Διασφάλιση του κινδύνου που συνδέεται με τις κυβερνοεπιθέσεις

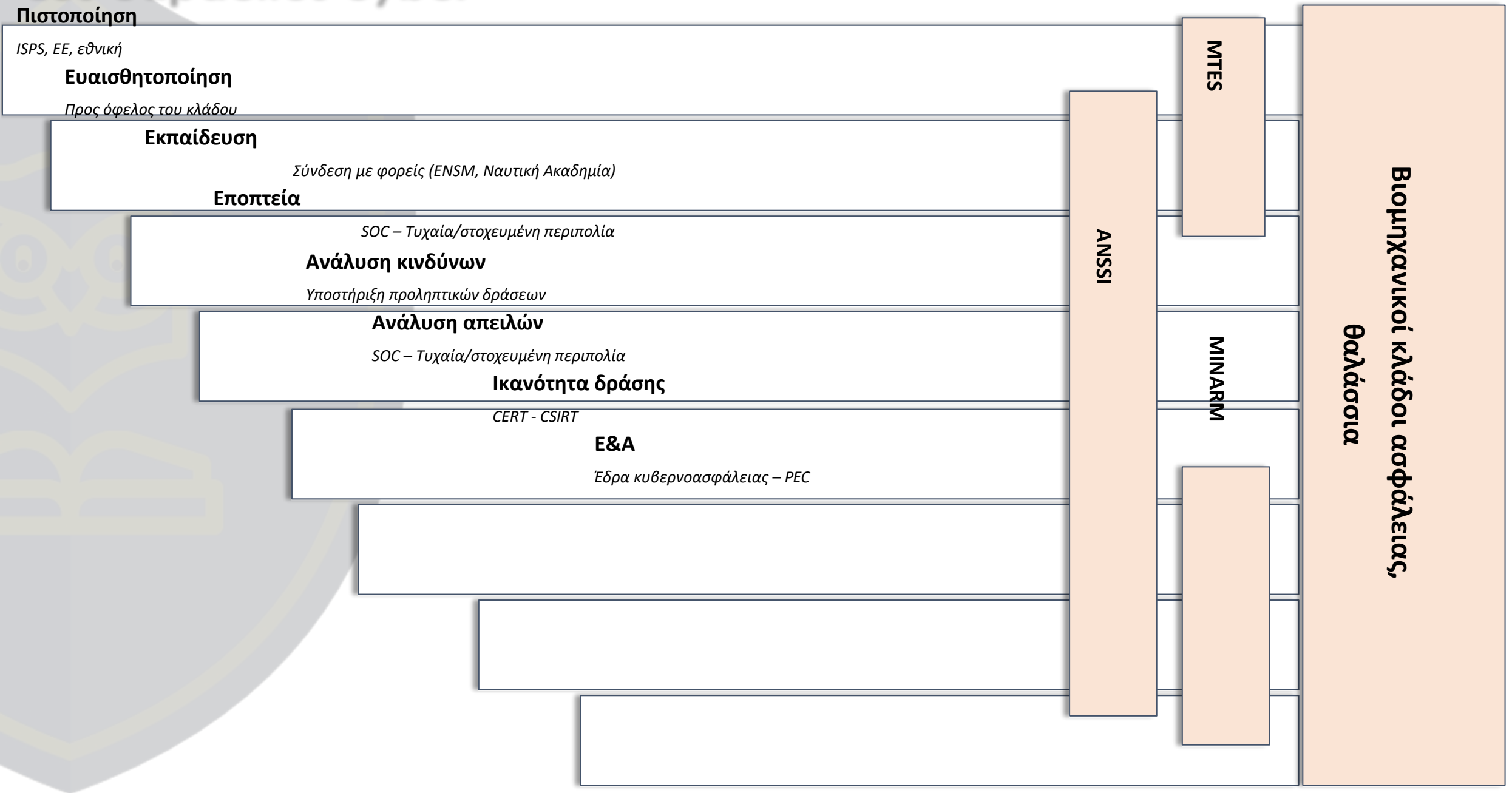
Ενότητα 7- C2 Ασφάλιση για την κάλυψη των δαπανών που προκύπτουν από κυβερνοεπιθέσεις σε συστήματα πληροφοριών

Κίνδυνος και ασφάλιση

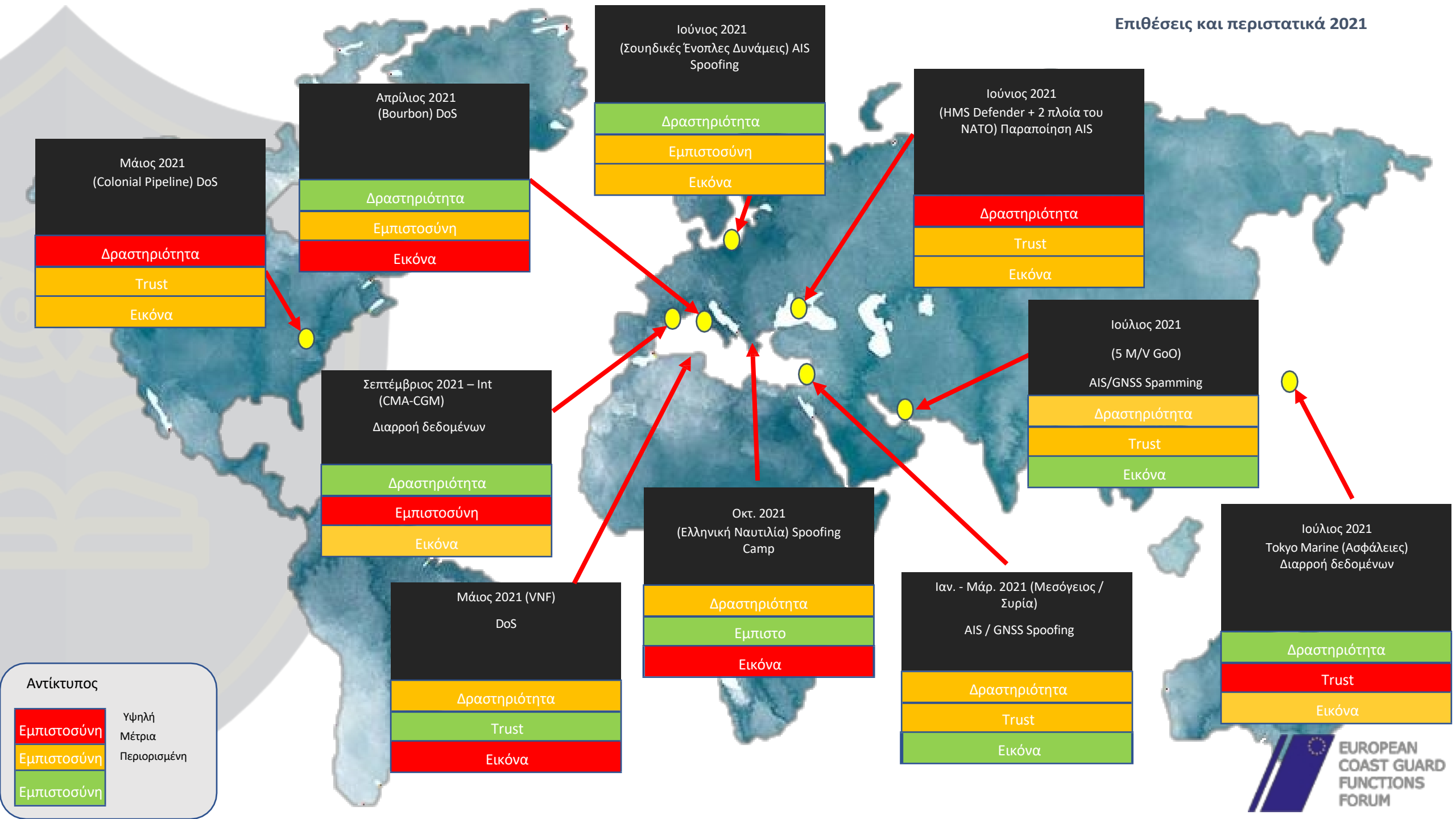
- Τεχνική ανάλυση (ANSSI)
- Τομεακή μελέτη (CFM)
- Ανάλυση κινδύνου (BESSE / ANSSI)

ΕΞΑΜΗΝΟ 10					
Ενότητα 7 - Εφαρμογή μιας αποτελεσματικής πολιτικής για την ασφάλεια στον κυβερνοχώρο		**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 τομείς αλλά ίσης σημασίας				
EU7-A-2	Κυβερνοασφάλεια: μια κοινή όραση μεταξύ χρηστών, σχεδιαστών εξοπλισμού, δίκτυα μετάδοσης, υπηρεσίες διαχείρισης δεδομένων				
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				

Οι ικανότητες στον κυβερνοχώρο



Επιθέσεις και περιστατικά 2021



EUROPEAN COAST GUARD FUNCTIONS FORUM

Τελευταίες εξελίξεις

Ένας παγκόσμιος κίνδυνος

Greek shipowners cyber tricked over Halloween weekend

Adis Ajdin · November 3, 2021 · 2,523 · 1 minute read

To protect Putin, Russia is spoofing GPS signals on a massive scale

GPS spoofing technology linked to Russia has been used almost 10,000 times, tricking ships into being off-grid. It's also used to protect Vladimir Putin and secretive Russian areas

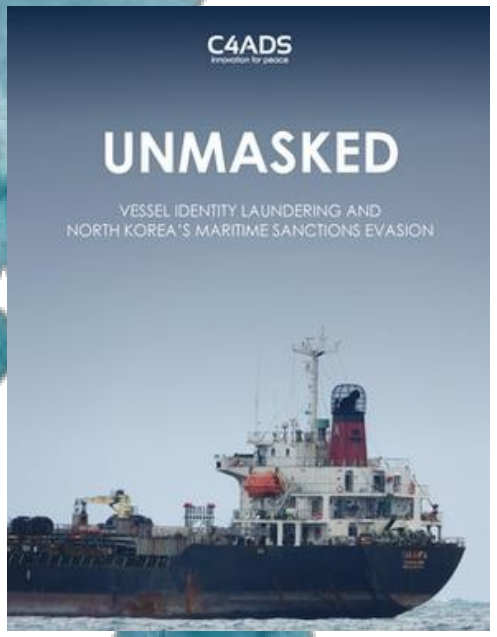
Το spoofing έχει επηρεάσει εκατοντάδες εμπορικά πλοία στα ρωσικά ύδατα τα τελευταία 5 χρόνια.

Η MAERSK δέχεται επίθεση στα θεμέλιά της

Maersk has suspended a number of crew members after allegations were posted online that a 19-year-old woman was raped aboard one of the company's vessels.

