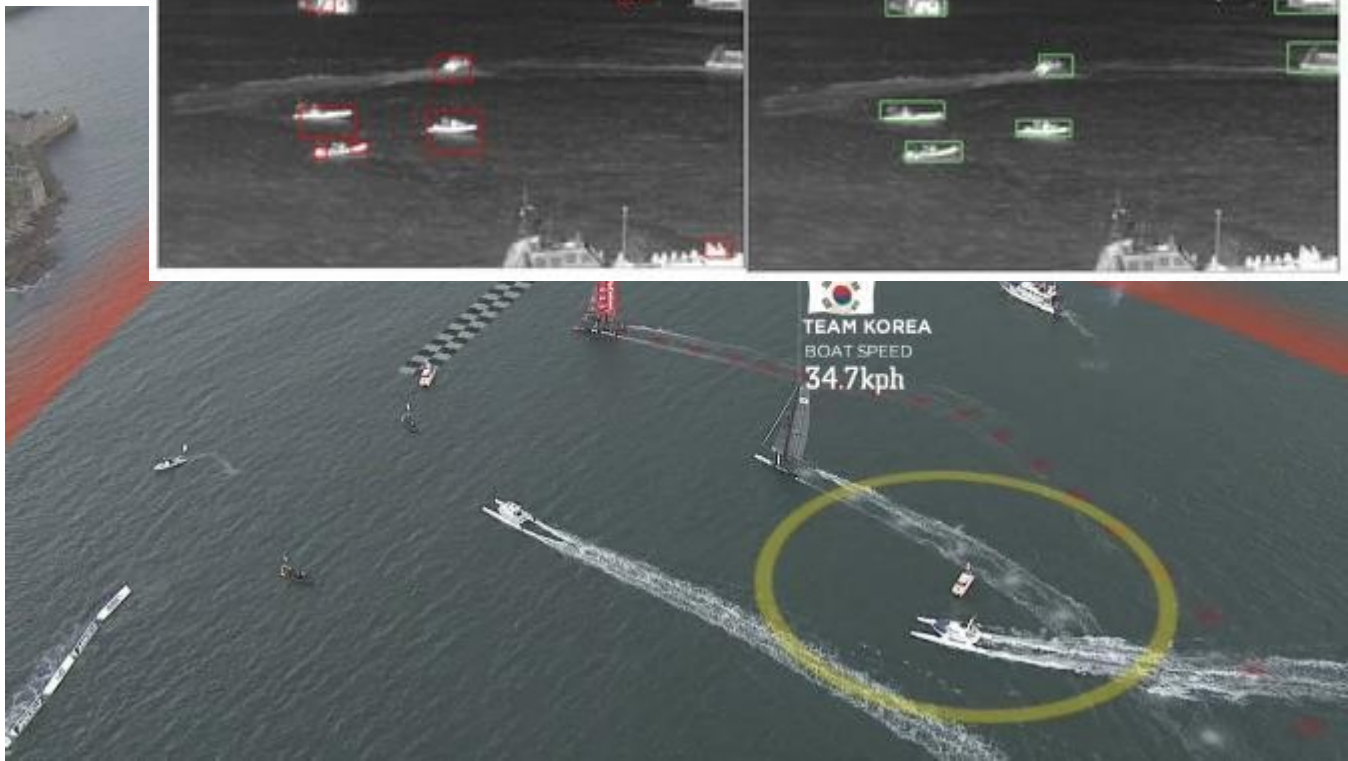
Creazione di un database Immagini dedicate all'apprendimento da parte del sistema

