CyberSecPro

EDUCATION AND TRAINING

CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training

Funded by the European Union

Ασφάλεια κρίσιμων υποδομών για τη ναυτιλία

Μάθημα

CSP008_C_M

ΠΑΡΟΥΣΙΑΣΗ ΑΠΟ: BRUNO BENDER

CyberSecPro

CyberSecPro creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity.

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Κίνδυνοι για τις κρίσιμες υποδομές της ναυτιλίας

01. Προσδιορισμός των κινδύνων για την ασφάλεια στον κυβερνοχώρο για τις κρίσιμες θαλάσσιες υποδομές

02. Ετήσιο μάθημα στο πλαίσιο των ναυτιλιακών εργαστηρίων – δια ζώσης - Τουλόν)

03. Κρίσιμες υποδομές, OES, ναυτιλιακοί φορείς

04. Εθνικές ιδιαιτερότητες – οδηγία NIS

05. Σημασία των δεδομένων (EUCI, ευαίσθητα δεδομένα κ.λπ.)

06. Αξιολόγηση και μετριασμός κινδύνων (π.χ. κρυπτογραφία)

07. C2B Consulting

115 rue du maréchal Foch –F83.200 LE REVEST – Γαλλία

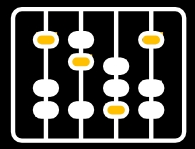
CyberSecPro
CC BY NC SA

Στόχοι: Αυτή η ενότητα, που έχει σχεδιαστεί για τους φορείς του ναυτιλιακού τομέα, στοχεύει στον εντοπισμό των κινδύνων για τις κρίσιμες υποδομές, με σκοπό τη βελτίωση της ανθεκτικότητάς τους.

ΠΟΙΟΙ

Κρίσιμες υποδομές και OES όπως προσδιορίζονται στην οδηγία NIS.

ΤΙ



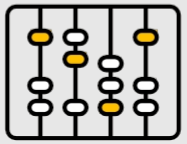
Βασικά στοιχεία της διαχείρισης κινδύνων στον τομέα της ασφάλειας στον κυβερνοχώρο στον ναυτιλιακό τομέα

ΓΙΑΤΙ

Εξοπλισμός των συμμετεχόντων με τις γνώσεις και τις δεξιότητες που απαιτούνται για τη διαχείριση των κινδύνων στον τομέα της ασφάλειας στον κυβερνοχώρο

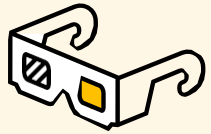
CSP Εκπαίδευση Logistics: CSP003_ ΚΙΝΔΥΝΟΙ ΤΩΝ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ ΣΤΗΝ ΝΑΥΤΙΛΙΑ

Π



Χρονοδιάγραμμα: Φθινόπωρο 2024 – Φθινόπωρο 2025

ΠΟΥ

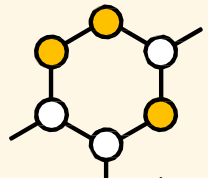


Επί τόπου

Τουλόν (Γαλλία) NMIOTC

(Ελλάδα)

ΠΩΣ



- Θεωρία
- Πρακτική εκπαίδευση

ΠΟΙΟΣ

Προφίλ των συμμετεχόντων στην εκπαίδευση

- Διευθυντές και ηγέτες
- Επαγγελματίες
- Μικρομεσαίες επιχειρήσεις και υπάλληλοι του δημόσιου τομέα
- ~~Επαγγελματίες και ενθουσιώδες στον τομέα της κυβερνοασφάλειας~~
- ~~Προγραμματιστές CIS στον τομέα της ναυτιλίας~~

Ποιος

Προφίλ του εκπαιδευτή

- Bruno BENDER
- C2B CONSULTING
- Πρώην αξιωματικός του Πολεμικού Ναυτικού / Ειδικός CIS
- Υπεύθυνος ασφάλειας πληροφοριών
  - ΝΑΤΟ
  - Σε εθνικό επίπεδο
  - Ε
- Από το 2017 Ειδικός σε θέματα κυβερνοασφάλειας και ιδρυτής της C2B
- ΜΜΕ ειδικευμένη στη θαλάσσια ασφάλεια / κυβερνοασφάλεια υποστήριξη
  - Κρίσιμες υποδομές
  - Διαχειριστές βασικών υπηρεσιών
  - Ναυτιλιακές εταιρείες και λιμάνια
  - Δημόσιες διοικήσεις που δραστηριοποιούνται στη θάλασσα

CSP0008_C_M_ΚΙΝΔΥΝΟΙ ΤΩΝ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ ΤΗΣ ΘΑΛΑΣΣΙΑΣ ΜΕΤΑΦΟΡΑΣ: ΠΡΟΤΥΠΟ ΠΑΡΟΥΣΙΑΣΗΣ ΠΟΥ ΔΗΜΙΟΥΡΓΗΘΗΚΕ ΑΠΟ ΤΟ PR

TI

Θέματα εκπαίδευσης

- Ποιος είναι ο ορισμός της κρίσιμης υποδομής
- Κοινότητες χρηστών
- Τεχνικές αρχιτεκτονικές / ΥΠΟΔΟΜΕΣ
  - Διοικήσεις
  - Τεχνική περιγραφή
- Κίνδυνοι
- Σχεδιασμός αρχιτεκτονικής ασφάλειας
- Εφαρμογή ασφάλειας
- Μέτρα μετριασμού

ΓΙΑ

Μαθησιακά αποτελέσματα

- Επίδειξη ηθικής και επαγγελματικής συμπεριφοράς σε όλες τις πτυχές της διαχείρισης πληροφοριών και της ασφάλειας στον κυβερνοχώρο.
- Κατανόηση και διατύπωση των βασικών εννοιών και αρχές της πληροφορικής και της ασφάλειας στον κυβερνοχώρο.
- Κατανόηση του εξελισσόμενου τοπίου των κυβερνοαπειλών και του ευρέος φάσματος των κυβερνοεπιθέσεων.
- Προσδιορίζει τις απειλές, τις ευπάθειες και τους κινδύνους για την ασφάλεια στον κυβερνοχώρο που αντιμετωπίζει ένας οργανισμός.
- Αναγνωρίζει τον ρόλο του ανθρώπινου παράγοντα στις παραβιάσεις της κυβερνοασφάλειας και στις στρατηγικές μετριασμού των κινδύνων.
- Ικανότητα να βοηθά και να επιλέγει τα κατάλληλα μέτρα ασφαλείας για την προστασία από αναγνωρισμένες απειλές και κινδύνους στον κυβερνοχώρο.

Θέμα 1:
Κίνδυνοι στον τομέα της ασφάλειας στον κυβερνοχώρο στον ναυτιλιακό τομέα

Θα καλύψουμε τις ακόλουθες δεξιότητες

- Εισαγωγή στην ασφάλεια των πληροφοριών: Σε αυτή την ενότητα θα παρουσιάσουμε την έννοια της ασφάλειας των πληροφοριών και τη σημασία της για τους οργανισμούς. Θα συζητήσουμε επίσης τους διαφορετικούς τύπους πληροφοριών που πρέπει να προστατεύονται, καθώς και τις διάφορες απειλές και ευπάθειες που αντιμετωπίζουν αυτές οι πληροφορίες.
- Εισαγωγή στην κυβερνοασφάλεια: Σε αυτή την ενότητα θα επικεντρωθούμε στις συγκεκριμένες απειλές και ευπάθειες που υπάρχουν στον κυβερνοχώρο. Θα συζητήσουμε επίσης τους διαφορετικούς τύπους κυβερνοεπιθέσεων που μπορούν να πραγματοποιηθούν, καθώς και τους διαφορετικούς τρόπους μετριασμού αυτών των επιθέσεων.
- Η τριάδα CIA: Σε αυτή την ενότητα θα συζητηθούν οι τρεις πυλώνες της ασφάλειας των πληροφοριών: εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα. Θα εξηγηθεί τι σημαίνει κάθε πυλώνας και γιατί είναι σημαντικός.
- Άλλα μοντέλα ασφάλειας: Σε αυτή την ενότητα θα συζητηθούν άλλα μοντέλα ασφάλειας που μπορούν να χρησιμοποιηθούν για την προστασία των πληροφοριών. Αυτά τα μοντέλα περιλαμβάνουν το πλαίσιο κυβερνοασφάλειας NIST, το πρότυπο ISO/IEC 27001 και το πλαίσιο COBIT.

Θέμα-2:

Απειλές και ευπάθειες

Θα καλύψουμε τις ακόλουθες δεξιότητες

- 1. AIS: Τι είναι μια κρίσιμη υποδομή – Νομική χρήση και ιδιαιτερότητες
- 2. Περιγραφή ενός πλαισίου CI που περιλαμβάνει υλικό, λογισμικό και δίκτυα.
- 3. Τρόποι με τους οποίους απειλούνται οι κρίσιμες υποδομές
- Επιτιθέμενοι
- Μέτρα μετριασμού
- 4. Σχέδια και δράσεις ανθεκτικότητας
- Άλλα

Θέμα-3:
Περιπτώσεις χρήσης

Θα καλύψουμε τις ακόλουθες δεξιότητες

- 1. Εθνικά σχέδια
- 2. Τοπικά μέτρα μετριασμού
- 3. Εκπαίδευση / Κατάρτιση
- 4. Έρευνες και διδάγματα από το παρελθόν
- 5. Απειλές και κίνδυνοι
- 5. Μέτρα μετριασμού
  - - Τεχνικά
  - - Οργανωτικά
  - - Ασφαλιστικά

CyberSecPro

EDUCATION AND TRAINING

CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training

Funded by the European Union

Ασφάλεια κρίσιμων υποδομών για τη ναυτιλία

Μάθημα

CSP0008_C_M

ΠΑΡΟΥΣΙΑΣΗ ΑΠΟ: BRUNO BENDER

Ασφάλεια κρίσιμων υποδομών για τη ναυτιλία

Θέμα 1 – Γενικά δεδομένα

- Ναυτιλία / Πλαίσιο κυβερνοασφάλειας
- Κυβερνοασφάλεια και τεχνολογία

Κυβερνοασφάλεια – όχι μόνο τεχνολογία

Υπηρεσίες

Υπηρεσίες προστασίας

EU CERT-M

Τεχνική

Παρακολούθηση τέλους/τέλους
Προσαρμοστική συντήρηση

Οργανωτική

Θαλάσσια κυβερνοκυβέρνηση

Σημασιολογία

Αξιολόγηση και διαχείριση κινδύνων, αναφορά περιστατικών, κοινή χρήση αναλύσεων

ETSI GS ISI 00X: «Δείκτες ασφάλειας πληροφοριών (ISI)…”

Νομικά

Εμπορικά ευαίσθητα δεδομένα, δεδομένα προσωπικού, θέσεις,

Θαλάσσια Κίνδυνος κυβερνοασφάλειας

Στόχος

Το μάθημα C2B_CSP008 έχει ως στόχο να περιγράψει τους κινδύνους για την ασφάλεια στον κυβερνοχώρο στο ναυτιλιακό περιβάλλον και να προσδιορίσει τις ιδιαιτερότητές του.

Έμφαση δίνεται στα πρότυπα και τις ιδιαιτερότητες του AIS, καθώς και στη διεθνή νομοθεσία. Αναλύονται λεπτομερώς οι κοινές ευπάθειες των συστημάτων και εφαρμογών AIS/GNSS.

Μέθοδοι Παραδείγματα και του hacking και spoofing του αυτών των συστημάτων παρουσιάζονται παρουσιάζονται κατά τη διάρκεια του μαθήματος.

Παρουσιάζονται η ανάλυση κινδύνων, τα σχέδια ασφάλειας, οι πολιτικές και οι διαδικασίες, το κανονιστικό πλαίσιο και τα πρότυπα ασφάλειας, καθώς και τα μέτρα συνέχειας και αποκατάστασης.

Ναυτιλιακή ασφάλεια στον κυβερνοχώρο
Κυβερνοασφάλεια Κίνδυνος

Κίνδυνος κυβερνοασφάλειας για τη ναυτιλία

- Παγκόσμια εικόνα
- Επιθέσεις / Περιστατικά
- Εξελίξεις

Κίνδυνος στον ναυτιλιακό τομέα / Μετριασμοί Ποια συστήματα

Κυβερνοασφάλεια της ακτοφυλακής της ΕΕ

Επιτεύγματα - Η συνέχιση των τρεχουσών προσπαθειών

Αξιοποίηση της πρωτοβουλίας των εργαστηρίων ECGFF με θέμα «Πρόληψη κυβερνοεπιθέσεων στον θαλάσσιο τομέα», που ξεκίνησε η γερμανική προεδρία, και δημιουργία «Ομάδας εργασίας για την ασφάλεια στον κυβερνοχώρο της ακτοφυλακής της ΕΕ».