CNN INVESTIGATES

'I was trapped': Shipping giant investigates alleged rape of 19-year-old during federal training program

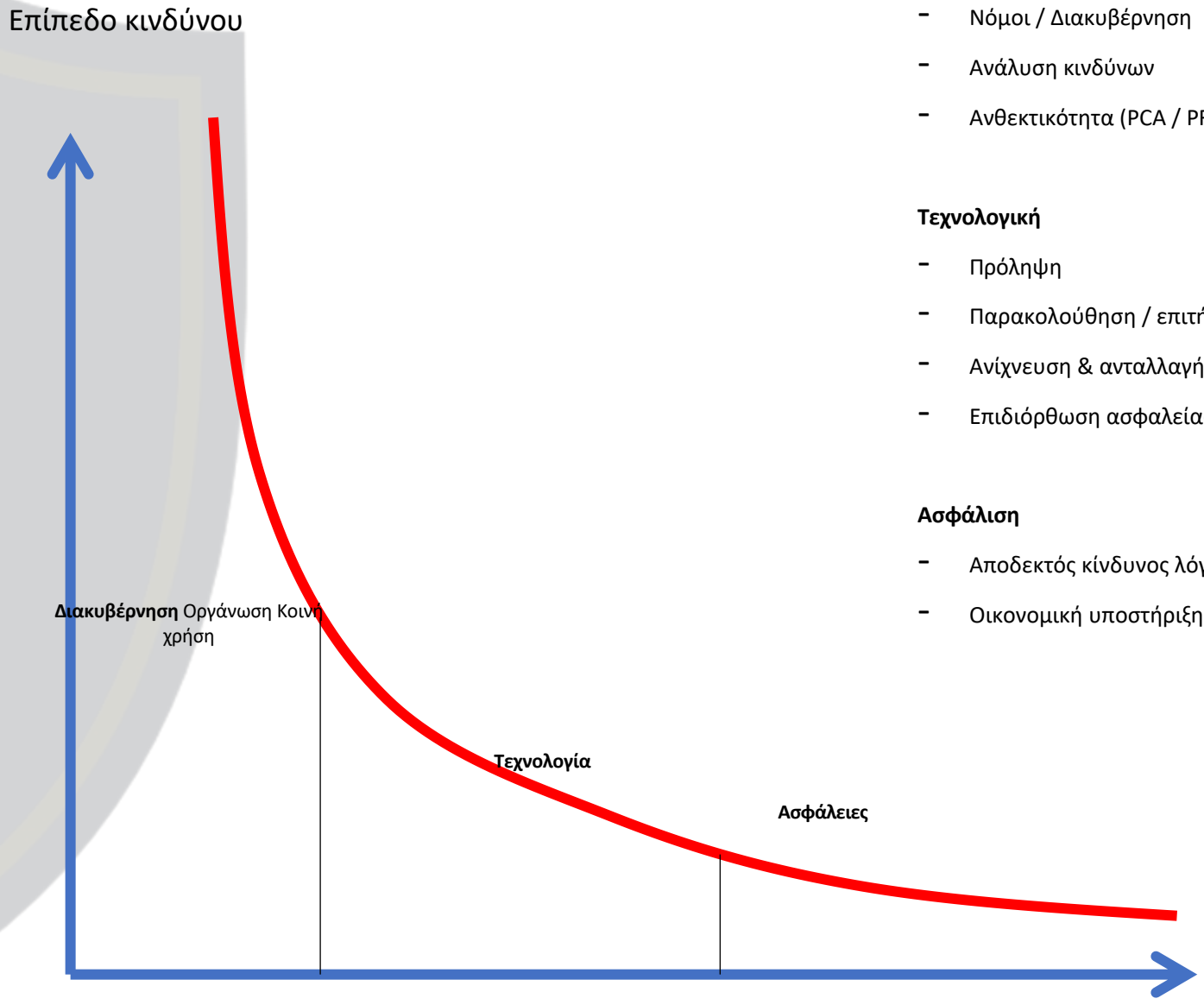


Μέσω **της «νομιμοποίησης της ταυτότητας των πλοίων»**, οι παραβάτες των κυρώσεων της Βόρειας Κορέας χρησιμοποιούν περίπλοκα σχέδια για να δημιουργήσουν ψευδείς ταυτότητες που επιτρέπουν στα πλοία που έχουν υποστεί κυρώσεις να λειτουργούν ατιμώρητα — σε ορισμένες περιπτώσεις για χρόνια (π.χ. το MV KINGSWAY, που έχει υποστεί κυρώσεις από το Συμβούλιο Ασφαλείας των Ηνωμένων Εθνών για λαθρεμπόριο καυσίμων προς τη Βόρεια
Η Κορέα, η οποία άλλαξε την ταυτότητά της στα τέλη του 2018 και συνέχισε να λειτουργεί χωρίς να εντοπιστεί για τρία χρόνια.

https://splash247.com/new-report-highlights-the-rise-of-vessel-identity-laundering/

Πληροφοριακές επιχειρήσεις
Πληροφοριακός πόλεμος

Μείωση του κινδύνου στον κυβερνοχώρο



Οργάνωση

- Νόμοι / Διακυβέρνηση
- Ανάλυση κινδύνων
- Ανθεκτικότητα (PCA / PRA)

Τεχνολογική

- Πρόληψη
- Παρακολούθηση / επιτήρηση
- Ανίχνευση & ανταλλαγή πληροφοριών για περιστατικά
- Επιδιόρθωση ασφαλείας

Ασφάλιση

- Αποδεκτός κίνδυνος λόγω χαμηλής συχνότητας εμφάνισης
- Οικονομική υποστήριξη / ανασυγκρότηση

Κυβερνοασφάλεια στον θαλάσσιο κόσμο

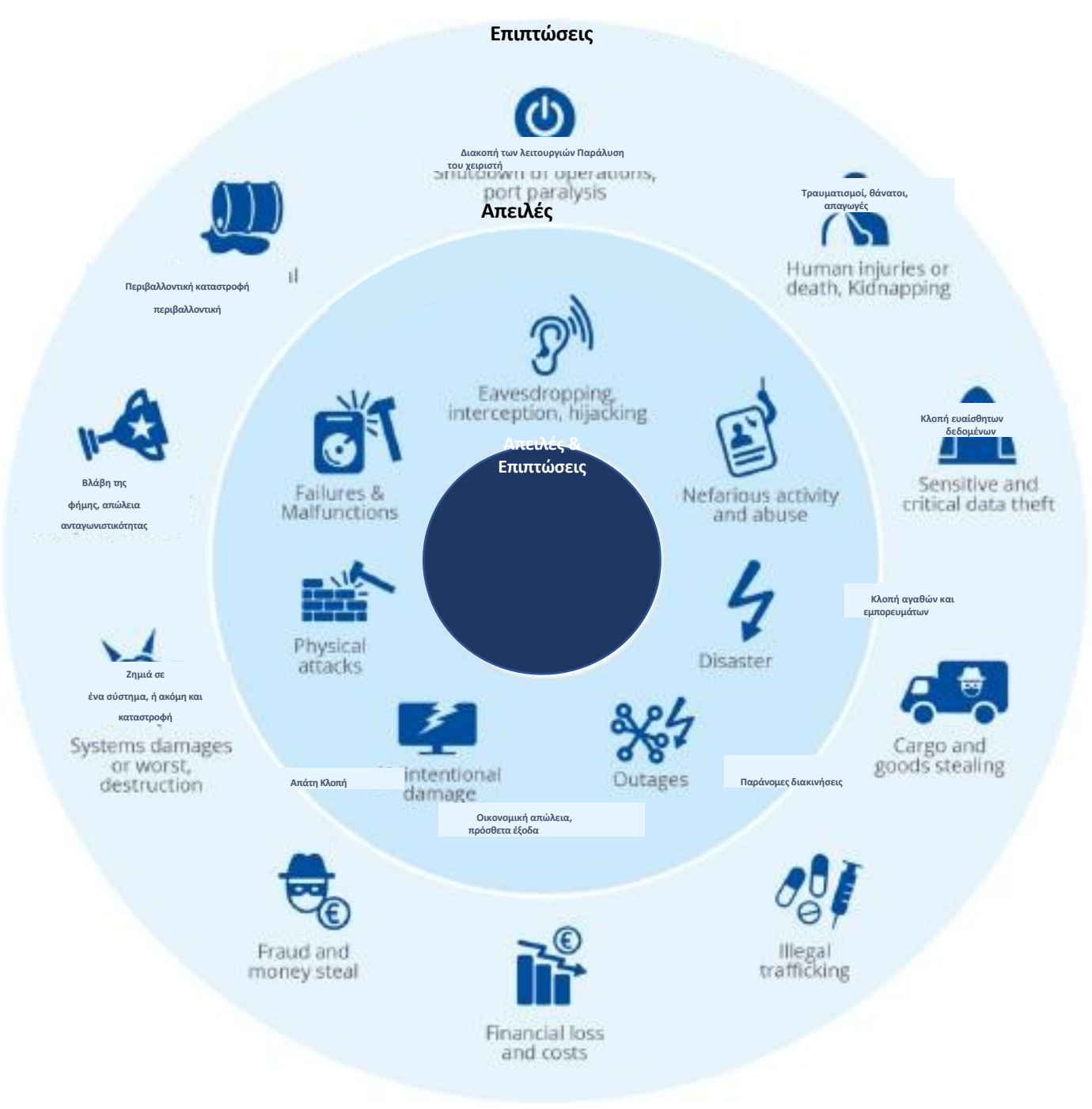
-

Μελέτες

1 – ANSSI

2 – CFM

3 – BESSE / ANSSI



ανάλυση

Οι αναλύσεις κινδύνου που διεξάγονται στον τομέα αυτό, ιδίως από την ANSSI, επιτρέπουν τον εντοπισμό πολλών απειλών που αφορούν τον ναυτιλιακό τομέα στο σύνολό του. Η μελέτη που παρουσιάστηκε στον ΔΝΟ το 2017 επισημαίνει τους ακόλουθους 5 τομείς:

- Οι πληροφορίες και των λειτουργικά λειτουργικά σε επιβαίνουντων πλοίων και των
- Η διασυνδεσιμότητα των συστημάτων (είτε επί του σκάφους είτε στην ξηρά)
- Η ανάπτυξη του Διαδικτύου των Πραγμάτων (IOT) και της κινητικότητας
- Η έλλειψη ανθεκτικότητας στα κτίρια
- Η έλλειψη εκπαίδευσης και κατάρτισης των πληρωμάτων για την αντιμετώπιση κακόβουλων ενεργειών

Η DAM κατά τη διάρκεια ενός ελέγχου περιέγραψε τα μέτρα που πρέπει να εφαρμοστούν για την αύξηση του

επίπεδο προστασίας του πλοίου.

Ιδιαίτερα στους τομείς της ψηφιακής εμπιστοσύνης, της διακυβέρνησης, της διαχείρισης της πρόσβασης και των διαρροών δεδομένων, της ασφάλειας και της ιχνηλασιμότητας των συναλλαγών, της εμπιστευτικότητας και της συνέχειας των υπηρεσιών.

Τέλος, πραγματοποίησε μια ανάλυση μετά την αξιολόγηση των κινδύνων, η οποία περιγράφει συνοπτικά τα μέσα που μπορούν να τεθούν σε εφαρμογή για την προστασία των ενσωματωμένων βιομηχανικών συστημάτων. Αυτές οι πρώτες προσπάθειες αξίζει να συνεχιστούν σε ένα καθορισμένο πλαίσιο και με εργαλεία ειδικά για τον τομέα.