Obiettivo: apprendere l'ambiente, i suoi attori e i loro comportamenti


OUDY BAY
97


CHINA TEAM
ETNZ
ARTEMIS
OR SPITHILL
ENERGY TEAM

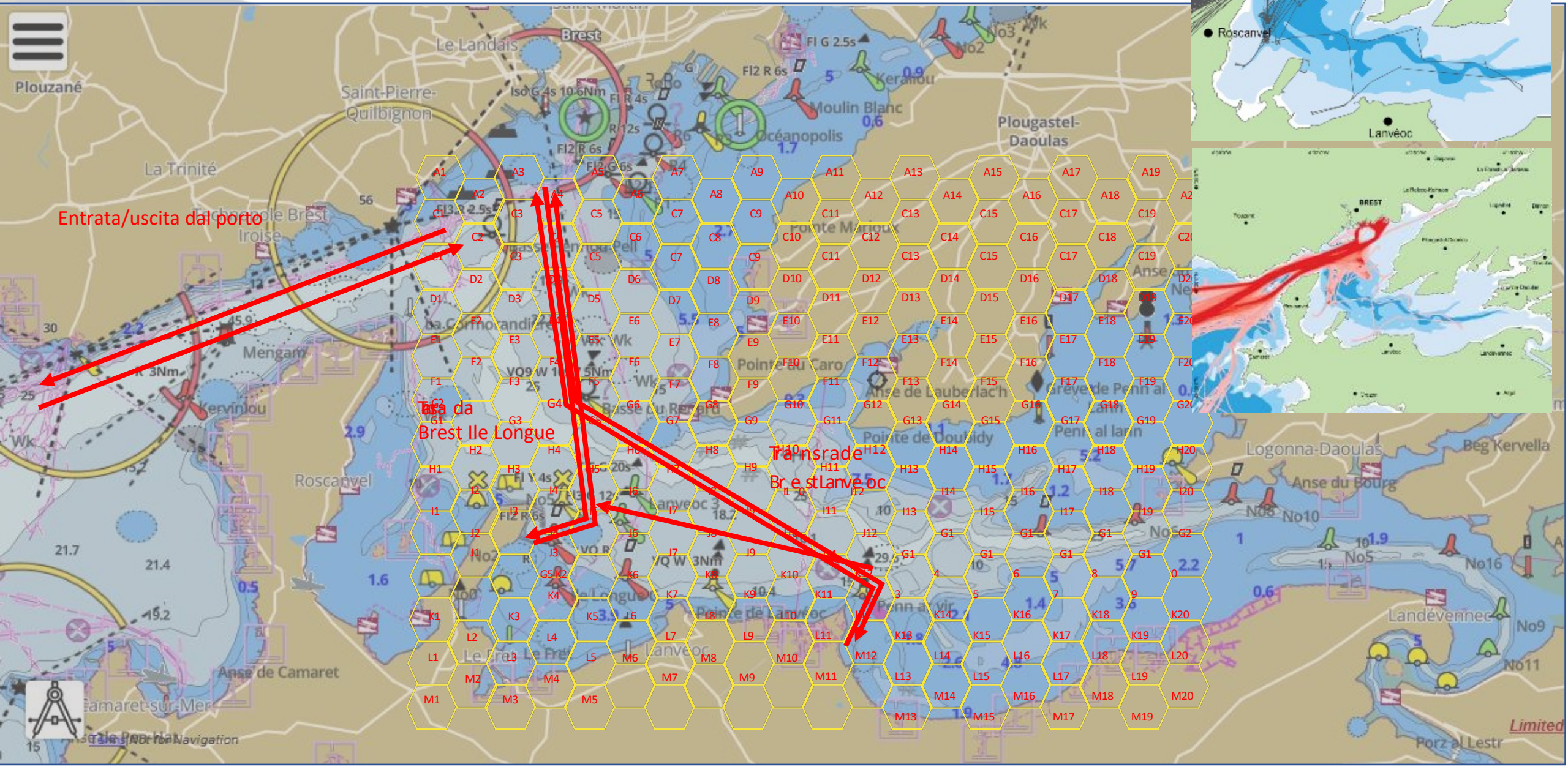

notated
SURFER
Saliency
SSD


TEAM KOREA
BOAT SPEED
34.7kph

Scenari

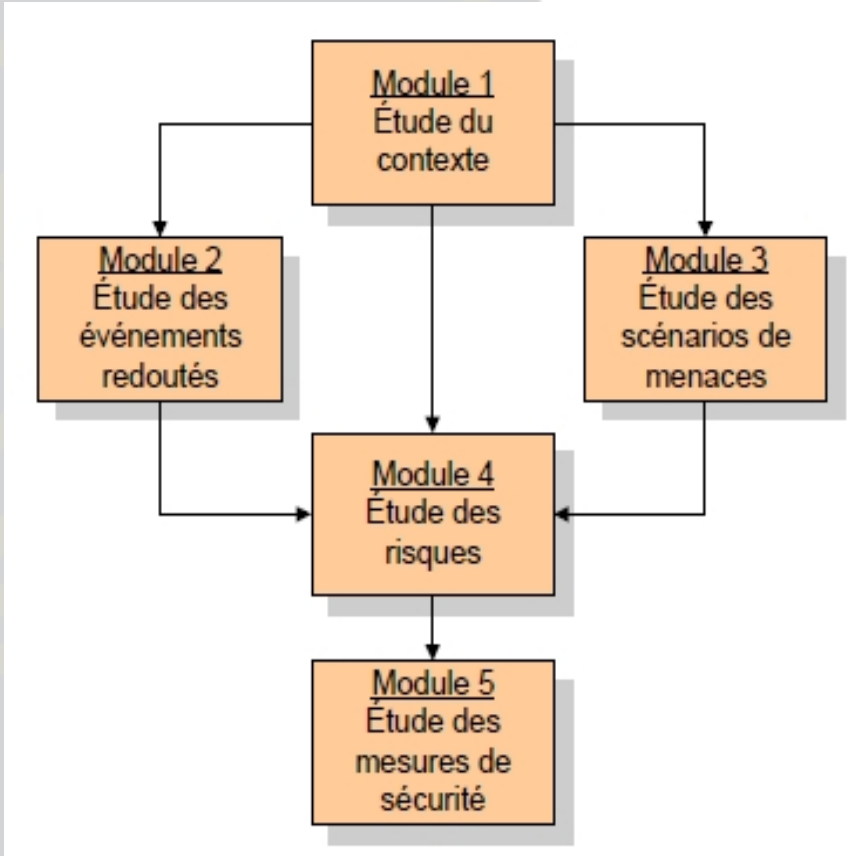
Scenari 1 - Gran premio della Scuola Navale

Modellizzazione dei modelli di routine



Studio sulla sicurezza (Segnali di sicurezza)

Metodologia



Modulo 1 – Studio del contesto

Definizione del quadro di gestione dei rischi, delle metriche e dell'ambito dello studio; vengono identificati i beni essenziali, i beni di supporto su cui si basano e i parametri da prendere in considerazione nel trattamento dei rischi.

Modulo 2 – Studio degli eventi temuti

Valutazione dei rischi. Identificazione e stima delle esigenze di sicurezza dei beni essenziali (in termini di disponibilità, integrità, riservatezza...), nonché di tutti gli impatti (sulle missioni, sulla sicurezza delle persone, finanziari, legali, sull'immagine, sull'ambiente, sui terzi e altri...) in caso di mancato rispetto di tali esigenze e delle fonti di minaccia (umane, ambientali, interne, esterne, accidentali, deliberate...) che potrebbero esserne all'origine, il che consente di formulare gli eventi temuti.

Modulo 3 – Studio degli scenari di minaccia

Identificazione e valutazione degli scenari che possono generare gli eventi temuti e quindi comporre i rischi. A tal fine, vengono studiate le minacce che le fonti di minaccia possono generare e le vulnerabilità sfruttabili

Modulo 4 – Studio dei rischi

Rischi che gravano sull'organizzazione confrontando gli eventi temuti con gli scenari di minaccia. Il modulo descrive anche come stimare e valutare tali rischi e, infine, come identificare gli obiettivi di sicurezza da raggiungere per affrontarli.

Modulo 5 – Studio delle misure di sicurezza

Gestione dei rischi. Questo modulo spiega come specificare le misure di sicurezza da attuare, come pianificare le misure e come convalidare la gestione dei rischi e i rischi residui.