Ανάγκη περαιτέρω ανάπτυξης κοινής προσέγγισης της κυβερνοασφάλειας για την κοινότητα της ακτοφυλακής. Για τον σκοπό αυτό, θα αναπτυχθεί περαιτέρω η νομική, οργανωτική και τεχνική κατανόηση, βελτιώνοντας παράλληλα τη διατομεακή και διασυνοριακή συνεργασία και εκπονούμε κατευθυντήριες γραμμές και βέλτιστες πρακτικές διαχείρισης προς τον σκοπό αυτό.

Ενθάρρυνση της κοινότητας της ακτοφυλακής στον τομέα της κυβερνοασφάλειας και εφαρμογή μιας πλατφόρμας ανταλλαγής πληροφοριών αφιερωμένης στην κυβερνοασφάλεια, η οποία θα φιλοξενείται από τον EMSA.

Συναινετική επικύρωση των όρων αναφοράς της «Ομάδας Εργασίας για την Κυβερνοασφάλεια της Ακτοφυλακής της ΕΕ»

που απευθύνεται στην Ευρωπαϊκή Επιτροπή (ΓΔ MARE).

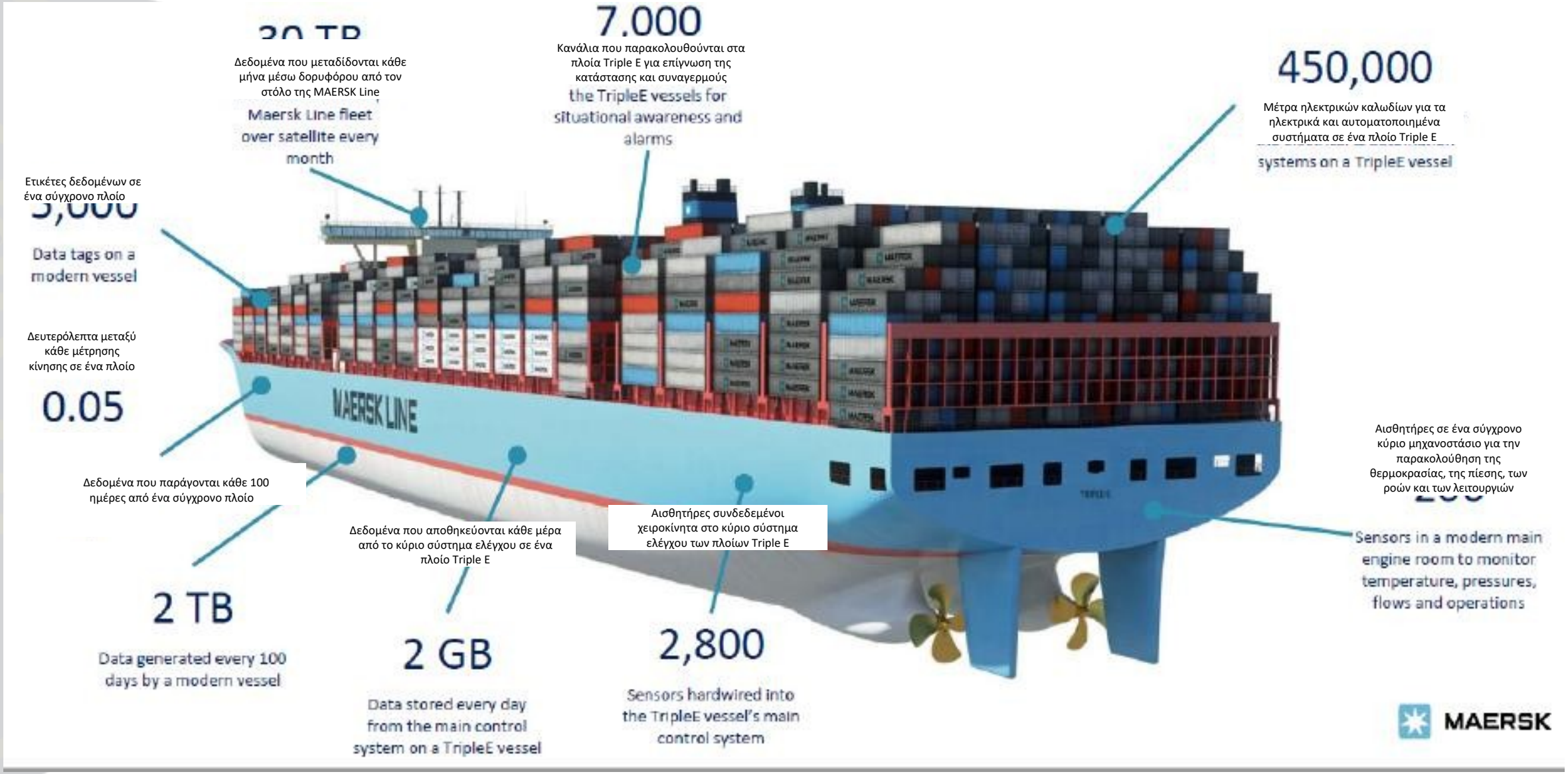
Υποστήριξη για περαιτέρω βελτιώσεις στις διαδικασίες ανταλλαγής πληροφοριών για την έγκαιρη ανταλλαγή πληροφοριών σχετικά με κυβερνοεπιθέσεις και συμβάντα που στοχεύουν τη ναυτιλιακή κοινότητα.

Συνέχιση κατά τη διάρκεια της κροατικής προεδρίας της ECGFF (2019-2020).

Κυβερνοασφάλεια στη ναυτιλία

- **Απειλή για την ασφάλεια στον κυβερνοχώρο στον ναυτιλιακό τομέα**
- Ναυτιλιακά δεδομένα
- Παγκόσμια εικόνα
- Επιθέσεις / Περιστατικά
- Κίνδυνοι

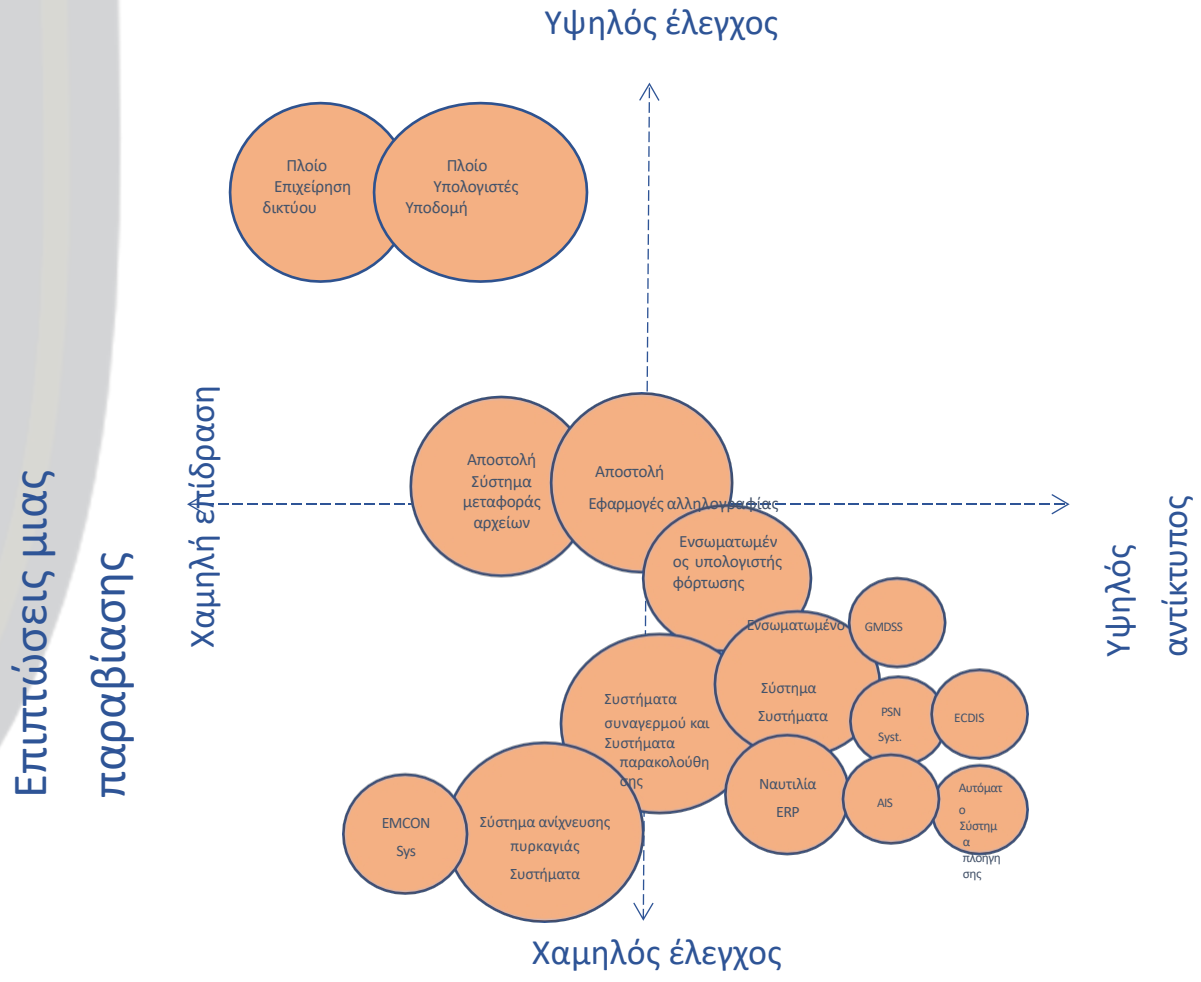
Ο κίνδυνος των δεδομένων στη ναυτιλία



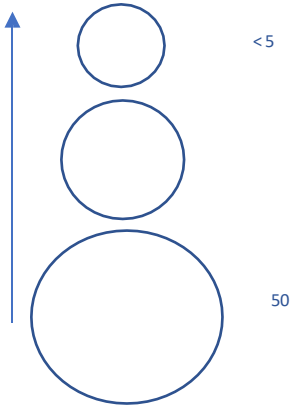
Κρίσιμες υποδομές - Ναυτιλιακές αρχές

Έλεγχος της ασφάλειας / Επιπτώσεις των συμβάντων

Έλεγχος της ασφάλειας από τον πλοιοκτήτη



Αριθμός χρηστών / επηρεαζόμενων συστημάτων



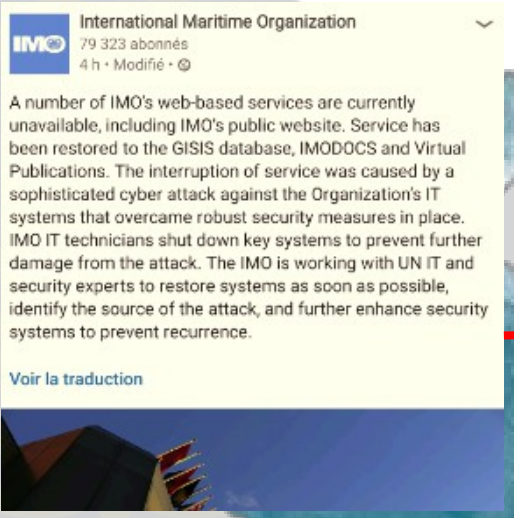
Ασφάλεια κρίσιμων υποδομών για τη ναυτιλία

Θέμα 2 – Απειλές και ευπάθειες

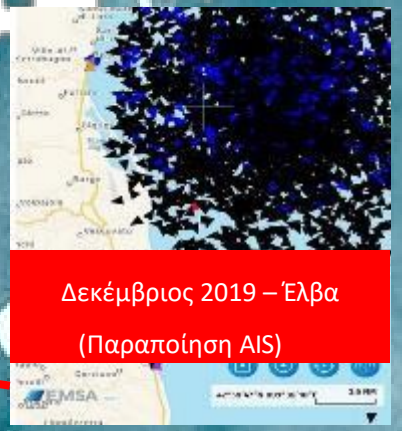
- Χαρτογραφία των θαλάσσιων συστημάτων
- Απειλές – Παγκοσμίως
- Παρατηρηθέντα συμβάντα

Απειλές – Σημαντικές επιθέσεις 2020 – 2023

Παγκοσμίως



Μάρτιος 2020 – Ελβετία (MSC)



Δεκέμβριος 2019 – Έλβα

(Παραποίηση AIS)

Απρίλιος 2020 – Ορμούζ Μπαντάρ Αμπάς

Σεπτέμβριος 2020 – Int (CMA-CGM)

Μάρτιος 2020 – Μασσαλία / FOS – Περιφερειακή επίθεση

2020 – Μεσόγειος (Brouillage GPS)

Ιανουάριος 2020 – Κίνα (Παραποίηση AIS)