Άλλες μελέτες έχουν διεξαχθεί, ιδίως από ιδιωτικές εταιρείες, τον IMO και τη ΓΔ MARE

Έξι τύποι απειλών

Κακόβουλο λογισμικό: Κακόβουλο λογισμικό του οποίου η διάδοση είναι ανεξέλεγκτη

Script kiddy (απασχολούμενος έφηβος ή, γενικότερα, μοναχικός και ευκαιριακός εισβολέας):

- Πολύ περιορισμένα μέσα (< 100 €)
- Το παιχνίδι (και ενδεχομένως το κέρδος) ως κίνητρο
- Ευκαιριακή επίθεση

Κακόβουλος υπάλληλος (μνησικακία / απληστία):

- Μικρά μέσα (< 1.000 €)
- Κύρια κίνητρα: να βλάψει τον εργοδότη του, αποφεύγοντας τα θύματα
- Διακριτικότητα, όποτε είναι δυνατόν
- Εύκολη πρόσβαση σε όλα τα μέρη του πλοίου

Τρομοκρατική ομάδα:

- Μέτρια μέσα (από 10 έως 50 000 €)
- Αναζήτηση ανθρώπινων θυμάτων, υλικών ζημιών, υψηλή προβολή στα μέσα μαζικής ενημέρωσης

Εγκληματική οργάνωση:

- Υψηλά μέσα (της τάξης του ενός εκατομμυρίου ευρώ)
- Στόχος κερδοφορίας
- Χαμηλές ηθικές υποχρεώσεις
- Αναζήτηση διακριτικότητας

Κατάσταση:

- Σχεδόν απεριόριστα μέσα
- Στόχοι κάθε είδους
- Απουσία ηθικών περιορισμών
- Απαιτείται διακριτικότητα

Συστήματα & Ευπάθειες

Συστήματα, εξοπλισμός και τεχνολογίες των θαλάσσιων κλάδων:

Συστήματα βασικής υποδομής Συστήματα «back-end» και διοικητικά
Συστήματα επικοινωνίας
Συστήματα διαχείρισης φορτίου Συστήματα ελέγχου
πρόσβασης Συστήματα γέφυρας
Συστήματα πρόωσης, διαχείρισης μηχανών και ελέγχου ισχύος Συστήματα συντήρησης και διαχείρισης επιβατών
Συστήματα βασικής υποδομής

Συνηθισμένες ευπάθειες

- Παρωχημένα και μη υποστηριζόμενα λειτουργικά συστήματα
- Λογισμικό προστασίας από ιούς που είναι παλιό ή λείπει (συμπεριλαμβανομένου του κακόβουλου λογισμικού)
- Ακατάλληλες ρυθμίσεις ασφαλείας και μη εφαρμογή βέλτιστων πρακτικών
- Ενσωματωμένα δίκτυα υπολογιστών που δεν διαθέτουν τμηματοποίηση δικτύου και σχετικές προστασίες

.

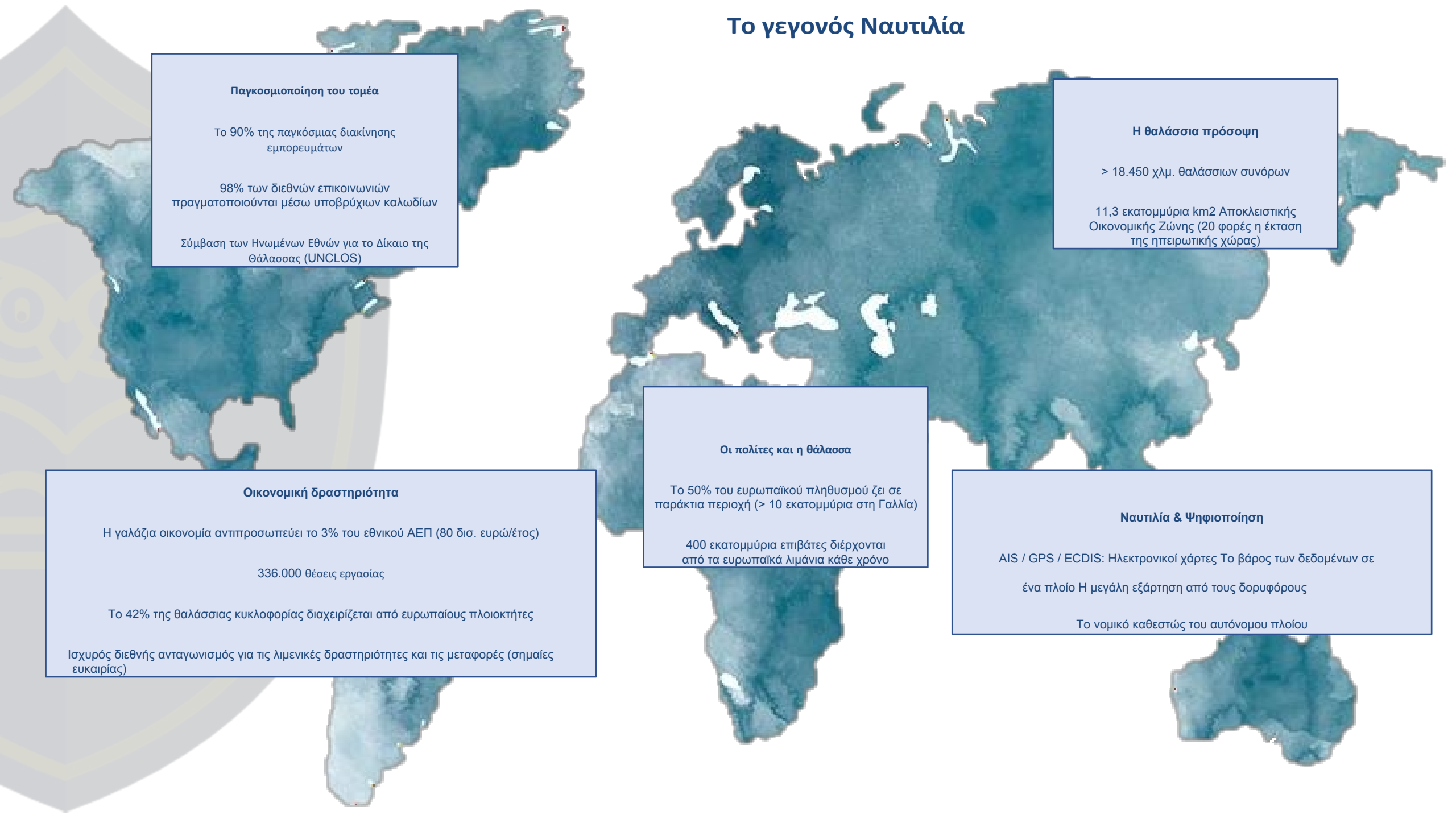
- Ανεπαρκές επίπεδο ασφάλειας για βασικό εξοπλισμό ή συστήματα

που είναι συνδεδεμένα

- Ανεπαρκείς έλεγχοι τρίτων, συμπεριλαμβανομένων των εργολάβων και των παρόχων

.

Το γεγονός Ναυτιλία



Παγκοσμιοποίηση του τομέα

Το 90% της παγκόσμιας διακίνησης εμπορευμάτων

98% των διεθνών επικοινωνιών πραγματοποιούνται μέσω υποβρύχιων καλωδίων

Σύμβαση των Ηνωμένων Εθνών για το Δίκαιο της Θάλασσας (UNCLOS)

Η θαλάσσια πρόσοψη

> 18.450 χλμ. θαλάσσιων συνόρων

11,3 εκατομμύρια km2 Αποκλειστικής Οικονομικής Ζώνης (20 φορές η έκταση της ηπειρωτικής χώρας)

Οικονομική δραστηριότητα

Η γαλάζια οικονομία αντιπροσωπεύει το 3% του εθνικού ΑΕΠ (80 δισ. ευρώ/έτος)

336.000 θέσεις εργασίας

Το 42% της θαλάσσιας κυκλοφορίας διαχειρίζεται από ευρωπαίους πλοιοκτήτες

Ισχυρός διεθνής ανταγωνισμός για τις λιμενικές δραστηριότητες και τις μεταφορές (σημαίες ευκαιρίας)

Οι πολίτες και η θάλασσα

Το 50% του ευρωπαϊκού πληθυσμού ζει σε παράκτια περιοχή (> 10 εκατομμύρια στη Γαλλία)