Esigenza di sicurezza del sistema ENDOUME

Domanda n. 1: ENDOUME è importante per lo svolgimento delle vostre mansioni?

1	No, il sistema è accessorio all'adempimento delle missioni	Sì, le missioni sarebbero fortemente compromesse da un malfunzionamento del SI.	Sì, le missioni dipendono totalmente dal SI	Non lo so
		2		

Domanda n. 2: Se un sinistro colpisse ENDOUME, causando un malfunzionamento o una perdita di dati,

2	No, le conseguenze interne di un sinistro sarebbero trascurabili	Sì, le conseguenze interne di un sinistro sarebbero significative	Sì, le conseguenze interne di un sinistro sarebbero gravi, se non fatali	Non so
	1			

Domanda n. 3: Se un sinistro compromettesse la sicurezza di ENDOUME (malfunzionamento o interruzione del servizio, furto di informazioni, ecc.), le conseguenze per l'esterno (per i vostri utenti, amministrati, ecc.) sarebbero gravi?

3	No, le conseguenze di un sinistro per l'esterno sarebbero trascurabili	Sì, le conseguenze di un sinistro per l'esterno sarebbero significative	Sì, le conseguenze di un sinistro per l'esterno sarebbero gravi, se non fatali	Non lo so	
		2			**2**

Gravità delle potenziali conseguenze (riportare qui il valore massimo delle risposte alle domande da 1 a 3)

Domanda n. 4: Il fatto che i dati di ENDOUME siano inaccessibili è grave? Esempio: non è possibile accedere ai dati a causa di un guasto

.

4	No, l'inaccessibilità non ostacola quasi per nulla l'attività	Sì, il fatto che non siano accessibili disturberà l'attività in in modo significativo	Sì, il fatto che non sia accessibile può essere fatale per attività	Non lo so
	1			

Domanda n. 5: Il fatto che i dati siano alterati è grave? Esempio: un virus ha modificato i valori in un database, riportandoli tutti a 0.

5	No, il fatto che i dati siano alterati non interferisce quasi per nulla l'attività	Sì, il fatto che i dati siano alterati disturberà l'attività in in modo significativo	Sì, il fatto che i dati siano alterati può essere fatale per attività	Non lo so
		2		

Domanda n. 6: Il fatto che i dati di ENDOUME non siano o non siano più riservati è grave? Esempio: viene resa pubblica la lista dei beneficiari dei servizi sociali.

6	No, la mancanza di riservatezza non ostacola quasi per nulla l'attività	Sì, la mancanza di riservatezza disturberà l'attività in modo significativo	Sì, la mancanza di riservatezza può essere fatale per l'attività	Non so
	1			

Sensibilità dei dati del sistema (riportare qui il valore massimo delle risposte alle domande da 4 a 6)