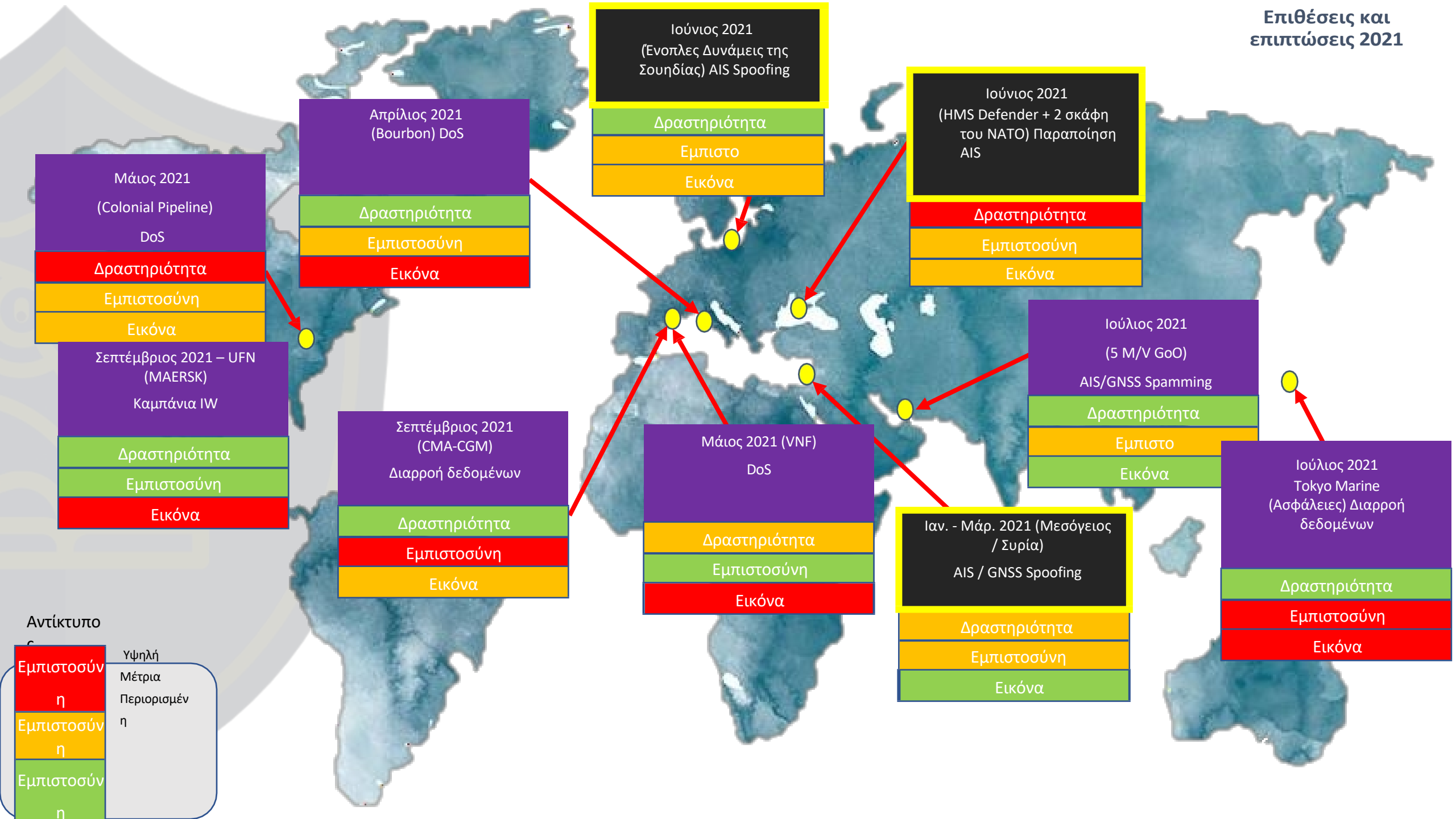
Μάιος 2020 – Καλιφόρνια (Spoofing AIS)

Σεπτέμβριος 2020 – Int (GEFCO)

Επιθέσεις / περιστατικά (2020 – 22)

Οντότητα	Ημερομηνία	Επιπτώσεις	Ανάλυση
Λιμάνι Μπαντάρ Αμπάς	2020	Αδυναμία υλοποίησης τερματικών σταθμών φόρτωσης και εκφόρτωσης	Σκόπιμη **στοχοποίηση ενός «μη κρίσιμου» λιμανιού από μια χώρα** σε προληπτική επίθεση που έχει ως αποτέλεσμα άμεση αντίδραση
MSC	2020	Μη λειτουργικές υπηρεσίες (>12 ώρες) Η ιστοσελίδα και η διεπαφή πελατών ήταν απρόσιτες για αρκετές ημέρες σε ορισμένες περιοχές	**Οι τοπικά φιλοξενούμενες υπηρεσίες** επέτρεψαν στον χειριστή να συνεχίσει να λειτουργεί σε ορισμένες περιοχές
MED EUROPE TERMINAL	20	Αποκλεισμένες υπηρεσίες διαδικτύου που επηρέασαν την διαδικτυακή πύλη και την ανταλλαγή μηνυμάτων.	Ο ναυτιλιακός φορέας ήταν το **παράπλευρο θύμα** μιας επίθεσης στην νότια περιοχή κατά τη διάρκεια της περιορισμού της
GNSS/AIS	2018 - 2020	Κορεσμός των δεκτών AIS (παρατηρήθηκε στη Μεσόγειο το 2019, στην Κίνα και στις ΗΠΑ το 2020) Μόνιμη παρεμβολή GPS στην Ανατολική Μεσόγειο, την Κίνα και τη Μαύρη Θάλασσα	Η παρεμβολή ή η πλαστογράφηση (κορεσμός) των συστημάτων GNSS/AIS αποτελεί πραγματικό **κίνδυνο για τη ναυσιπλοΐα**. Οι επιθέσεις στα συστήματα GNSS/AIS, που παρατηρούνται στις πιο ωμές μορφές τους, μπορούν τελικά **να παραμορφώσουν όλα τα ναυτιλιακά δεδομένα**.
CARNIVAL	20	Απώλεια δεδομένων πελατών και υπαλλήλων. Απώλεια δραστηριότητας στην κρουαζιέρα (κρατήσεις)	Κλασική επίθεση ransomware που κρυπτογράφησε μέρος των συστημάτων και των δεδομένων της CIS και μπλόκαρε τη δραστηριότητα για αρκετές ώρες.
CMA / CGM	20	Δεδομένα και υπηρεσίες μη προσβάσιμα λόγω του tiocryptolocker Απώλεια πελατών	Η επίθεση αντιμετωπίστηκε σε περισσότερο από 2 εβδομάδες από ειδικούς **που δεν ήταν εξοικειωμένοι με το CIS της εταιρείας**. Η επικοινωνία πρέπει να επικεντρώνεται στις προτεραιότητες των χειριστών.
BENETEAU	2021	Επίθεση σε συστήματα και απώλεια δεδομένων	Η BENETEAU δέχτηκε επίθεση για πρώτη φορά το 2018 και έχασε δεδομένα (λίστες πελατών) για δεύτερη φορά σε λιγότερο από 3 χρόνια
BOURBON	2021	Επίθεση στο κύριο σύστημα εκμετάλλευσης	Προβλήματα στη διαχείριση των αλλαγών πληρωμάτων και της καθημερινής δραστηριότητας και των αναφορών για τα πλοία.
GAZOCEAN	20	Πρόεδρος Rip-Off	Οικονομική απώλεια
VNF	2021	Επίθεση στο κύριο σύστημα πληροφοριών	Το σύστημα διαχείρισης παρέμεινε μπλοκαρισμένο για αρκετές ημέρες
Λιμάνι του Αμπιτζάν	2021	Λογισμικό εκβιασμού MATRIX	Περιορισμένες επιπτώσεις στη θαλάσσια κυκλοφορία μετά από συντονισμένη αντίδραση
DNV-GL	20	Κατασκοπεία για λογαριασμό του κράτους - Κλοπή δεδομένων Εικόνα της απομιμωμένης κοινωνίας	Οι ταξικές κοινωνίες εκτίθενται συχνά σε αυτού του είδους τον κίνδυνο λόγω των πληροφοριών στις οποίες έχουν πρόσβαση

Επιθέσεις και επιπτώσεις 2021



Επίθεση CMA / CGM 2020

Édition du jeudi 31 octobre 2024
Feuilleter l'édition

LA LETTRE

La Matinale | Se connecter | S'abonner

Menu | À la Une | Action publique | Entreprises | Médias | Paris-Bruxelles | Enquêtes | Entourages | Mouvements | Feuilletons

L'enquête sur la cyberattaque de CMA CGM avance à grands pas

Si la plupart des enquêtes sur les rançongiciels échouent à identifier les hackers, les cybergendarmes ont arrêté en Ukraine des suspects dans l'attaque qui a ciblé le transporteur maritime CMA CGM en 2020. L'enquête en cours confirme les premières pistes sur le gang Ragnar Locker. [...]

Publié le 07/12/2021 à 6h30 • Lecture 2 minutes

Créez une veille sur les mots-clés cités dans cet article

Agence Nationale de la Securite des Systemes d'Information

CMA CGM

Η έρευνα για την κυβερνοεπίθεση κατά της CMA CGM προχωρά με γρήγορους ρυθμούς Ενώ οι περισσότερες έρευνες για ransomware δεν καταφέρνουν να εντοπίσουν τους χάκερ, η κυβερνοαστυνομία συνέλαβε υπόπτους στην Ουκρανία για την επίθεση που είχε ως στόχο τη ναυτιλιακή εταιρεία CMA CGM το 2020. Η έρευνα που βρίσκεται σε εξέλιξη επιβεβαιώνει τις πρώτες ενδείξεις για τη συμμορία Ragnar Locker. [...]

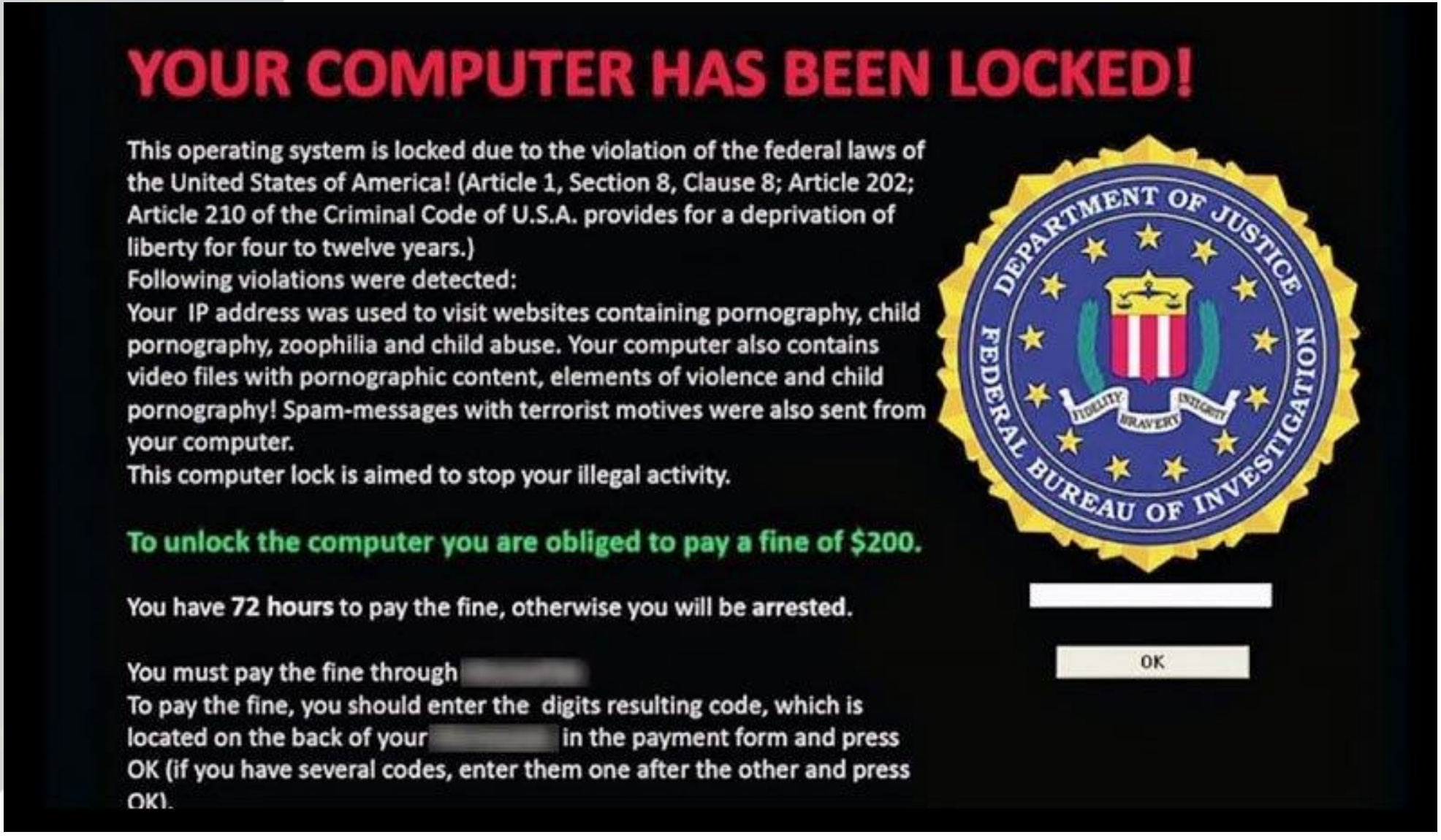
Περίπτωση χρήσης - ransomware

- **Τι είναι το «ransomware»**
  - Κακόβουλο λογισμικό που απειλεί με ζημιές εάν δεν καταβληθεί λύτρα