400 εκατομμύρια επιβάτες διέρχονται από τα ευρωπαϊκά λιμάνια κάθε χρόνο

Ναυτιλία & Ψηφιοποίηση

AIS / GPS / ECDIS: Ηλεκτρονικοί χάρτες Το βάρος των δεδομένων σε

ένα πλοίο Η μεγάλη εξάρτηση από τους δορυφόρους

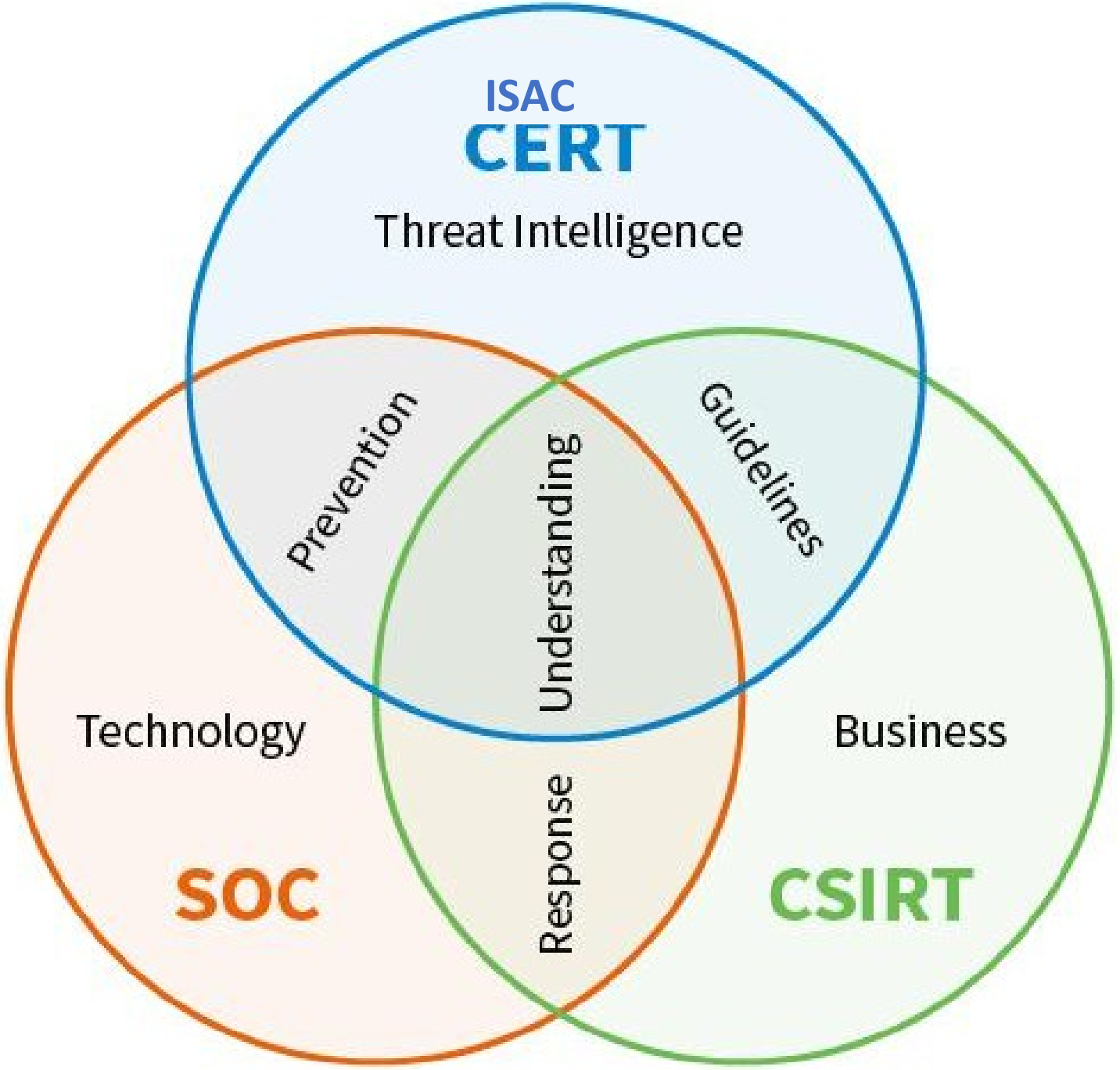
Το νομικό καθεστώς του αυτόνομου πλοίου

Ερώτηση

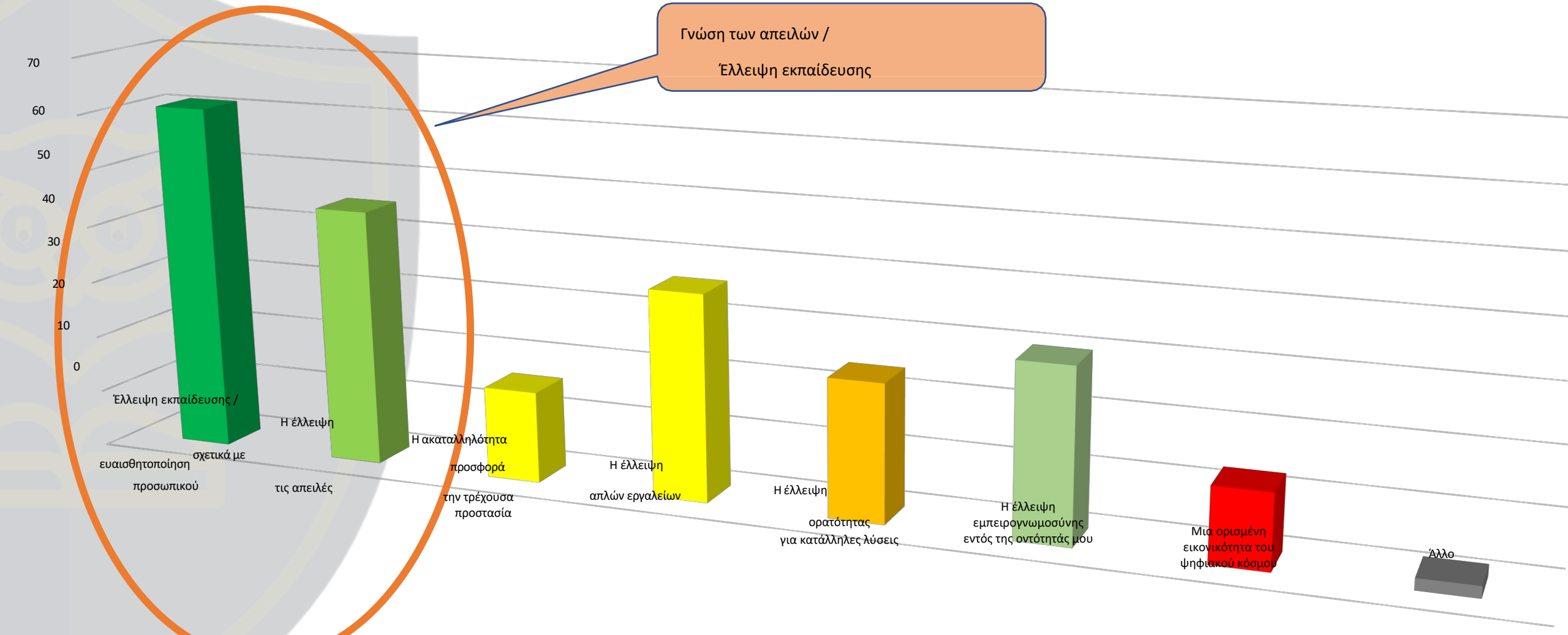
-

Πώς να οργανωθείτε για την αντιμετώπιση απειλών στον κυβερνοχώρο

;



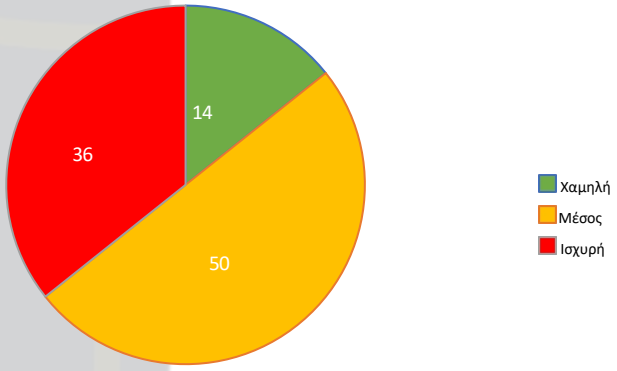
Ποιος είναι ο μεγαλύτερος κίνδυνος όσον αφορά την ασφάλεια στον κυβερνοχώρο;



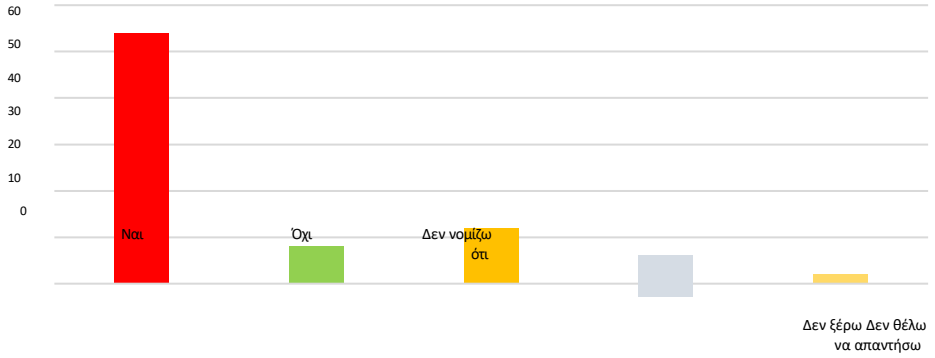
Μελέτη CYBER 2020

Έκθεση του ναυτιλιακού κλάδου - δεδομένα 2020 σε κλίμακα 171 οργανισμών που απάντησαν

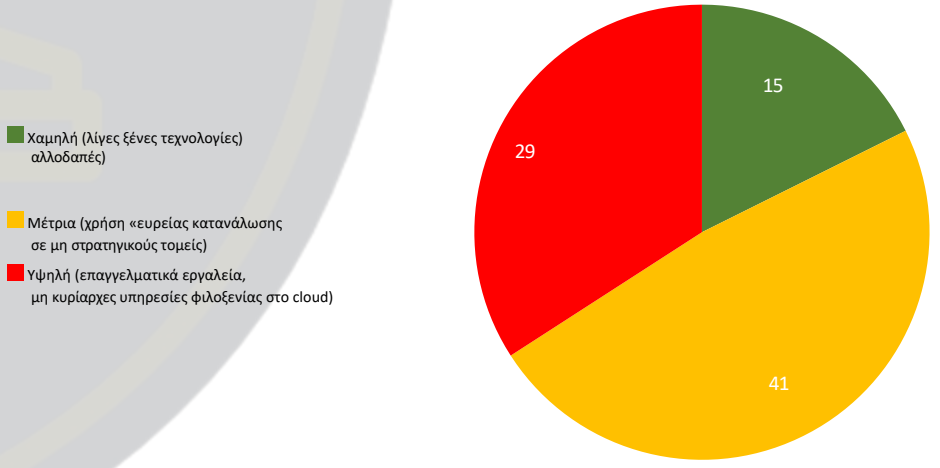
Εκτιμώμενο επίπεδο έκθεσης στην απειλή του κυβερνοχώρου