2

Modulo 1 – Studio del contesto

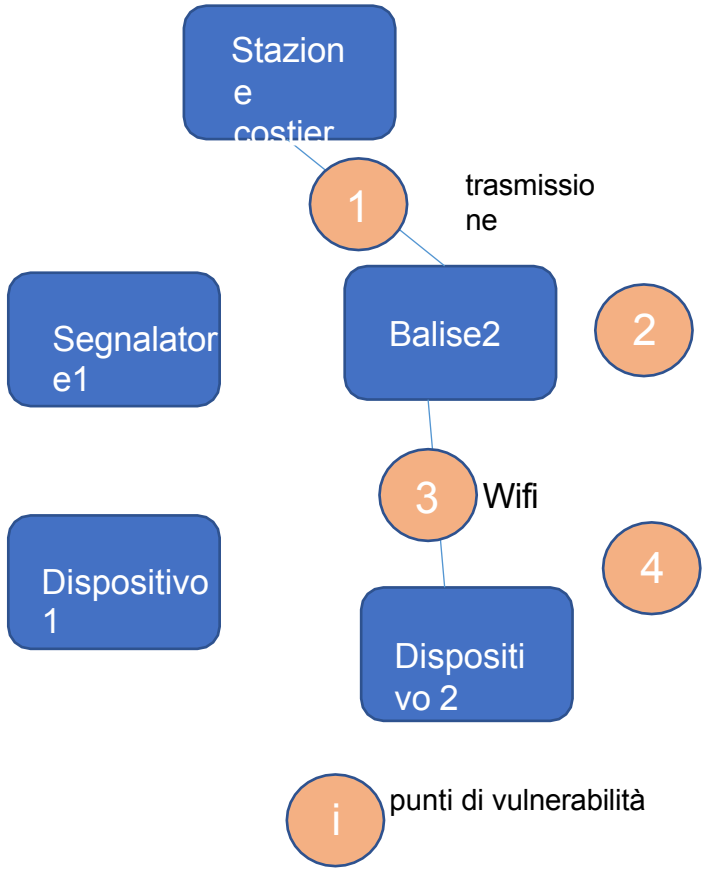
- Il sistema è composto da tre tipi di entità:
    - Una stazione costiera (SC)
    - Fari
    - Clienti/Dispositivi
- Interazioni tra queste entità:
    - Scambi tra la SC e i radiofari
    - Scambi tra i beacon e i dispositivi
- Il quadro di gestione dei rischi:
    - La SC è sicura (non può essere compromessa fisicamente)
    - Gli scambi tra la SC e i beacon avvengono tramite broadcast, su "frequenze proprietarie"
    - Gli scambi tra i beacon e le valute avvengono tramite Wi-Fi;
    - Ogni beacon mette a disposizione una pagina web che mostra la situazione tattica (SITAC) ricevuta dalla SC

Modulo 2 – Studio degli eventi temuti

- Accesso non autorizzato alla SITAC **(a)**
- Modifica della sitac **(b)**
- Diffusione di una falsa sitac / falsi messaggi **(c)**

Modulo 3 – Studio degli scenari di minaccia

I punti **da 1** a **4** nella figura a destra rappresentano i punti di vulnerabilità attraverso i quali possono verificarsi gli eventi temuti.



Scenari:

- Usurpazione della stazione costiera (ripetizione: da parte di una persona nelle vicino) **(1)** ⇒ **(c)** (e **(b)** indirettamente)
- Interferenza delle frequenze **(1)** ⇒ **(c)** (e **(b)** indirettamente)
- Furto di un segnalatore **(2)** ⇒ **(a)** (e **(b)** indirettamente)
- Accesso non autorizzato in prossimità di un beacon **(3)** ⇒ **(a)**
- Connessione illegale di un dispositivo a un beacon **(4)** ⇒ **(a)**

⇒: implica l'evento temuto

Modulo 4 Identificazione delle minacce (esigenza di sicurezza del sistema)

Domanda n. 1: ENDOUME è importante per lo svolgimento delle vostre mansioni?

1	No, il sistema è accessorio al all'adempimento delle missioni	Sì, le missioni sarebbero fortemente perturbate da un malfunzionamento del sistema informativo.	Sì, le missioni dipendono totalmente dal SI	Non so
		2		

Domanda n. 2: Se un sinistro colpisse ENDOUME, causando un malfunzionamento o una perdita di dati, 2

	No, le conseguenze interne di un sinistro sarebbero trascurabili	Sì, le conseguenze interne di un sinistro sarebbero significative	Sì, le conseguenze interne di un sinistro sarebbero gravi, se non fatali	Non so
	1			

Domanda n. 3: Se un sinistro compromettesse la sicurezza di ENDOUME (malfunzionamento o interruzione del servizio, furto di informazioni...), le conseguenze per l'esterno (per i vostri utenti, amministrati...) sarebbero gravi?

3	No, le conseguenze di un sinistro per l'esterno sarebbero trascurabili	Sì, le conseguenze di un sinistro per l'esterno sarebbero significative	Sì, le conseguenze di un sinistro per l'esterno sarebbero gravi, se non addirittura fatali	Non lo so	
Gravità delle potenziali conseguenze (riportare qui il valore massimo delle risposte alle domande da 1 a 3)		**2**			**2**

Domanda n. 4: Il fatto che i dati ENDOUME siano inaccessibili è grave? Esempio: non è possibile accedere ai dati a causa di un guasto hardware.