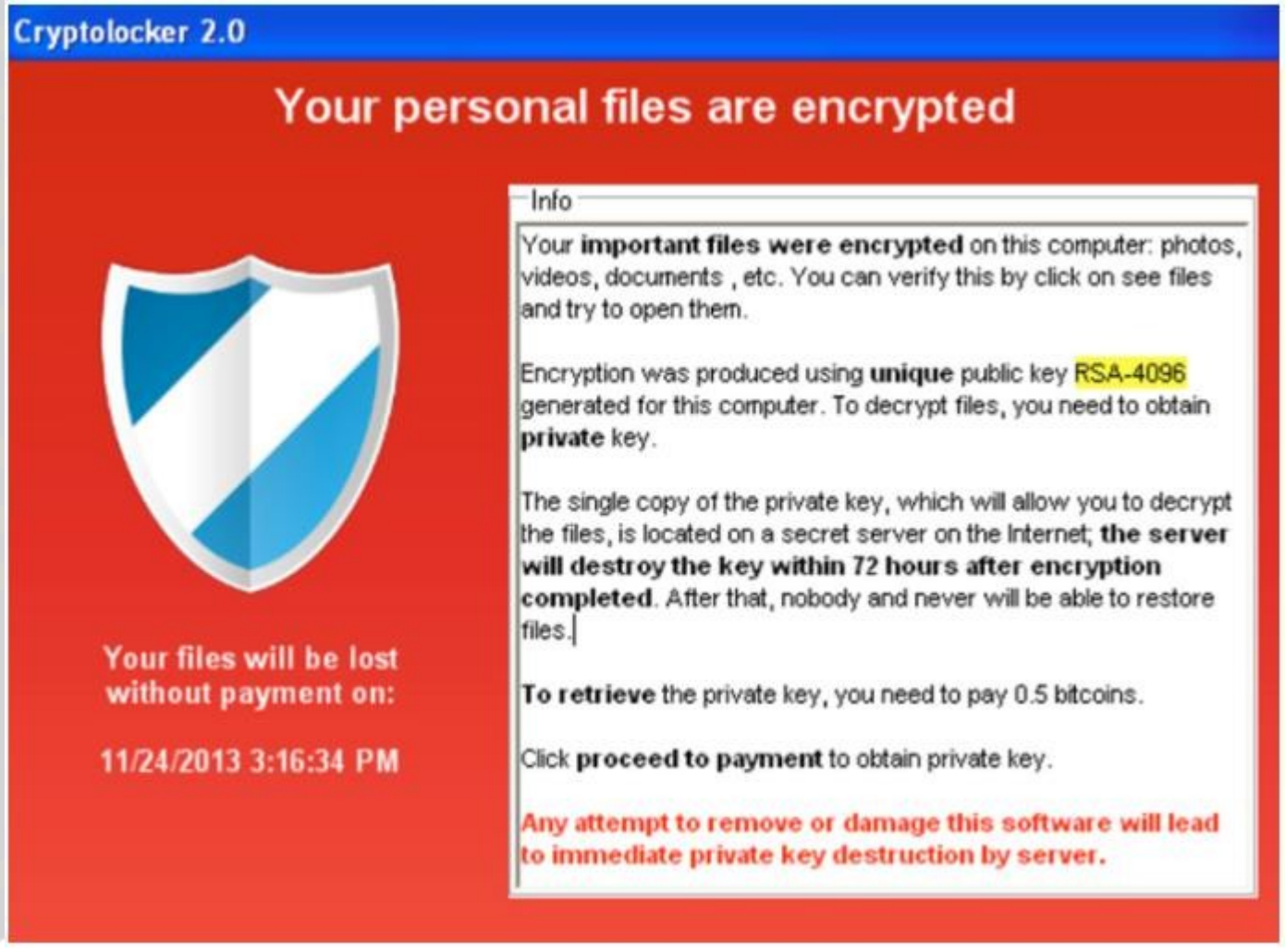
- **Τύποι**
  - *Κλείδωμα οθόνης*
  - *Κρυπτογράφηση αρχείων*
  - *DDOS*
  - *Συνδυασμός*