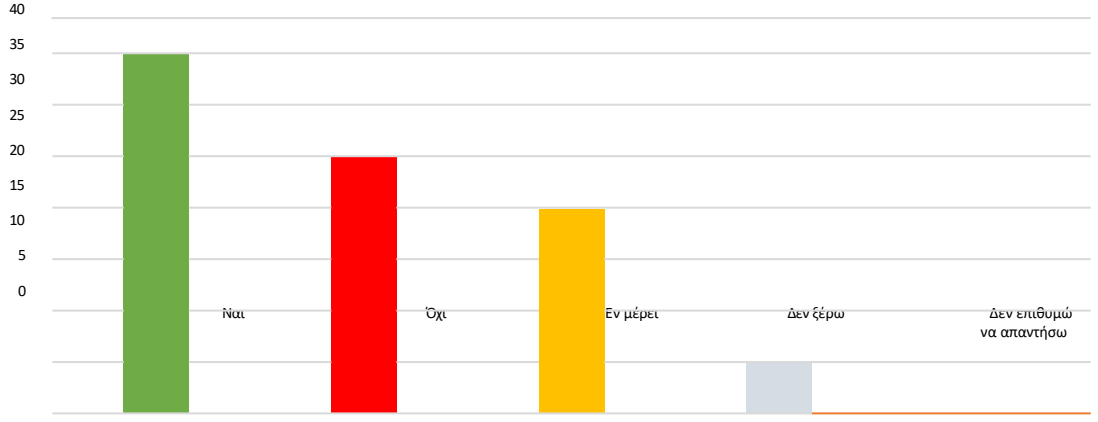
Απόπειρα κυβερνοεπίθεσης κατά του φορέα



Εξάρτηση από ξένες τεχνολογίες



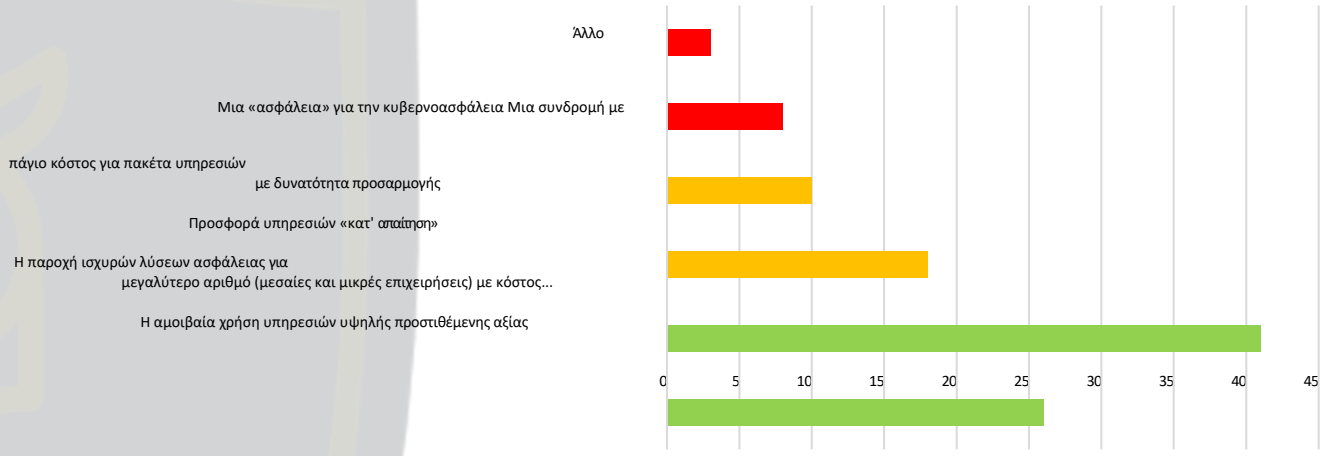
Υπηρεσίες υπεύθυνες για την κυβερνοασφάλεια εντός της οντότητας



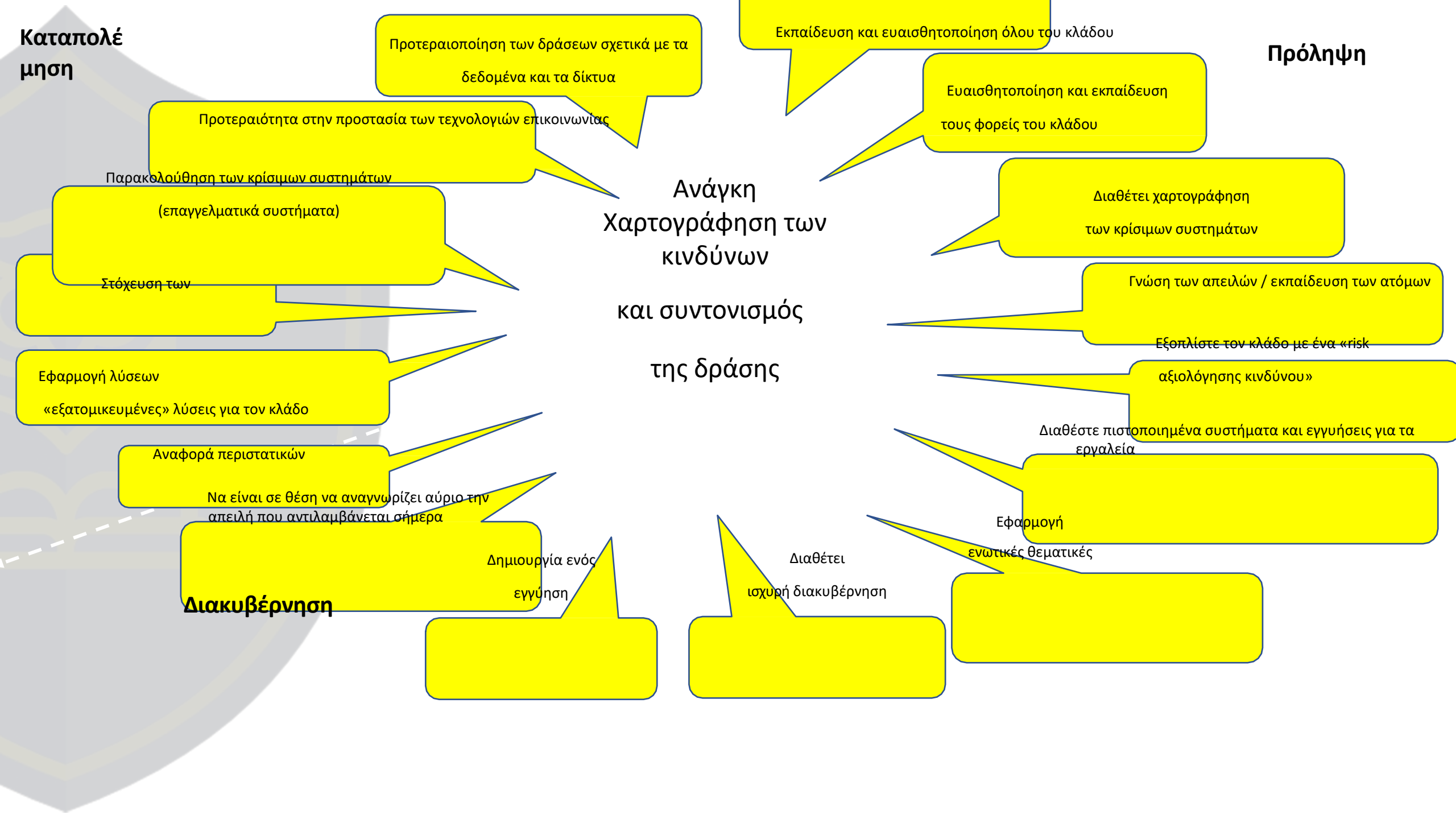
Συντονισμός Κυβερνοχώρου

Επιθυμητά αποτελέσματα

Παράγοντες αποτελεσματικότητας ενός κέντρου κυβερνοασφάλειας

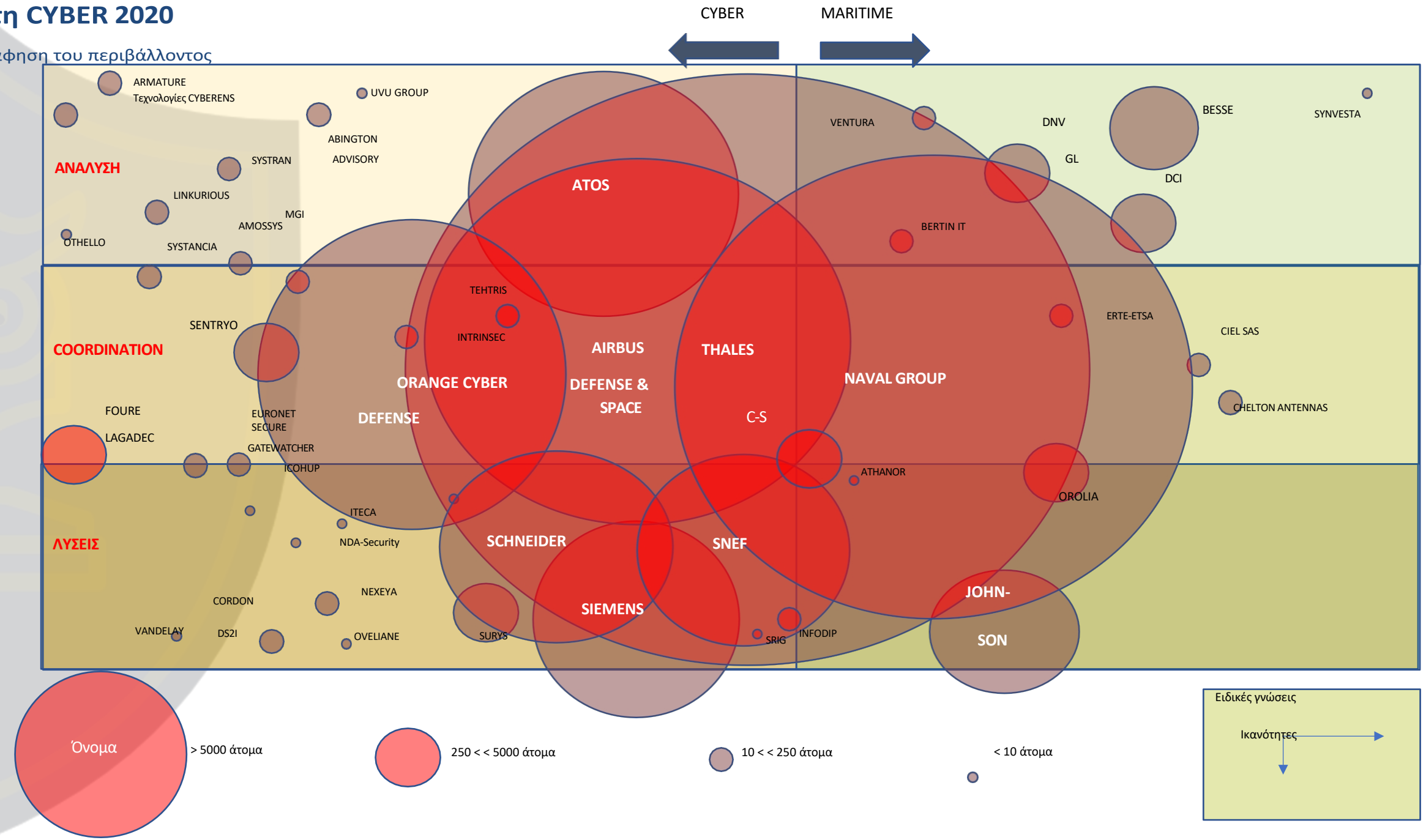


Συμμετοχή στο κέντρο κυβερνοασφάλειας


Καταπολέμηση
Προτεραιοποίηση των δράσεων σχετικά με τα δεδομένα και τα δίκτυα
Προτεραιότητα στην προστασία των τεχνολογιών επικοινωνίας
Παρακολούθηση των κρίσιμων συστημάτων
(επαγγελματικά συστήματα)
Στόχευση των
Εφαρμογή λύσεων
«εξατομικευμένες» λύσεις για τον κλάδο
Αναφορά περιστατικών
Να είναι σε θέση να αναγνωρίζει αύριο την απειλή που αντιλαμβάνεται σήμερα
Διακυβέρνηση
Δημιουργία ενός
εγγύηση
Διαθέτει
ισχυρή διακυβέρνηση
Εφαρμογή
ενωτικές θεματικές
Διαθέστε πιστοποιημένα συστήματα και εγγυήσεις για τα εργαλεία
Εξοπλίστε τον κλάδο με ένα «risk
αξιολόγησης κινδύνου»
Γνώση των απειλών / εκπαίδευση των ατόμων
Διαθέτει χαρτογράφηση
των κρίσιμων συστημάτων
Ευαισθητοποίηση και εκπαίδευση
τους φορείς του κλάδου
Εκπαίδευση και ευαισθητοποίηση όλου του κλάδου
Πρόληψη
Ανάγκη
Χαρτογράφηση των κινδύνων
και συντονισμός
της δράσης