4	No, l'inaccessibilità dei dati non ostacola in alcun modo l'attività	Sì, l'inaccessibilità dei dati comprometterà in modo significativo l'attività significativo	Sì, il fatto che non siano accessibili può essere fatale per l'attività	Non lo so
	1			

Domanda n. 5: Il fatto che i dati siano alterati è grave? Esempio: un virus ha modificato i valori in un database, riportandoli tutti a 0.

5	No, il fatto che i dati siano alterati non ostacola quasi per nulla l'attività	Sì, il fatto che i dati siano alterati disturberà l'attività in in modo significativo	Sì, il fatto che i dati siano alterati può essere fatale per l'attività	Non lo so
		2		

Domanda n. 6: Il fatto che i dati di ENDOUME non siano o non siano più riservati è grave? Esempio: viene reso pubblico l'elenco dei beneficiari del servizio sociale.

6	No, la mancanza di riservatezza non ostacola quasi per nulla l'attività	Sì, la mancanza di riservatezza disturberà l'attività in modo significativo	Sì, la mancanza di riservatezza può essere fatale per l'attività	Non so
	1			
Sensibilità dei dati del sistema (riportare qui il valore massimo delle risposte alle domande da 4 a 6)				**2**

Domanda n. 7: Qual è il livello massimo di competenza presunto dell'autore o del gruppo di autori dell'attacco che potrebbero danneggiare il sistema?

7	Singolo individuo con livello di competenza elementare	Individuo isolato con livello di competenza avanzato	Gruppo di individui organizzati, con livelli di competenza individuali da bassi a medi, o individuo isolato con competenze esperte	Gruppo di individui esperti, organizzati, con mezzi quasi illimitati
				1

Domanda n. 8: Qual è la precisione dei potenziali attacchi al sistema informativo?

8	Attacchi "casuali" al cyberspazio	Attacchi diretti verso il continente europeo o la Francia	Attacchi mirati a un gruppo di vittime con caratteristiche comuni	Attacchi mirati specificatamente al sistema
				1

Domanda n. 9: Qual è il livello di sofisticazione dei potenziali attacchi contro il sistema informativo?

9	Strumenti di attacco banali (software di scansione delle porte, virus noti, ecc.)	Strumenti generici sofisticati pronti all'uso uso (reti botnet a noleggio, vulnerabilità , ecc.)	Strumenti sofisticati, adatti al SI (zero-day, ecc.)	Toolkit altamente sofisticato.
				1

Domanda n. 10: Qual è la visibilità dei potenziali attacchi contro il sistema informativo?

10	Attacco annunciato (rivendicazioni di "hacktivisti", richiesta di riscatto, ecc.)	Attacco immediatamente rilevabile dai suoi effetti sul sistema informatico	Attacco discreto, che lascia tracce nei registri degli eventi, ma non interferisce con il funzionamento del sistema informativo	Attacco invisibile, realizzato lasciando tracce minime
				1

Domanda n. 11: Qual è la frequenza e la persistenza dei potenziali attacchi contro il sistema informativo?

11	Permanente.	Ricorrenti: attacchi a ondate successive di notevole entità	Puntuale: l'attacco si verifica più volte senza regolarità nella sua frequenza (può essere collegata all'attualità).	Unica: l'attacco si verifica sul bersaglio solo una una sola volta
				1

Base di stima del potenziale di attacchi informatici (riportare qui il valore massimo delle risposte alle domande da 7 a 11)	**1**

Domanda n. 12: Qual è il livello di eterogeneità del sistema? Esempio: diversi software, hardware o reti per lo stesso sistema.

12	Il sistema è considerato omogeneo	Il sistema è considerato leggermente eterogeneo	Il sistema è considerato fortemente eterogeneo	Non so
		2		

Domanda n. 13: Qual è il grado di apertura/interconnessione del sistema? Esempio: Internet, un altro sistema interno o esterno (quello di un fornitore, di un'altra autorità amministrativa...)