Πηγή: Trend Micro

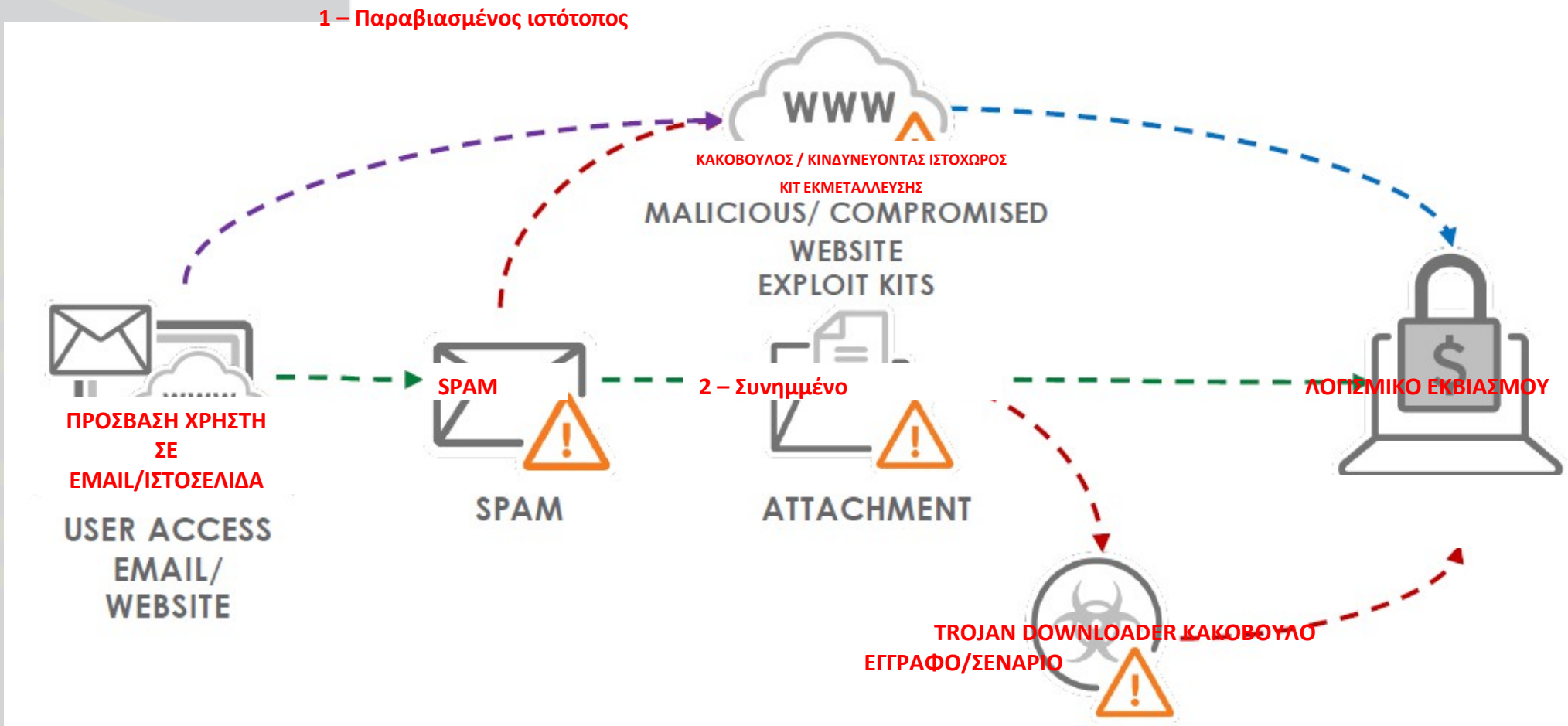
ΕΙΣΑΓΩΓΗ – Κλείδωμα οθόνης



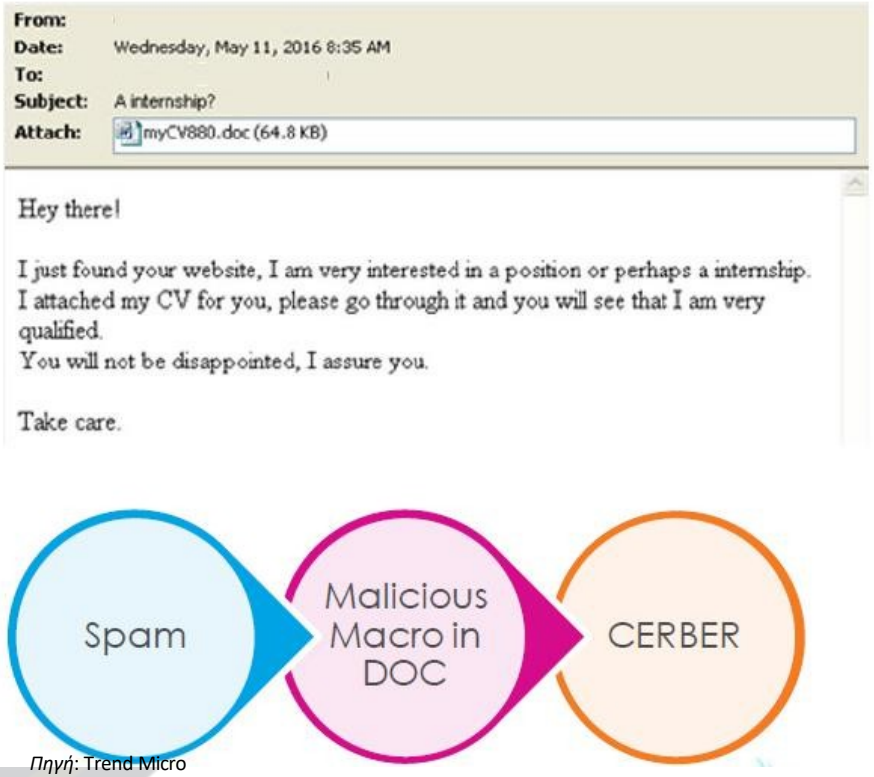
ΕΙΣΑΓΩΓΗ – Κρυπτογράφος αρχείων

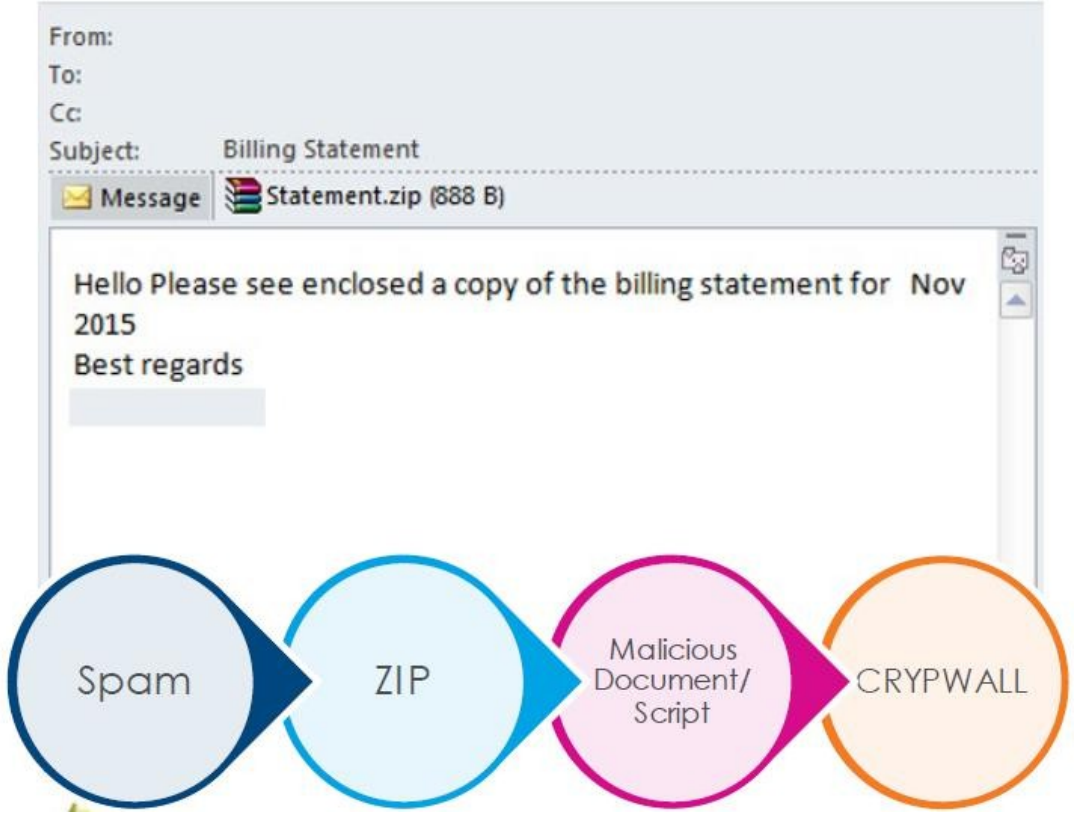


«ΚΟΙΝΟΣ» ΔΙΑΔΡΟΜΟΣ ΕΙΣΟΔΟΥ



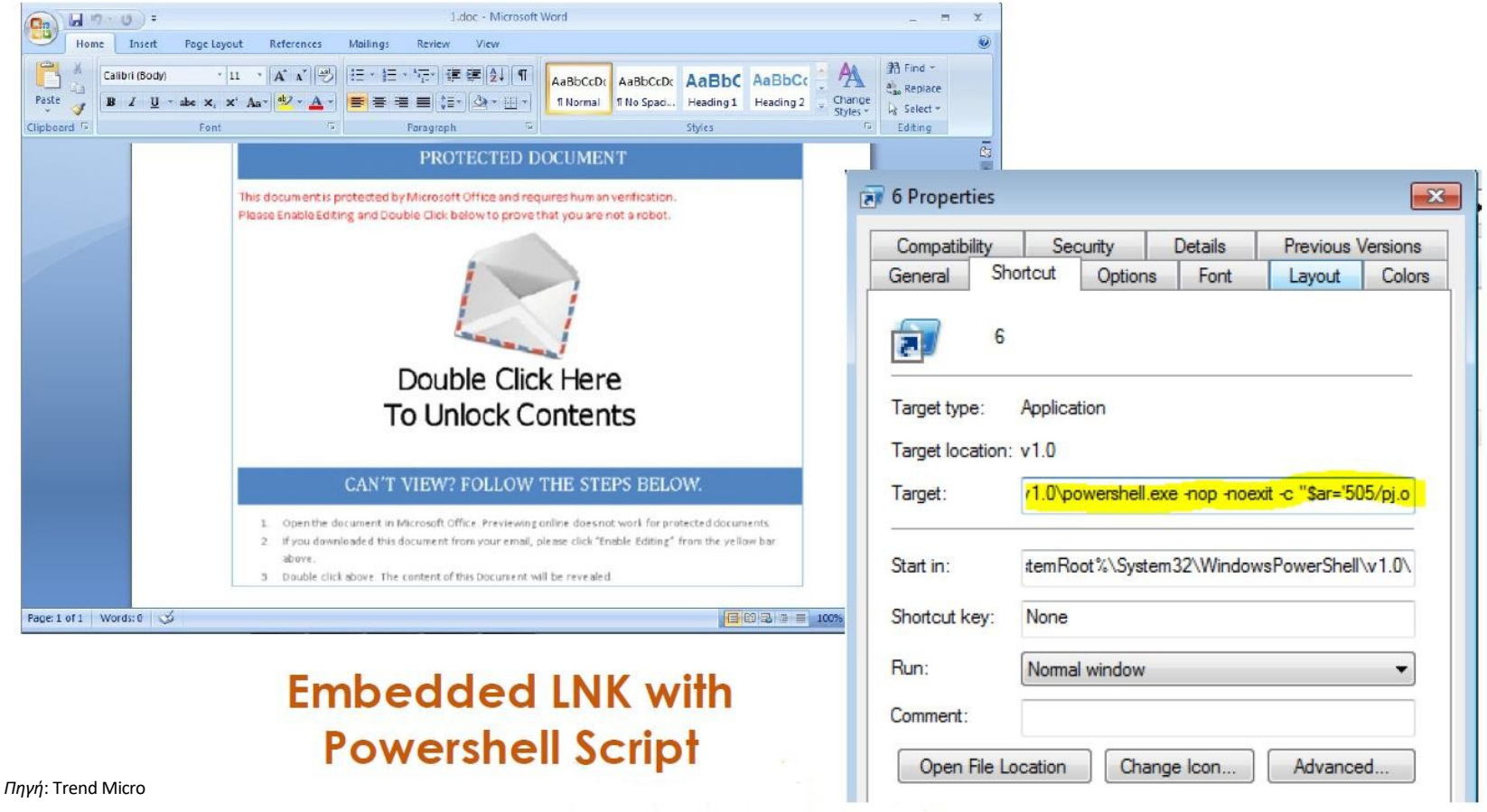
«ΚΟΙΝΟΣ» ΦΟΡΤΕΙΟΣ ΑΦΙΞΗΣ





Πηγή: Trend Micro

«ΚΟΙΝΟΣ» ΦΟΡΤΕΙΟΣ ΑΦΙΞΗΣ



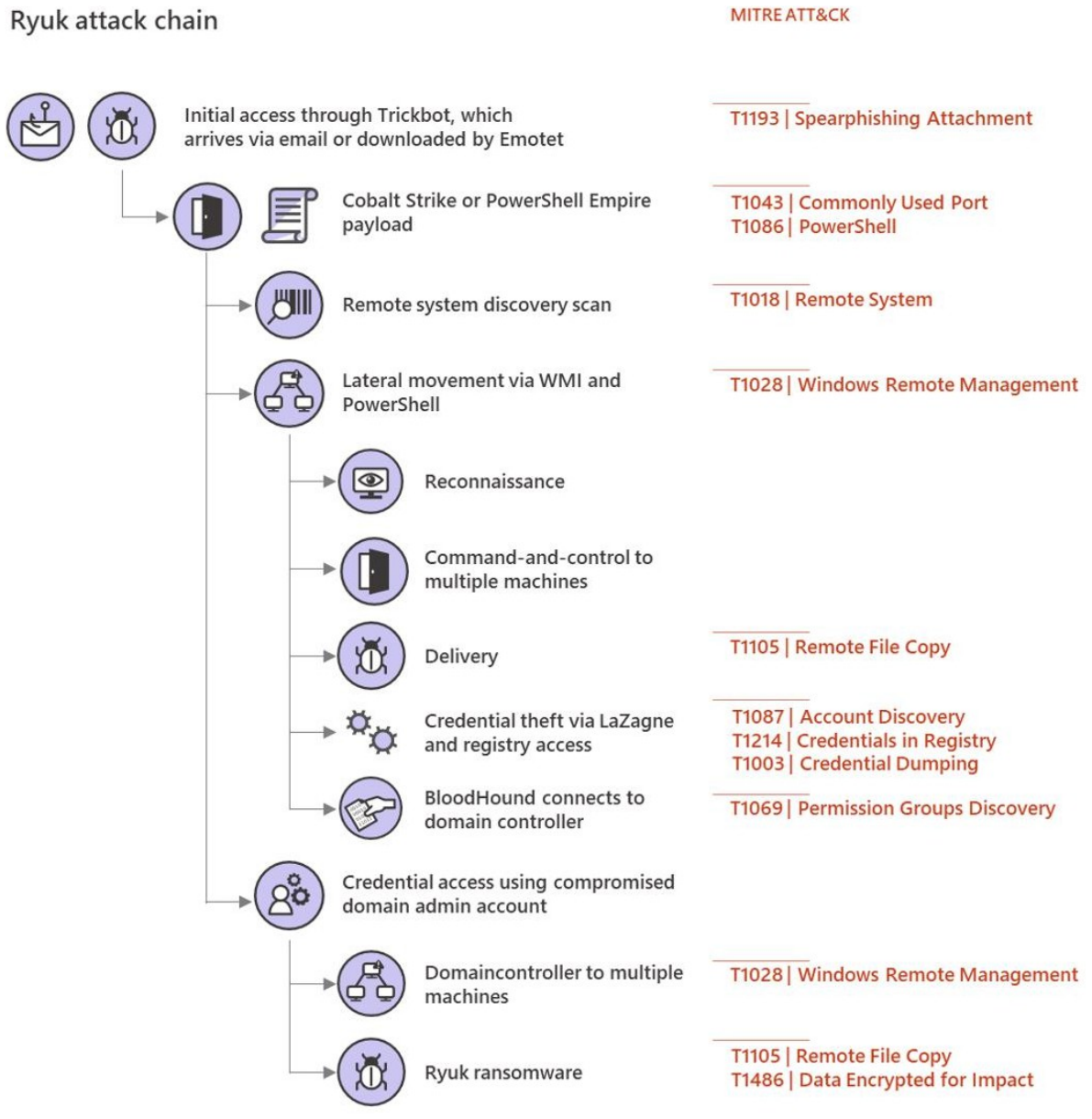
Πηγή: Trend Micro

ΕΙΣΑΓΩΓΗ – ΙΣΤΟΡΙΚΟ

- 1989 – «PC CYBORG»
  - μπλοκάρισε τον υπολογιστή για «λήξη άδειας χρήσης»
  - διανεμήθηκε στη διάσκεψη του WHO για το AIDS (δισκέτα)
  - κρυπτογράφηση αρχείων δίσκου
- 2005-2006 – πρώτη κύμα «σύγχρονου» ransomware (στη Ρωσία)
- 2011 – Λογισμικό εκβιασμού μέσω SMS (κλήση σε αριθμό SMS με υψηλή χρέωση)
- 2012 – Ψεύτικο ransomware «Screen Locker» με βάση την αστυνομία
- 2013 – Cryptolocker (ισχυρή κρυπτογράφηση, χρήση TOR)
- 2014 – «Φρενίτιδα» κρυπτογράφησης αρχείων: CryptoWall, CTB-Locker, Locky, TeslaCrypt …
- 2017 – WannaCry (με δυνατότητες «σκουληκιού»)
- 2018 – NotPetya (διαγραφή)
  - χτύπησε τη δανική ναυτιλιακή εταιρεία «Maersk» (10 ημέρες εκτός λειτουργίας!)
- 2019 – Maze (διπλή εκβίαση)
- 2021 – Τριπλή εκβίαση (με προσθήκη απειλής DDOS)

ΝΕΕΣ ΤΑΣΕΙΣ

- **Ανθρώπινα χειριζόμενο ransomware**
  - Προσαρμοσμένοι φορείς μόλυνσης (αναγνώριση)
  - ανακάλυψη στόχων (υψηλής αξίας)
  - Αύξηση προνομίων – Πλευρική κίνηση
  - Τεχνικές, τακτικές και διαδικασίες (TTP) τύπου APT



«ΚΟΙΝΕΣ» ΤΑΣΕΙΣ ΣΤΙΣ ΤΕΧΝΙΚΕΣ, ΤΕΧΝΙΚΕΣ ΚΑΙ ΠΡΟΤΑΣΕΙΣ ( )

- **Μεσάζων αρχικής πρόσβασης (IAB)**
  - Βρείτε έναν τρόπο να αποκτήσετε πρόσβαση σε «τυχαία» δίκτυα οργανισμών
  - Πουλήστε την πρόσβαση στο δίκτυο (συνήθως μέσω του dark web, 500-10.000$)
- **RaaS** – Ransomware As a Service
  - Το κακόβουλο λογισμικό μπορεί να μεταφερθεί
  - Η πλατφόρμα απομακρυσμένης χρήσης κακόβουλου λογισμικού μπορεί να μεταφερθεί
    - Διαμόρφωση: ποσό λύτρων, σημείωμα πληρωμής, θύματα...
  - η πλατφόρμα μπορεί να παρέχει ήδη πρόσβαση στα θύματα
    - π.χ. Emotet (γενικός downloader)

Θέμα 2 - Απειλές

Ναυτιλιακός τομέας

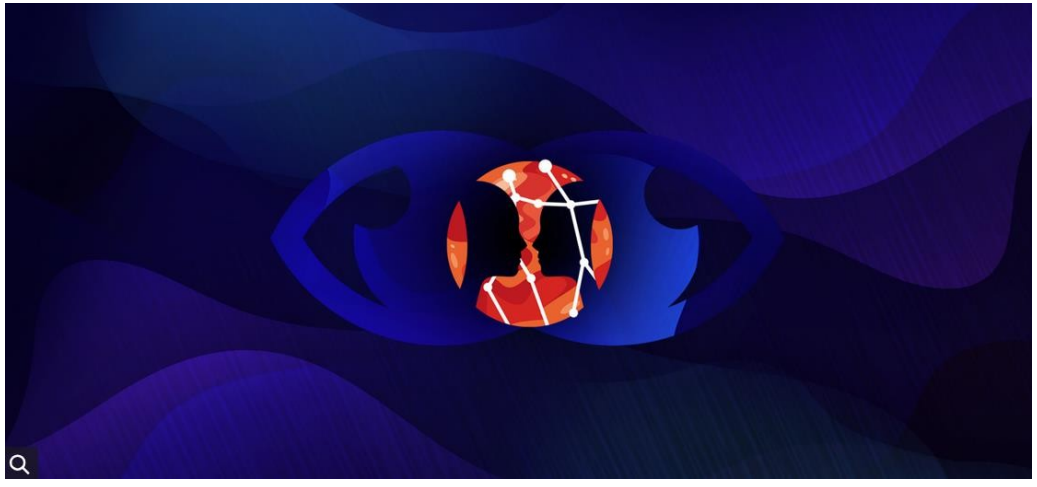
- Προσδιορισμένες πηγές
- Περιπτώσεις χρήσης

Πηγές πληροφοριών (Εταιρείες)