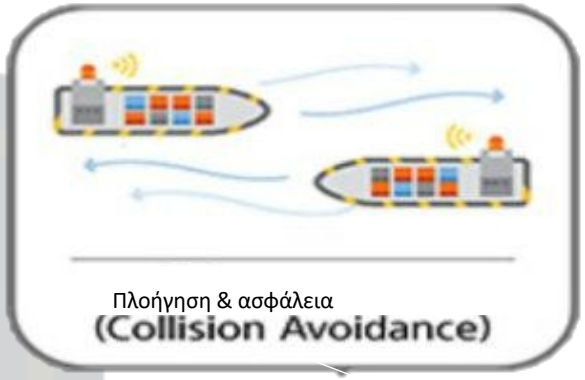
Μελέτη CYBER 2020

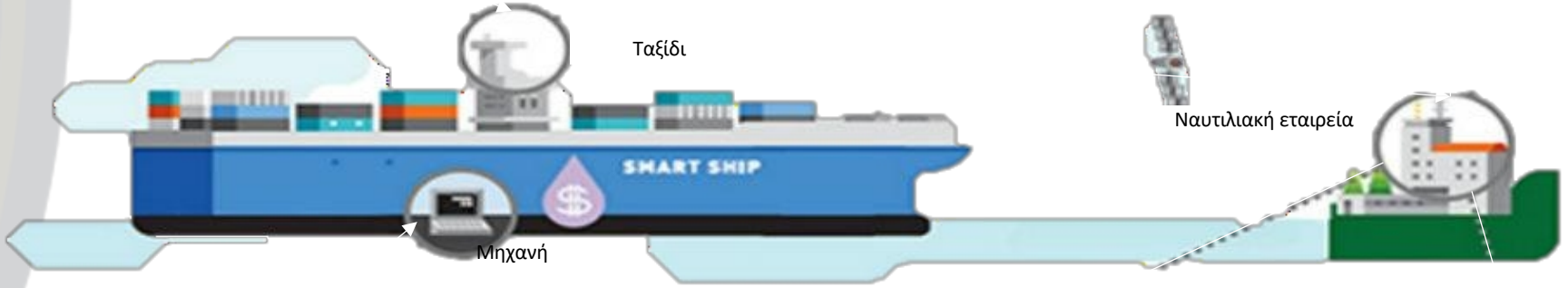
Χαρτογράφηση του περιβάλλοντος

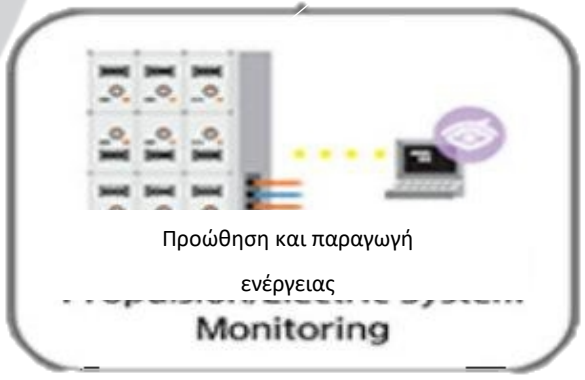


Μελέτη CYBER 2020

Χαρτογράφηση συστημάτων

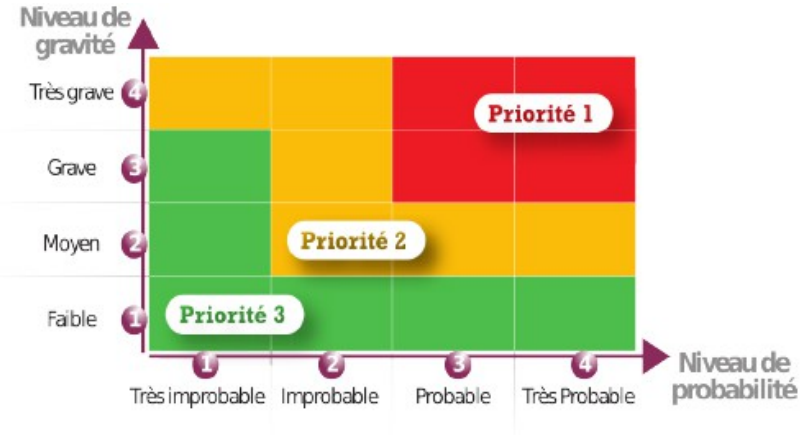






Παρουσίαση από την επιτροπή Ανάλυση κινδύνων

Objectif



- Analyse de risques **sectorielle**
  - Identifier les risques **représentatifs** et **les plus impactants** pour le secteur

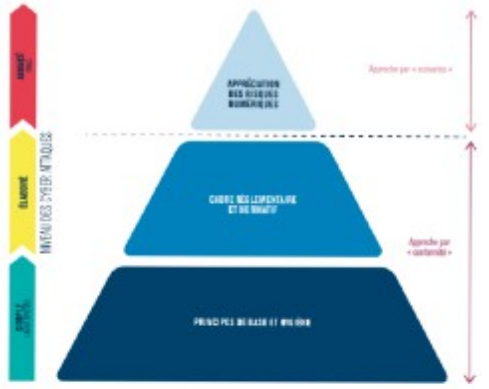
    Opérateur => Secteur => **Missions d'importance Vitale** => **Etat**

  - Disposer d'une cartographie des risques permettant de sensibiliser et d'orienter les actions
  - Recommandations pour compléter la stratégie de cybersécurité maritime du SGMer

Ανάλυση των κινδύνων στον κυβερνοχώρο στον τομέα της ναυτιλίας

EBIOS RISK MANAGER

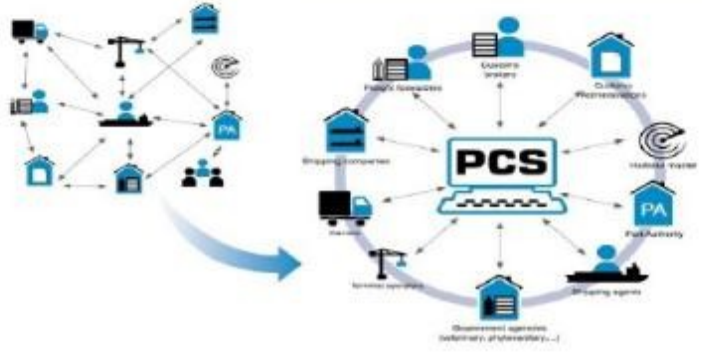
ANSSI



ATELIER 1	ATELIER 2	ATELIER 3	ATELIER 4	ATELIER 5
Cadrage/socle de sécurité	Sources de risque	Scénarios stratégiques	Scénarios opérationnels	Traitement du risque

Périmètre

- Focus sur le « transport maritime » :
  - Compagnies maritimes (marchandises, passagers)
  - Gestion et exploitation d'infrastructures portuaires
  - Fournisseurs de services numériques portuaires (CCS/PCS)



Ανάλυση των κινδύνων στον κυβερνοχώρο στον τομέα της ναυτιλίας

NANTES SAINT-NAZAIRE PORT

COMPAGNIE MARITIME NANTAISE MN

Marseille Fos
Le port euroméditerranéen

SOGET
Fluidity for your business

LE HAVRE port
Connecting Europe

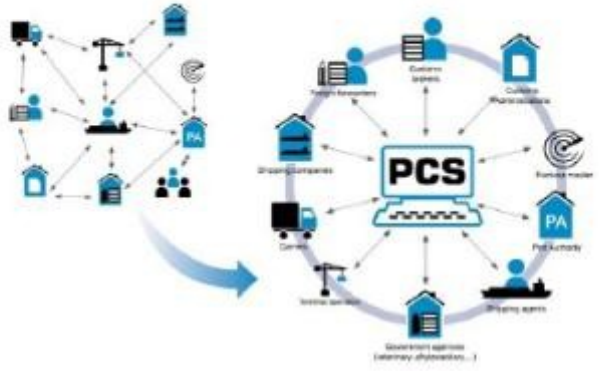
mgi

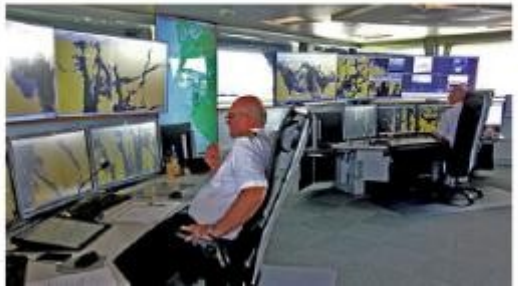
Processus essentiels

Opérateurs	Processus
Compagnies maritimes	*Opération des navires : propulsion, gouverne, navigation, communication, stabilité, énergie…*
	Gestion des marchandises / passagers
	Réservation / Gestion commerciale
	Planification des routes
Ports de commerce	*Gestion des escales*
	Surveillance du trafic (VTS)
	Gestion des infrastructures maritimes (écluses, ponts, bassins...)
	Gestion des marchandises dangereuses
	Gestion de la sûreté et de la sécurité
	GTB – Alimentation électrique
Fournisseur de services numériques portuaires	*Hébergement de services de CCS et PCS*

Evènements redoutés

- +40 identifiés dont 9 jugés critiques ou catastrophiques
- Atteintes à la disponibilité et/ou l'intégrité