13	Il SI non è aperto	Il SI è aperto solo a sistemi interni controllati	Il sistema è aperto a sistemi interni non controllati o esterni	Non lo so
		2		

Domanda n. 14: Il contesto in cui si trovano il SI e i suoi componenti (hardware, software, reti) è soggetto a cambiamenti regolari?

14	Il SI e il suo contesto sono considerati stabili	Il SI e il suo contesto cambiano spesso	Il SI e il suo contesto evolvono costantemente	Non so
		2		

Domanda n. 15: I componenti del SI vengono aggiornati regolarmente?

15	Tutti i componenti del SI sono aggiornati costantemente	Una parte dei componenti del SI viene aggiornata regolarmente	Gli aggiornamenti vengono effettuati in modo irregolare	Non lo so
		2		

Esposizione e vulnerabilità (riportare qui il valore massimo delle risposte alle domande da 12 a 15) **2**

Totale: **7**

Somma dei quattro valori	Necessità di sicurezza del sistema
Da 4 a 6	1 - Basso
Da 7 a 9	2 - Medio
Da 10 a 16	3 - Forte

Modulo 5 – Studio delle misure di sicurezza

- Messa in sicurezza del punto **(1)**:

  - Crittografia delle comunicazioni con AES a 128 bit; una chiave comune a tutti i beacon e alla SC
  - Lo scambio e la gestione di questa chiave avverranno con un sistema crittografico a chiave pubblica (RSA 3072 bit); ogni beacon avrà la propria chiave pubblica memorizzata sulla SC a tale scopo.
  - La chiave AES deve essere rinnovata ad ogni implementazione del sistema. Può anche essere rinnovata periodicamente (ad esempio ogni giorno).
  - Misura contro l'usurpazione della SC (replay) da considerare separatamente.

- Messa in sicurezza del punto **(2)**:

  - In caso di furto di un beacon (furto che si presume rilevabile in modo efficace), la SC avvia la procedura di rinnovo della chiave AES con i beacon non compromessi.

- Messa in sicurezza del punto **(3)**:

  - Un dispositivo si connette in Wi-Fi, tramite un browser web, al server di un beacon per ricevere la SITAC; questa connessione sarà protetta con il protocollo HTTPS (o WSS).

Modulo 5 – Studio delle misure di sicurezza (continua)

Messa in sicurezza del punto **(4)**:

- **Dopo** la sicurezza del punto **(3)**, l'obiettivo qui è garantire che il dispositivo abbia il diritto di accedere al SITAC. Sono possibili diverse opzioni.
- Soluzione con codice PIN / tag:
  - Si considera una funzione di hash H (ad esempio SHA-256)
  - Per ogni tag *bi:*
    - si genera un codice PIN ***pi*** e si sceglie un testo *ti;*
    - si calcola: *hi* = H(*ti, rand_seed*)*, ki* = Epsilon(*pi*) = H*(pi, no_seed*) e *ci* = **ENC_AES_256**(*ki*, *hi*)
    - si memorizza su *bi* la coppia ***(hi, ci)***
- Autenticazione della valuta sul tag *bi* per l'accesso al sito: (dopo aver completato il punto **(3)**)
  - *bi* invia ***ci*** a *d*
  - *d* calcola: *ki* = Epsilon(***pi***) = H(***pi***, *no_seed*), quindi *m* = ***DEC_AES_256****(ki, hi);* e invia *m* a *bi*
  - *bi* verifica se *m* = ***hi***; se sì, l'autenticazione è valida; se no, reget.
  - Saranno consentiti al massimo 5 (?) tentativi al dispositivo, dopodiché verrà bloccato.
- Ogni codice PIN ***pi*** deve essere rinnovato ad ogni implementazione del sistema e anche periodicamente (ad esempio ogni giorno). Quindi anche ogni coppia ***(hi, ci)*** su ciascuno dei beacon.

DOMANDE?