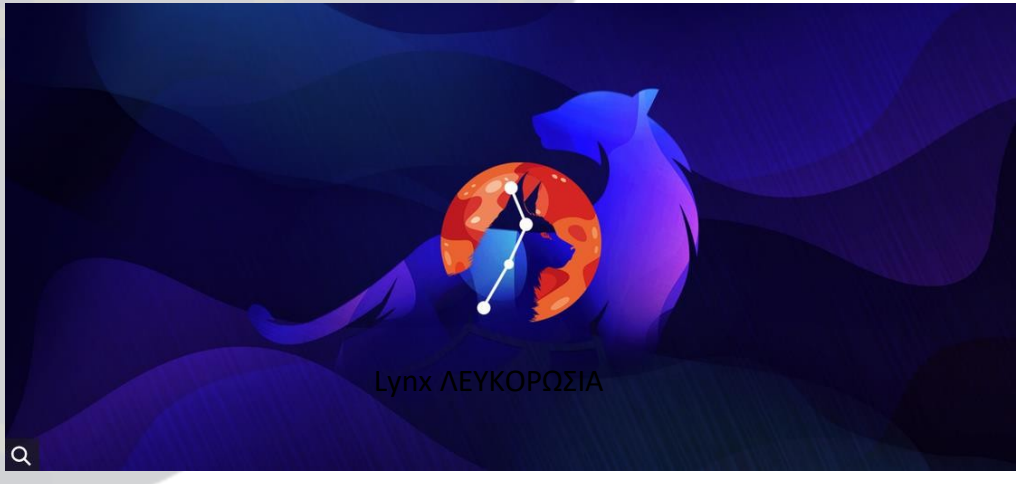
Ομάδες απειλών που παρακολουθούνται από την Palo Alto Networks Unit 42

Πλατφόρμα RaaS: https://unit42.paloaltonetworks.com/threat-actor-groups-tracked-by-palo-alto-networks-unit-42/

Draco ΠΑΚΙΣΤΑΝ



Gemini ΙΝΔΙΑ



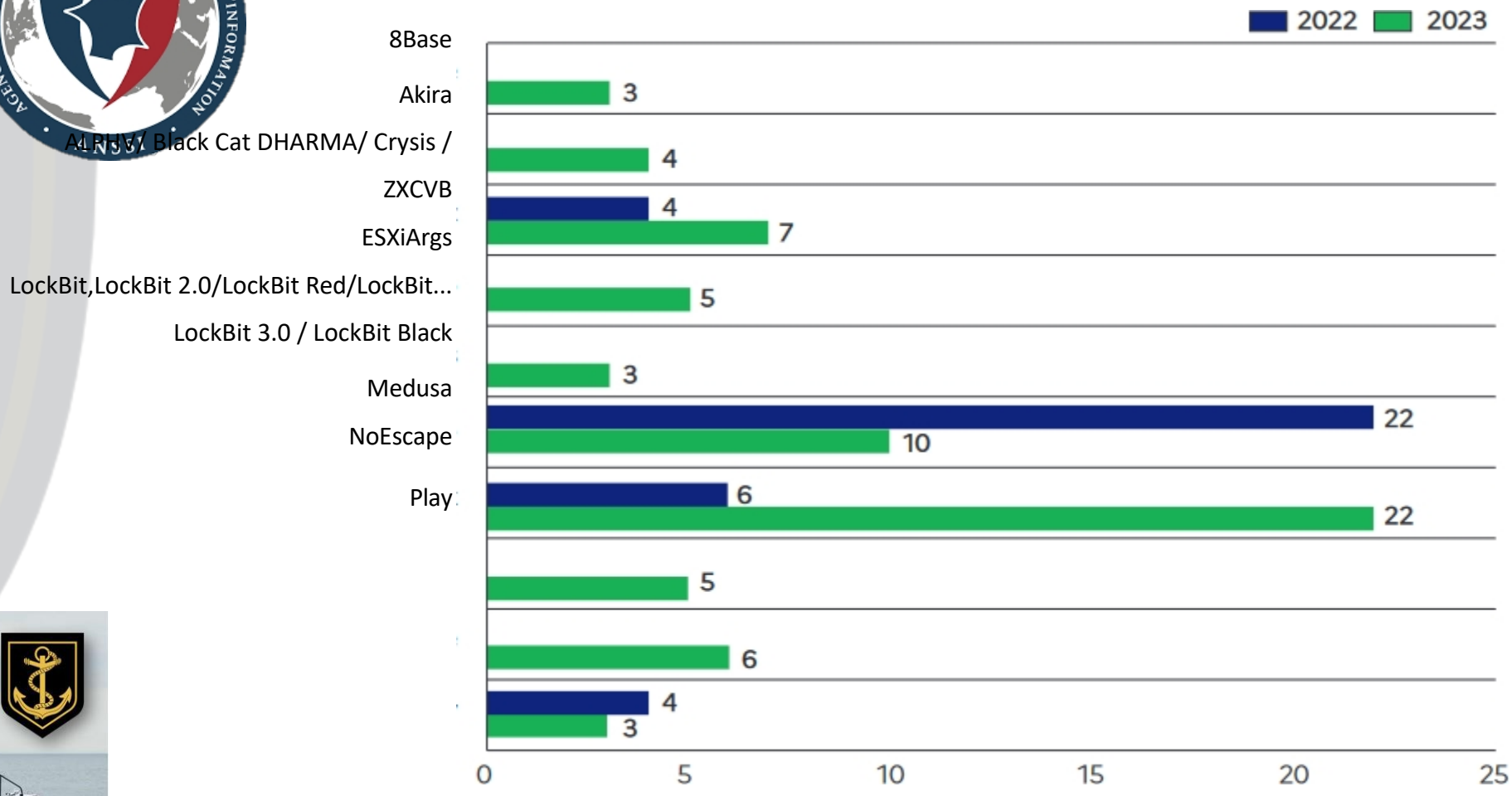
Lynx ΛΕΥΚΟΡΩΣΙΑ

Θέμα: Η νομική τοποθεσία των παράνομων παραγόντων

RaaS: RANSOM As a Service

Πηγές πληροφοριών (εθνικές υπηρεσίες)

Σύγκριση των κύριων στελεχών ransomware που χρησιμοποιήθηκαν σε περιστατικά που αναφέρθηκαν στην ANSSI το 2022 και το 2023



RANSOMWARE στον τομέα της ναυτιλίας

- **Τάσεις**
  - αυξανόμενη ψηφιοποίηση
  - φυσική μετάβαση από τοπικές επιχειρήσεις σε απομακρυσμένες
  - COVID-19 απομακρυσμένη ώθηση
- **Επιθέσεις ransomware – ιδιαιτερότητες;**
  - ίδιοι επιτιθέμενοι, ίδιες TTP
  - ενδιαφέρον στόχος: υποστηρίζει το 90% του παγκόσμιου εμπορίου!
    - πιθανός στόχος πολέμου
  - Σύνθετα και ολοκληρωμένα οικοσυστήματα πληροφορικής (επίσης με τεχνολογία λειτουργίας – OT)
    - αυξημένοι κίνδυνοι στην αλυσίδα εφοδιασμού: το «σημείο εισόδου» μπορεί να είναι μια συνεργαζόμενη εταιρεία!
    - πολλοί διαθέσιμοι φορείς επίθεσης για τους επιτιθέμενους
  - Η αποστολή είναι βασικό σημείο στην εφοδιαστική αλυσίδα
    - μπορεί να χρησιμοποιηθεί ως ενδιάμεσο βήμα προς άλλο στόχο (επίθεση στην εφοδιαστική αλυσίδα)

RANSOMWARE στον ναυτιλιακό τομέα

Ransomware attack on US maritime facility confirmed

Story By: Rob O'Dwyer | January 8, 2020 | Blockchain and Cyber Security

The US Coast Guard (USCG) has issued a marine safety bulletin confirming a recent ransomware attack at a Maritime Transportation Security Act (MTSA) regulated facility, which locked users out of access to critical files and saw the infection move beyond the local facility and into wider corporate networks.

Ransomware Attack on Swire Pacific Offshore Breaches Personnel Data

Swire Pacific Offshore notified authorites of a cyber attack on its systems (Swire file photo)

PUBLISHED NOV 26, 2021 12:05 PM BY **THE MARITIME EXECUTIVE**

Image: Dimitry Anikin

With today's news that French shipping giant CMA CGM has been hit by a ransomware attack, this now means that all of the four biggest maritime shipping companies in the world have been hit by cyber-attacks in the past four years, since 2017.

Previous incidents included:

1. APM-Maersk - taken down for weeks by the NotPetya ransomware/wiper in 2017.
2. Mediterranean Shipping Company - hit in April 2020 by an unnamed malware strain that brought down its data center for days.
3. COSCO - brought down for weeks by ransomware in July 2018.

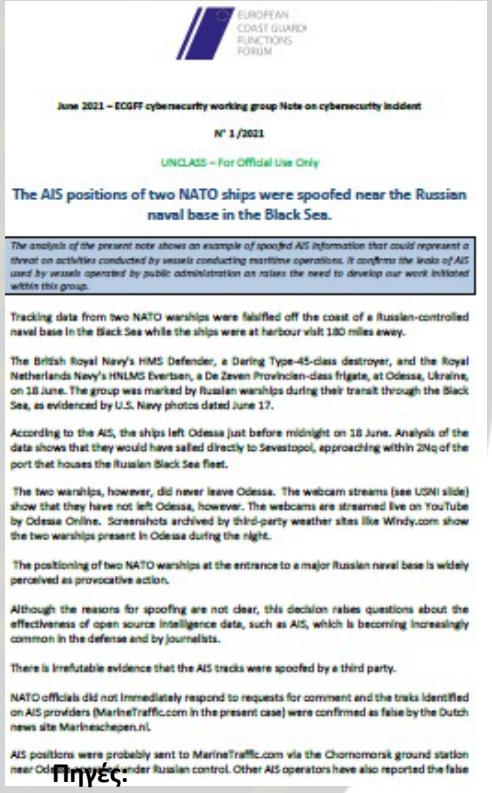
Λύσεις

- **Απλώς εφαρμόζει τις βέλτιστες πρακτικές ασφάλειας πληροφορικής**
- **Κύρια θέματα μετριασμού**
  - **ισχυρή πιστοποίηση** (ειδικά για διαδικτυακές πύλες και VPN)
    - **ή προσέγγιση μηδενικής εμπιστοσύνης**, σε μια προσέγγιση χωρίς περίμετρο
  - **αρχή του ελάχιστου προνομίου** (ειδικά με τα προνόμια των χρηστών)
  - **διαχωρισμός συστήματος/δικτύου (φυσικός/λογικός)**
  - Διαδικασίες **επιχειρησιακής συνέχειας**
    - **δημιουργία αντιγράφων ασφαλείας** (hot και cold)
  - Συνεχής **αξιολόγηση ευπαθειών** και **επιδιόρθωση**
  - Παρακολούθηση **Κέντρου Λειτουργίας Ασφαλείας**
  - **Ενίσχυση ασφάλειας (**πρωτόκολλα δικτύου, τείχος προστασίας κεντρικού υπολογιστή, διαμόρφωση λογισμικού, ασφάλεια λειτουργικού συστήματος, κ.λπ.)

Περίπτωση χρήσης – AIS / GNSS

Κύριο μέλημα των ναυτιλιακών οργανισμών – AIS / GNSS Spoofing /Jamming

Οι θέσεις AIS δύο πλοίων του NATO παραποιήθηκαν κοντά στη ρωσική ναυτική βάση στη Μαύρη Θάλασσα.



EUROPEAN COAST GUARD FUNCTIONS FORUM

June 2021 – ECGFF cybersecurity working group Note on cybersecurity incident

N° 1/2021

UNCLASS – For Official Use Only

The AIS positions of two NATO ships were spoofed near the Russian naval base in the Black Sea.

The analysis of the present note shows an example of spoofed AIS information that could represent a threat on activities conducted by vessels conducting maritime operations. It confirms the leaks of AIS used by vessels operated by public administration an raises the need to develop our work initiated within this group.

Tracking data from two NATO warships were falsified off the coast of a Russian-controlled naval base in the Black Sea while the ships were at harbour visit 180 miles away.

The British Royal Navy's HMS Defender, a Daring Type-45-class destroyer, and the Royal Netherlands Navy's HNLMS Evertsen, a De Zeven Provincien-class frigate, at Odessa, Ukraine, on 18 June. The group was marked by Russian warships during their transit through the Black Sea, as evidenced by U.S. Navy photos dated June 17.

According to the AIS, the ships left Odessa just before midnight on 18 June. Analysis of the data shows that they would have sailed directly to Sevastopol, approaching within 2Nq of the port that houses the Russian Black Sea fleet.

The two warships, however, did never leave Odessa. The webcam streams (see USNI slide) show that they have not left Odessa, however. The webcams are streamed live on YouTube by Odessa Online. Screenshots archived by third-party weather sites like Windy.com show the two warships present in Odessa during the night.

The positioning of two NATO warships at the entrance to a major Russian naval base is widely perceived as provocative action.

Although the reasons for spoofing are not clear, this decision raises questions about the effectiveness of open source intelligence data, such as AIS, which is becoming increasingly common in the defense and by journalists.

There is irrefutable evidence that the AIS tracks were spoofed by a third party.