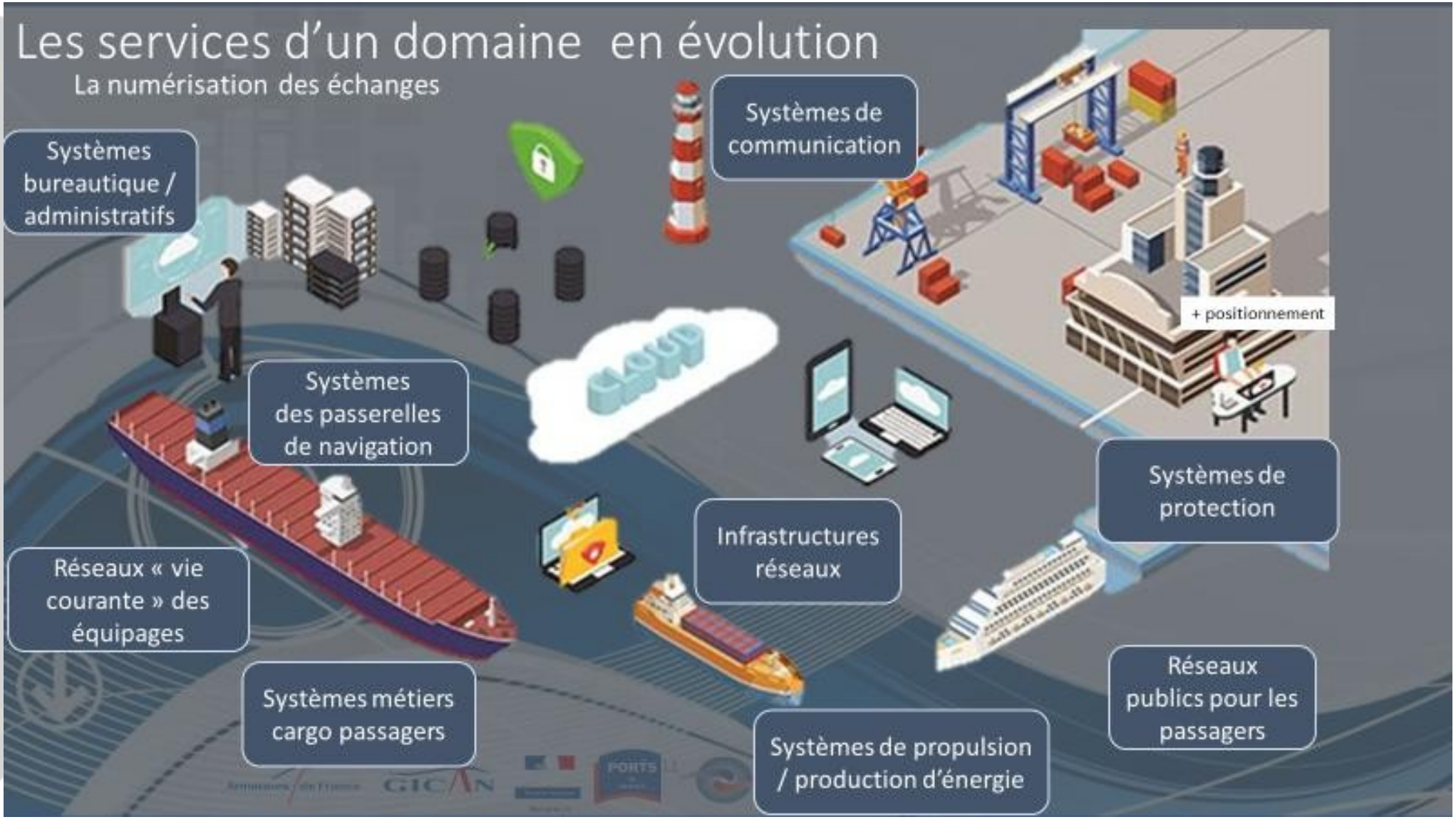


Φοβισμένα σενάρια

Επίθεση
• Συστήματα ΟΤ Πλοίο ή Στόλος • Συστήματα ελέγχου της λιμενικής υποδομής • Σύστημα παρακολούθησης της κυκλοφορίας (VTS) • PCS και CCS

Σαμποτάζ
• Συστήματα ΟΤ Πλοίο ή Στόλος • Συστήματα ελέγχου λιμενικής υποδομής • Σύστημα παρακολούθησης κυκλοφορίας (VTS) • PCS και CCS • Ηλεκτρική τροφοδοσία του λιμένα

Ανάλυση και αποτελέσματα



Στρατηγική για την ασφάλεια στον κυβερνοχώρο στον τομέα της ναυτιλίας

Στρατηγικές κατευθύνσεις

ΟΙ ΚΥΡΙΕΣ ΣΤΡΑΤΗΓΙΚΕΣ ΓΡΑΜΜΕΣ

Μεταφορά των βασικών αρχών της κυβερνοασφάλειας στον ναυτιλιακό και λιμενικό τομέα που έχουν καθοριστεί σε διατομεακό επίπεδο από τον νόμο LPM και την οδηγία NIS σχετικά με:

- ***Τη διακυβέρνηση (γενική πολιτική για την ασφάλεια στον κυβερνοχώρο)***
- ***Την προστασία των δικτύων και των συστημάτων πληροφοριών***
- ***Την άμυνα των δικτύων και των συστημάτων πληροφοριών***
- ***Την ανθεκτικότητα των δραστηριοτήτων***

Καθορισμός δράσεων και καθηκόντων

Πίνακας παρακολούθησης δράσεων/δείκτες

Στρατηγική

Συνυπογραφή SGM / ANSSI

Η κυβερνοασφάλεια στο επίκεντρο των έργων Η ισορροπία του ανταγωνισμού

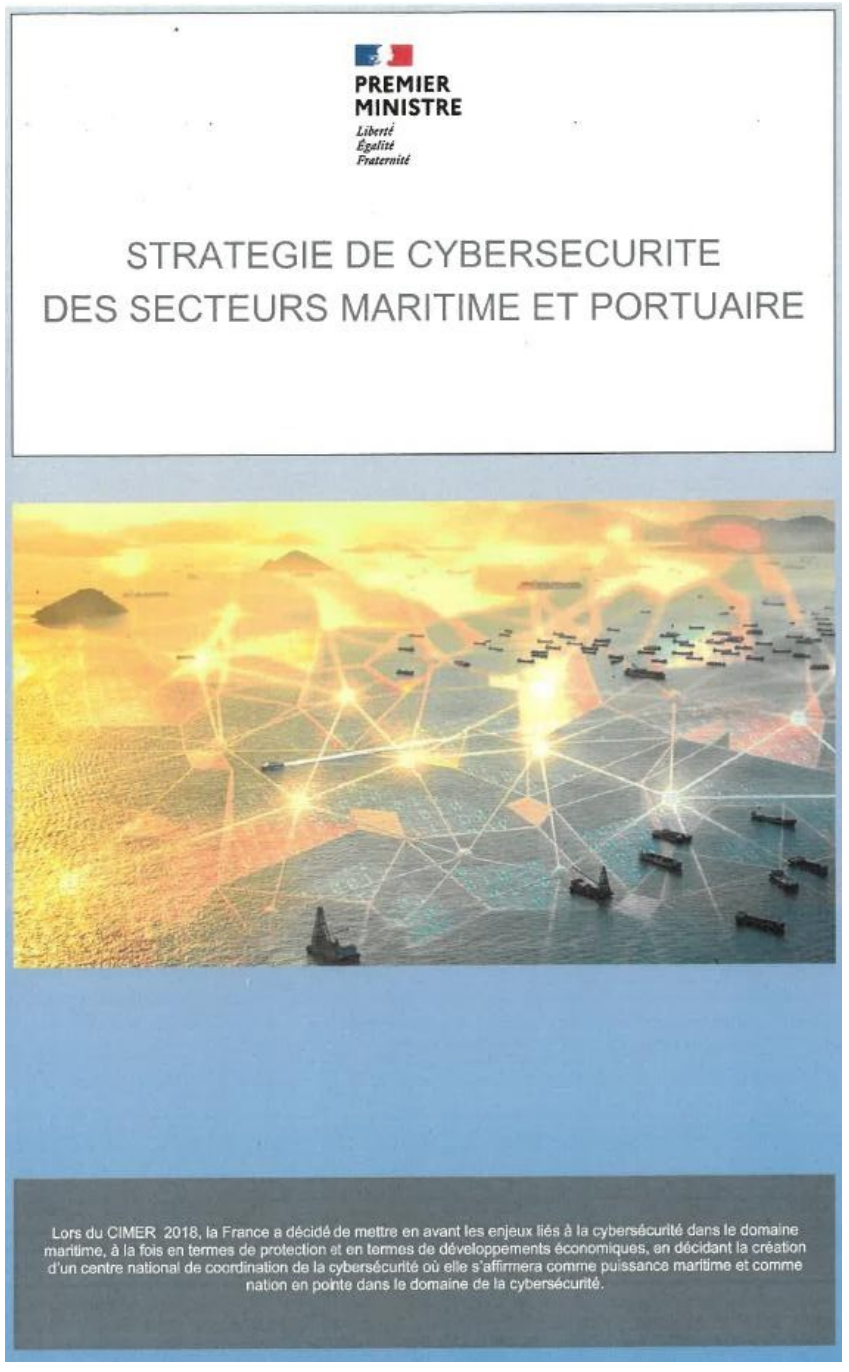
Η ανταλλαγή πληροφοριών

Η πρόκληση της πολυπλοκότητας των συστημάτων

Συμφιλίωση της κυβερνοασφάλειας και της λειτουργικής ασφάλειας

Η κάλυψη των κυβερνοκινδύνων

Πίνακας περιεχομένων



Παρουσίαση της στρατηγικής

Σχέδιο δράσης (1.1 έως 1.7)

Τομέας	Αριθμός δράσης	Δράση	Εργασία(-ες)	Υπεύθυνος	Συνεισφέροντες	Προθεσμία	Σχόλια	Πρόοδος προ
L1: ΔΙΑΚΥΒΕΡΝΗΣΗ	Δράση 1.1	Δημιουργία και προώθηση της διακυβέρνησης της θαλάσσιας κυβερνοασφάλειας	Ανάπτυξη και προώθηση του συμβουλίου για την κυβερνοασφάλεια στον που συστάθηκε το 2019	Γραμματεία του C2M2	Επιτροπές του C2M2	2019		Ολοκληρώθηκε
			Δημιουργία και τήρηση πίνακα παρακολούθησης των δράσεων και των υπευθύνων για αυτές	Γραμματεία του C2M2	Επιτροπές του C2M2	Σεπτέμβριος 21	Αυτός ο πίνακας ελέγχου θα αναθεωρηθεί στις κάθε συνεδρίαση του COMEX	Να ξεκινήσει
	Δράση 1.2	Δημιουργία και διατήρηση χαρτογράφησης των κινδύνων του θαλάσσιου τομέα	Δημιουργία χαρτογράφησης των πληροφοριακών συστημάτων που χρησιμοποιούνται στον τομέα της ναυτιλίας και των λιμένων, πριν από τη χαρτογράφησης των κινδύνων.	Επιτροπή ανάλυσης Κίνδυνοι C2M2	Όλοι οι φορείς σχετικοί κίνδυνοι του ναυτιλιακού	Ιανουάριος 2022	Καθορισμός του πεδίου εφαρμογής και εμβάθυνση της ανάλυσης κοινή χρήση πληροφοριών	ξεκίνησε
			Δημιουργία και ενημέρωση χαρτογράφησης των κινδύνων στον κυβερνοχώρο του ναυτιλιακού κόσμου.	Επιτροπή ανάλυσης κινδύνων C2M2	Όλοι οι σχετικοί σχετικοί φορείς του ναυτιλιακό	Ιούνιος 2022		Να ξεκινήσει
	Δράση 1.3	Εφαρμογή και εφαρμογή για τον ναυτιλιακό τομέα της εθνικοί δείκτες κυβερνοασφάλειας για την παρακολούθηση των πολιτικών και την αξιολόγηση της αποτελεσματικότητάς τους.	Ανάπτυξη δεικτών παρακολούθησης των δράσεων της της παρούσας στρατηγικής	Επιτροπές του C2M2	Επιτροπές του C2M2	Απρίλιος 2022	Προσθήκη στήλης δεικτών στον παρόντα πίνακα	Να ξεκινήσει
			Ενημέρωση του πίνακα ελέγχου της εξέλιξης των δεικτών	Επιτροπές του C2M2	Επιτροπές του C2M2	Απρίλιος 2022	Μόνιμη δράση	Να ξεκινήσει
			Ετήσια ανασκόπηση των δεικτών και εξέταση των δράσεων που πρέπει να αναληφθούν αναλόγως	COMEX του C2M2	Επιτροπές του C2M2	Απρίλιος 2022	Συνάντηση του COMEX	Να ξεκινήσει
	Δράση 1.4	Συντονισμός των θέσεων και την δράση της Γαλλίας των εταίρων της διεθνείς	Συνεισφορά στη σύνταξη ανακοινώσεων και προτάσεις προς τον IMO	DGITM/DAM (πλοία) DGITM/DST (λιμάνια)	C2M2	Δράση μόνιμη	Το C2M2 συντονίζει, αλλά το Η επικύρωση είναι διαυπουργική και η RP στον IMO.	ξεκίνησε
			Συμβολή στις ευρωπαϊκές εργασίες μέσω των ομάδων εργασία της ΕΚ (π.χ. MARSEC, ομάδα συνεργασίας NIS, ECGFF Cybersecurity WG)	Επιτροπών C2M2	SGMER, MIMER, MTE, ANSSI, μόνιμη επιτροπή France Maritime	Δράση μόνιμη		ξεκίνησε
	Δράση 1.5	Υλοποίηση δράσεων ευαισθητοποίησης σχετικά με κυβερνοασφάλειας και δημιουργία πλαίσιο κατάρτισης απευθυνόμενο σε όλους τους επαγγέλματα του ναυτιλιακού τομέα	Προσδιορισμός των υφιστάμενων προσφορών και υποβολή τους στον τομέα ναυτιλιακούς οδηγούς (FR, EE)	France Cyber Ναυτιλία	C2M2 DGITM/DAM (πλοία) DGITM/DST (λιμάνια)	Μάρτιος 2022	Ενημέρωση των οδηγών καλών πρακτικών υφιστάμενες πρακτικές	Να ξεκινήσει
			Ανάπτυξη πλατφόρμας ευαισθητοποίησης CYBER ναυτιλιακού τομέα σε σχέση με τις εθνικές και υφιστάμενες ευρωπαϊκές	France Cyber Maritime	C2M2 DGITM/DAM (πλοία) DGITM/DST (λιμάνια)	Ιούνιος 2022	Σε σχέση με Cybermalveillance.gouv.fr	Να ξεκινήσει
	Δράση 1.6	Οργάνωση και έλεγχος του ανταλλαγή πληροφοριών για όλους τους φορείς	Εκδώστε ένα ενημερωτικό δελτίο C2M2 cyber ανά έτος (γενικά θέματα και διεθνή επικαιρότητα, έργα)	Γραμματεία του C2M2	Επιτροπές C2M2	Τριμηνιαία	Ξεκίνησε το 2018 · επισημοποίηση της πεδίο εφαρμογής αυτής της επιστολής με την FCM	Ολοκληρώθηκε
			Ανάπτυξη και δημοσίευση τεχνικών δελτίων	France Cyber Maritime	ANSSI (CERT-FR)		Σύμφωνα με το πρόγραμμα που θα καταρτιστεί από τη France Cyber Maritime	Να ξεκινήσει