NATO officials did not immediately respond to requests for comment and the traks identified on AIS providers (MarineTraffic.com in the present case) were confirmed as false by the Dutch news site Marineschepen.nl.

AIS positions were probably sent to MarineTraffic.com via the Chornomorsk ground station near Odessa, now under Russian control. Other AIS operators have also reported the false

Πηγές:

- EU CERT & M-CERT
- Κράτη μέλη
- Ιδιωτικές εταιρείες

Απειλές για κρίσιμες υποδομές

Κακόβουλο λογισμικό:
Κακόβουλο λογισμικό του οποίου η εξάπλωση είναι ανεξέλεγκτη

Script kiddy (αδρανής έφηβος ή, γενικότερα, μοναχικός και ευκαιριακός επιτιθέμενος):

- Πολύ χαμηλά μέσα (€<,100)
- Κίνητρο το τζόγο (και ενδεχομένως το κέρδος)

Ευκαιριακή επίθεση Κακόβουλος υπάλληλος (μνησικακία/απληστία):

- Χαμηλά μέσα (< 1.000 €)
- Κύριο κίνητρο: να βλάψει τον εργοδότη του, αποφεύγοντας τα θύματα
- Διακριτικότητα, όταν είναι δυνατόν
- Εύκολη πρόσβαση σε όλα τα στοιχεία του σκάφους

Τρομοκρατική ομάδα:

- Μέτρια μέσα (από 10.000 έως 50.000 ευρώ)
- Αναζήτηση ανθρώπινων θυμάτων, υλικές ζημιές, υψηλή προβολή στα μέσα ενημέρωσης

Εγκληματική επιχείρηση:

- Υψηλοί πόροι (περίπου ένα εκατομμύριο ευρώ)
- Στόχος κερδοφορίας
- Χαμηλοί ηθικοί περιορισμοί
- Επιδίωξη διακριτικότητας

Κατάσταση:

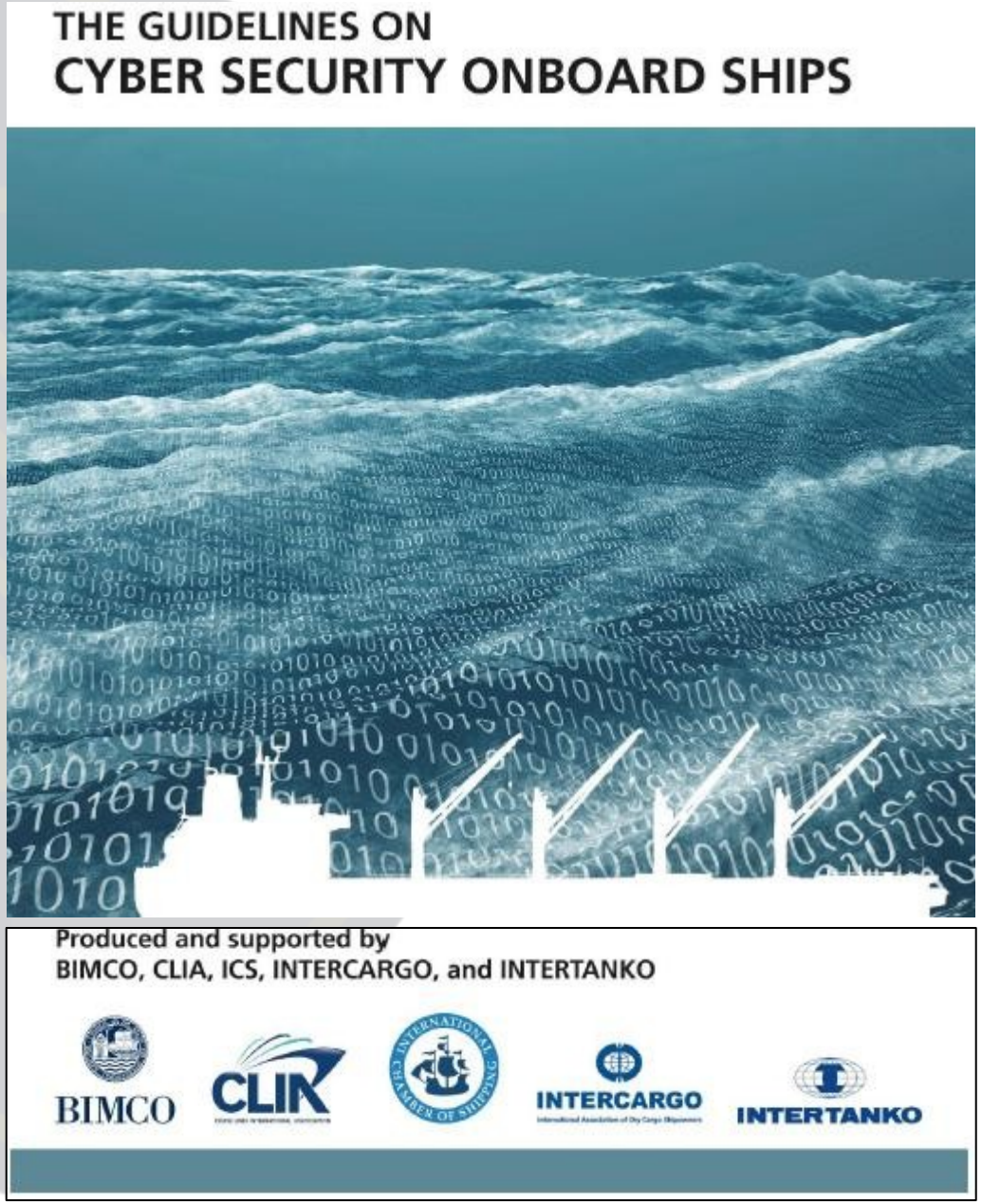
- Σχεδόν απεριόριστα μέσα
- Στόχοι όλων των τύπων –
- Απουσία ηθικών περιορισμών
- Απαραίτητη διακριτικότητα

Απειλές για τα συστήματα

Παραποίηση πλοίου – Μεταδίδεται μήνυμα AIS με λεπτομέρειες για ένα πλοίο που δεν υπάρχει. Σενάρια όπου αυτό θα μπορούσε να χρησιμοποιηθεί περιλαμβάνουν την παραποίηση ενός πλοίου μιας χώρας στα χωρικά ύδατα μιας εχθρικής χώρας, οδηγώντας την εν λόγω χώρα να λάβει αντίμετρα. Εναλλακτικά, μπορούν να μεταδοθούν πολλαπλές εκδοχές των λεπτομερειών ενός πραγματικού πλοίου, τοποθετώντας το σε πολλές διαφορετικές τοποθεσίες ταυτόχρονα για να αποκρύψουν την πραγματική του θέση (π.χ. παράνομη αλιεία).
Παραποίηση βοηθημάτων πλοήγησης – Ψεύτικα βοηθήματα πλοήγησης, όπως μια σημαδούρα που προειδοποιεί για κρυμμένα ύφαλα, μεταδίδονται προκειμένου να αναγκάσουν ένα πλοίο να αλλάξει πορεία. Αυτό μπορεί να γίνει για να αναγκαστεί ένα σκάφος να εισέλθει σε μια περιοχή όπου μπορεί να καταληφθεί.
Παραποίηση σύγκρουσης – Η αποφυγή συγκρούσεων είναι μία από τις κύριες χρήσεις του AIS. Παρέχοντας παραποιημένα στοιχεία για ένα σκάφος που βρίσκεται σε πορεία σύγκρουσης, ένας εισβολέας μπορεί να αναγκάσει ένα πλοίο να αλλάξει πορεία για να αποφύγει την αναμενόμενη σύγκρουση. Αυτό θα μπορούσε, για παράδειγμα, να χρησιμοποιηθεί για να οδηγήσει το πλοίο σε πραγματική σύγκρουση.

Παραποίηση AIS-SART – Η αναζήτηση και διάσωση είναι μια άλλη από τις κύριες χρήσεις του AIS. Αυτή η επίθεση δημιουργεί ένα παραποιημένο σήμα αναμεταδότη SAR-T, το οποίο παρέχει λεπτομέρειες για μια κατάσταση έκτακτης ανάγκης. Καθώς τα πλοία είναι νομικά υποχρεωμένα να παρέχουν βοήθεια, η παραποίηση SART μπορεί να χρησιμοποιηθεί ως δόλωμα για να προσελκύσει πλοία σε μια τοποθεσία όπου μπορούν να δεχθούν επίθεση.
Παραποίηση πρόγνωσης καιρού – Το AIS μπορεί να χρησιμοποιηθεί για τη μεταβίβαση πληροφοριών σχετικά με τις επικρατούσες καιρικές συνθήκες μεταξύ των σκαφών. Μια ψεύτικη πρόγνωση, ιδιαίτερα μια που προβλέπει καλές συνθήκες όταν πλησιάζει καταιγίδα, θα μπορούσε να χρησιμοποιηθεί για να οδηγήσει τα σκάφη σε δυσκολίες.
Κατάληψη AIS – Είναι επίσης δυνατό να παρακάμψετε τα σήματα που στέλνουν τα σκάφη, μεταδίδοντας ένα σήμα υψηλότερης ισχύος την ίδια στιγμή και συχνότητα. Ο επιτιθέμενος μπορεί στη συνέχεια να αλλάξει ορισμένες λεπτομέρειες του αρχικού μηνύματος, για παράδειγμα να υποδείξει ότι το σκάφος μεταφέρει πυρηνικό φορτίο σε μια περιοχή όπου τέτοια φορτία είναι παράνομα.

Κοινές ευθύνες – Μεγάλη κοινότητα – Περιορισμένες πρωτοβουλίες

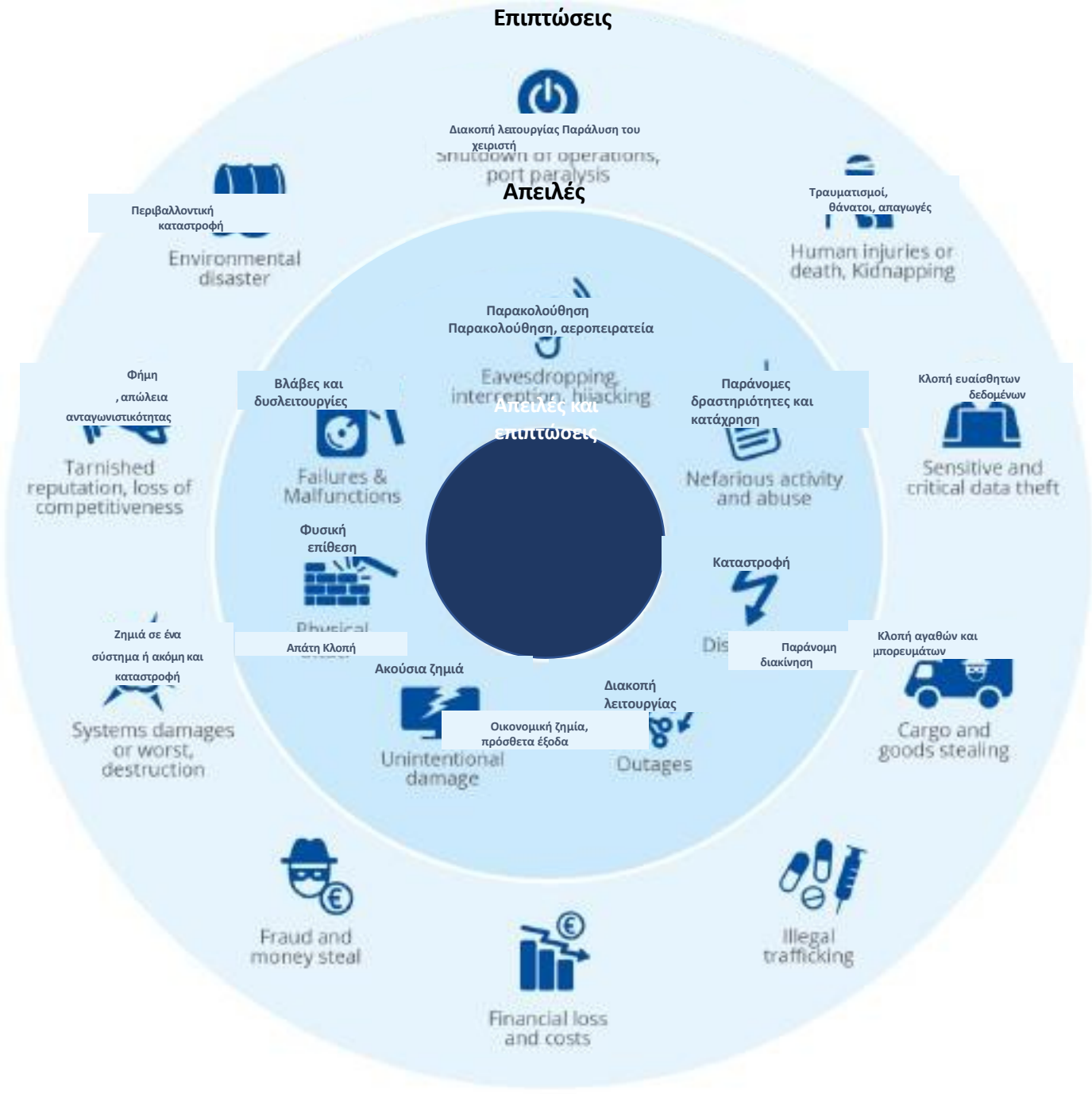


- Χώρες σημαίας
- Ναυπηγοί
- Εταιρείες διαχείρισης πλοίων
- Λιμάνια
- Συνδέσεις με την οικονομία (περιφερειακή, μεταφορές)
- Ναυτικοί πράκτορες
- Ασφαλιστικές εταιρείες
- Οργανισμοί πιστοποίησης
- Ναυπηγοί
- Πάροχοι επικοινωνιών
- Πάροχοι συστημάτων
- Πάροχοι υπηρεσιών ασφαλείας