Παρουσίαση της στρατηγικής

Σχέδιο δράσης (2.1 έως 2.4)

Τομέας	Αριθμός δράσης	Δράση	Καθήκον(τα)	Υπεύθυνος	Συνεισφέροντες	Προθεσμία	Σχόλια	Πρόοδος προ
L2: ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ	Δράση 2.1	Ανάλυση των αναγκών των νομοθετικών και κανονιστικών εξελίξεων που ισχύουν στον ναυτιλιακό τομέα	Συμπεράσματα από την ανάλυση των κινδύνων, συμπεριλαμβανομένων των εμπειριών από περιστατικά ασφάλειας, προκειμένου να καθοριστούν οι ανάγκες για αλλαγές.	Επιτροπή Προοπτικής και Ρύθμισης C2M2	France Cyber Maritime, Επιτροπή Ανάλυσης Κινδύνων	Μόνιμη δράση		Να ξεκινήσει
			Παρακολούθηση των εξελίξεων των διεθνών κειμένων και προτύπων που ενδέχεται να δικαιολογούν την αναθεώρηση των εθνικών κειμένων εθνικών	Επιτροπή Προοπτικής και ρύθμισης C2M2	DGITM/DAM (πλοία) DGITM/DST (λιμάνια) ANSSI	Δράση μόνιμη		ξεκίνησε
	Δράση 2.2	Συμβολή στη δημιουργία ενός πλαισίου πιστοποίησης/σήμανσης προϊόντων και υπηρεσιών που ανταποκρίνονται στις ανάγκες του ναυτιλιακού τομέα	Υποστήριξη μιας διαδικασίας πιστοποίησης/σήμανσης ενώπιον του ΔΝΟ σε συνεργασία με τις διοικήσεις και τα νηογνώμονα με βάση τις υπάρχουσες εργασίες υφιστάμενων	MIMER / DAM	DGITM/DAM (πλοία) DGITM/DST (λιμάνια) ANSSI	2024	Σημειώστε τις δράσεις που πραγματοποιήθηκαν κατά τη διάρκεια του έτους	Να ξεκινήσει
	Δράση 2.3	Καθορισμός ενός πλαισίου αναφοράς για τη συστηματική συνεκτίμηση της κυβερνοασφάλειας στα σχέδια σχεδιασμού και κατασκευής πλοίων και λιμενικών υποδομών	Ανάπτυξη της «κυβερνοασφάλειας από το σχεδιασμό» μεταξύ των βιομηχανικών φορέων	Επιτροπή Προοπτικής και Ρύθμισης C2M2	GICAN ANSSI	Μόνιμη δράση	Σημειώστε τις δράσεις που πραγματοποιήθηκαν κατά τη διάρκεια του έτους	Να ξεκινήσει
			Ενσωμάτωση της ασφάλειας στον κυβερνοχώρο στις σκέψεις για την ανάπτυξη του αυτόνομου πλοίου	Επιτροπή Προοπτικής και ρύθμισης C2M2	DGITM / DAM CLUSTER MARITIME ANSSI	Δράση μόνιμη	Στο πλαίσιο του ΔΝΟ διεξάγονται συζητήσεις στις ομάδες που ασχολούνται με τα αυτόνομα πλοία.	Να ξεκινήσει
	Δράση 2.4	Διεξαγωγή ειδικών έργων για την ασφάλεια των βασικών συστημάτων	Ενσωμάτωση των κινδύνων παρεμβολών και παραπλάνησης των GNSS και των συνεπειών τους σε συστήματα όπως το AIS ή τις πληροφορίες PNT	Επιτροπή ανάλυσης Κινδύνων C2M2	DGITM CNES ANFR	Σεπτέμβριος 22	Διαυπουργική ομάδα εργασίας - Παρεμβολές AIS / GNSS	ξεκίνησε
			Συνέχιση της ασφάλειας των συστημάτων πλοήγησης	Επιτροπή ανάλυσης κινδύνου C2M2	CNES CCTA	2024		Πρόκειται να ξεκινήσει
			Συμβολή στην ασφάλεια των λιμενικών συστημάτων και των συστημάτων διαχείρισης εμπορευμάτων	Μεγάλα θαλάσσια λιμάνια	Γαλλία PCS	2024	Τριετές πρόγραμμα PIA	Πρόκειται να ξεκινήσει
			Συνέχιση της ανάπτυξης της ασφάλειας των ηλεκτρικών δικτύων των λιμένων	Μεγάλα θαλάσσια λιμάνια	Γαλλία PCS	2024	Τριετές πρόγραμμα PIA	Πρόκειται να ξεκινήσει
			Προώθηση της εφαρμογής λύσεων παρακολούθησης και ανίχνευσης περιστατικών ασφαλείας στα λιμενικά συστήματα	Μεγάλα θαλάσσια λιμάνια	France Cyber Maritime MICA	2024		Να ξεκινήσει

Παρουσίαση της στρατηγικής

Σχέδιο δράσης (δράσεις 3.1, 4.1 και 4.2)

Τομέας	Αριθμός δράσης	Δράση	Καθήκον(τα)	Υπεύθυνος	Συνεισφέροντες	Προθεσμία	Σχόλια	Πρόοδος
L3: ΥΠΕΡΑΣΠΙΣΗ ΤΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ	Δράση 3.1	Συνοδεία των φορέων του ναυτιλιακού τομέα στην εφαρμογή διαδικασιών παρακολούθησης, ανίχνευσης και αντιμετώπισης περιστατικών κυβερνοασφάλειας.	Προώθηση της αναφοράς περιστατικών στους των φορέων του ναυτιλιακού τομέα	France Cyber maritime	C2M2 MICA Center	Δεκέμβριος-2021	Υπάρχουν ήδη υποχρεώσεις αναφοράς (LPM, NIS). Το 2018, η DAM εξέδωσε έναν οδηγό που διανεμήθηκε σε όλους τους πλοιοκτήτες.	Προς έναρξη
			Ανάπτυξη και εφαρμογή μηχανισμών καταγραφής περιστατικών	France Cyber maritime	MICA Center ANSSI (CERT-FR)	Δεκέμβριος 2021		Να ξεκινήσει
			Δημιουργία ενός CERT Maritime	France Cyber Maritime	Κέντρο MICA ΘΑΛΑΣΣΙΑ ΧΑΡΜΑΡΙΑ ANSSI	Δεκέμβριος 2023		Να ξεκινήσει
L4: ΑΝΘΕΚΤΙΚΟΤΗΤΑ ΤΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ	Δράση 4.1	Οργάνωση της ανθεκτικότητας του τομέα	Εφαρμογή και δοκιμή διαδικασιών διαχείρισης κρίσεων.	Γραμματεία του C2M2	France Cyber Maritime ANSSI	Δεκέμβριος 2021	Καθορισμός στόχων, πεδίων εφαρμογής και αλληλεπιδράσεων με τα υπάρχοντα προγράμματα	Να ξεκινήσει
			Ανάπτυξη του συντονισμού μεταξύ των φορέων και ανάπτυξη της ανταλλαγής βέλτιστων πρακτικών.	Γραμματεία του C2M2	France Cyber Maritime ANSSI	Δεκέμβριος 2021		Να ξεκινήσει
	Δράση 4.2	Σε συνεργασία με τους τομείς της ναυτιλίας και των λιμένων, διοργάνωση ασκήσεων αντιμετώπισης κυβερνοκρίσεων	Καθιέρωση προγραμματισμού ασκήσεων για τους θαλάσσιους και λιμενικούς τομείς, σε συνάρτηση με τις μεγάλες εθνικές ασκήσεις.	Γραμματεία του C2M2	France Cyber Maritime ANSSI	Κάθε δύο χρόνια	Καθιέρωση προγράμματος ασκήσεων για τους τομείς της ναυτιλίας και των λιμένων.	Να ξεκινήσει
			Διανομή σε όλους τους ενδιαφερόμενους της ανάλυσης των συμπερασμάτων των ασκήσεων και των επακόλουθων ενεργειών.	Γραμματεία του C2M2	France Cyber Maritime ANSSI	Κάθε δύο χρόνια		Να ξεκινήσει

**"I'm applying for the Information Security position.
Here is a copy of my resumé, encoded, encrypted and shredded."**