Όροι χρήσης

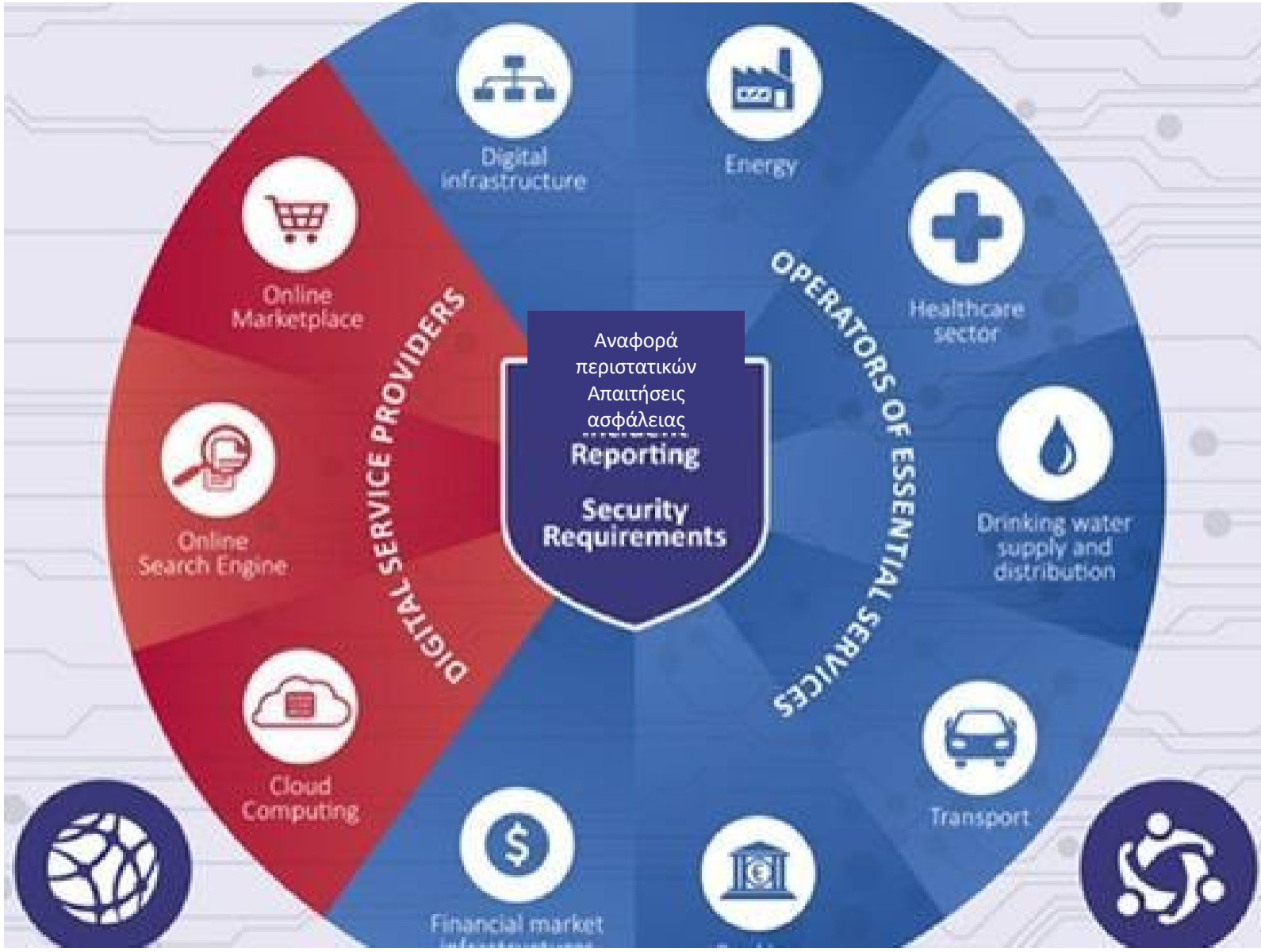
Οι συμβουλές και οι πληροφορίες που παρέχονται στις Κατευθυντήριες γραμμές για την ασφάλεια στον κυβερνοχώρο επί των πλοίων προορίζονται αποκλειστικά ως οδηγίες **που χρησιμοποιούνται με ευθύνη του χρήστη**. *Δεν παρέχονται εγγυήσεις ή δηλώσεις, ούτε αναλαμβάνεται οποιαδήποτε υποχρέωση φροντίδας ή ευθύνης από τους συντάκτες, τα μέλη τους ή τους υπαλλήλους οποιουδήποτε προσώπου, εταιρείας, οργανισμού ή οργανισμού ... για την ακρίβεια των πληροφοριών ή των συμβουλών που παρέχονται στις κατευθυντήριες γραμμές ή για οποιαδήποτε παράλειψη από τις κατευθυντήριες γραμμές ή για οποιαδήποτε συνέπεια που προκύπτει άμεσα ή έμμεσα από τη συμμόρφωση, την υιοθέτηση ή την εξάρτηση από τις οδηγίες που περιέχονται στις κατευθυντήριες γραμμές, ακόμη και αν προκλήθηκε από την παράλειψη άσκησης εύλογης προσοχής εκ μέρους οποιουδήποτε από τα προαναφερθέντα μέρη.*

Απειλές / Επιπτώσεις



Ιδιαίτερες συνθήκες της ναυτιλίας

- Κοινότητες
- Ομοιότητα Ναυτιλία / Ψηφιακό
- Εξάρτηση από το GNSS
- Περιβάλλον ανταλλαγής πληροφοριών



Κίνδυνοι για τις κρίσιμες θαλάσσιες υποδομές

Θέμα 3 – Η σημασία των δεδομένων

- Κανονισμός της ΕΕ
- Ταξινομημένα δεδομένα / Ευαίσθητα δεδομένα
- Επεξεργασία δεδομένων

Θαλάσσιες / Ψηφιακές ομοιότητες

	Ναυτιλιακές	Ψηφιακές
Διάσταση	80% της γης	Απεριόριστη
Νομικός	Αδύναμη διεθνής ρύθμιση UNCLOS	Περιορισμένη διεθνής ρύθμιση GDPR
Οικονομικά	90 % του διεθνούς εμπορίου Σταθερό	50 % των διεθνών συναλλαγών Μόνιμη ανάπτυξη
Περιβάλλον	Απρόβλεπτο: Κατάσταση της θάλασσας, άνεμος, αλάτι, φυσικοί κίνδυνοι	Απρόβλεπτο: Εικονικότητα,
Απειλή	Παράνομες δραστηριότητες και χειρισμοί, Πειρατεία, τρομοκρατία	Παγκόσμια εμβέλεια των κυβερνοαπειλών Παράνομες δραστηριότητες με επίκεντρο τα αγαθά
Εστίαση	Κοινή χρήση πληροφοριών (IFC) Δυνατότητες δράσης = Κράτη	Πρόληψη και ανταλλαγή πληροφοριών Συντονισμός δράσεων

Ναυτιλία και ψηφιακός κόσμος: ομοιότητες

Σε 10 δευτερόλεπτα….

Παρόμοιοι κόσμοι (ίδιες εκτιμήσεις – ίδιες συνέπειες ???)

800 - 1260 Τ σκουπίδια

225.000 GB δεδομένα

- 500.000 δημοσιεύσεις στο Facebook,
- 57.000 tweets,
- 46.000 αναζητήσεις στο Google
- 2 εκατομμύρια μηνύματα στο WhatsAp

Σχέδιο επικοινωνίας

Προσαρμοσμένο στους φορείς εκμετάλλευσης

Κρίσιμες υποδομές

Οδηγία ECI 2008

Παγκόσμιος κίνδυνος (ασφάλεια, κατασκοπεία, δεδομένα, δραστηριότητα)

Η επίθεση θα μπορούσε να θέσει σε κίνδυνο την ασφάλεια μιας χώρας

Τομεακή παρακολούθηση

- Ανάλυση κινδύνου
- Ευπάθειες
- Οδηγίες

Διατομεακός συντονισμός

Διαχειριστής βασικών υπηρεσιών

Οδηγία NIS 2015

Κίνδυνος κατασκοπείας, δεδομένων, δραστηριότητας

Η επίθεση θα μπορούσε να θέσει σε κίνδυνο την οικονομική δραστηριότητα

Τομεακή εκτίμηση κινδύνου

Προειδοποιήσεις

Διατομεακές πληροφορίες

Κοινός χρήστης του τομέα Maritim

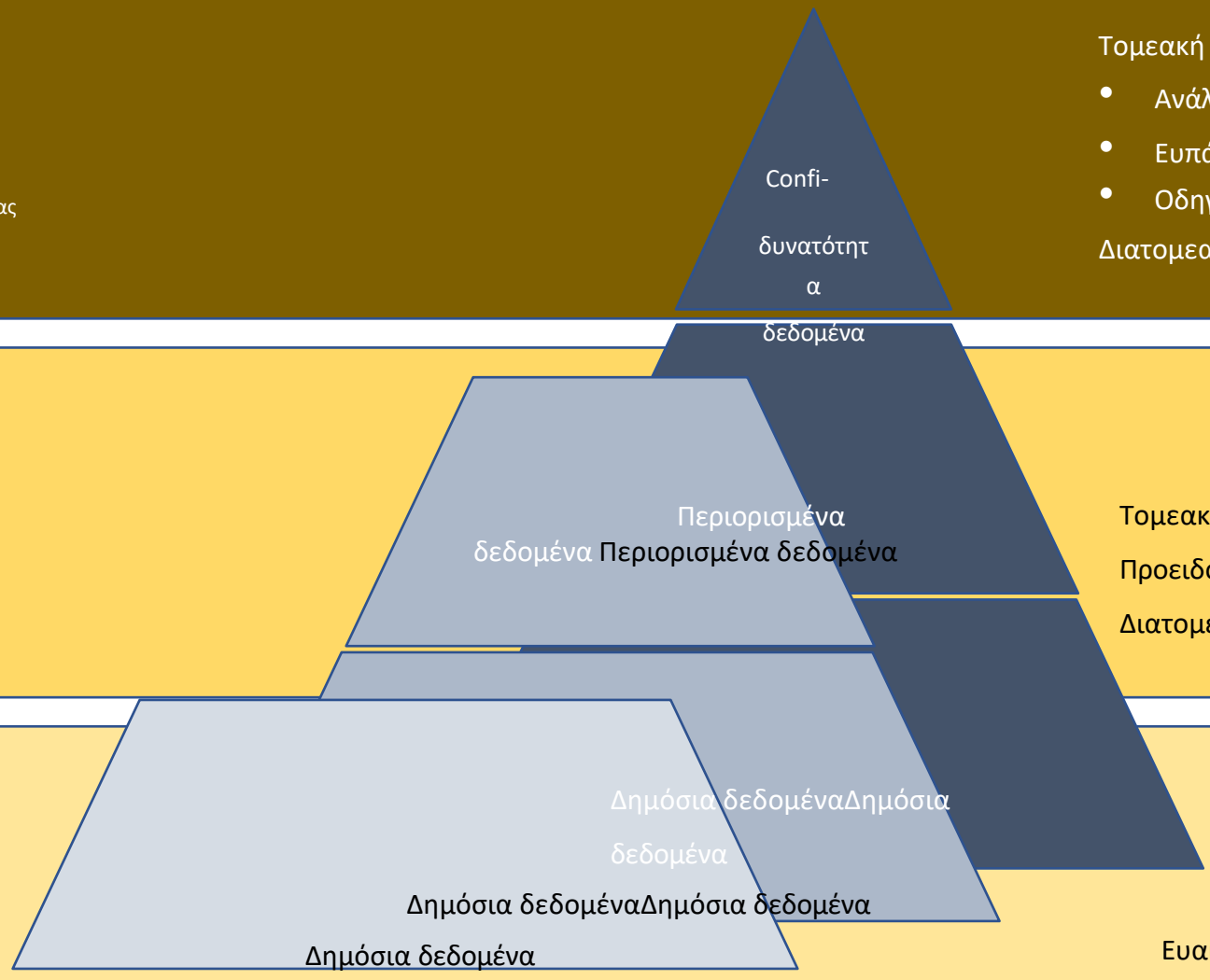
GDPR 2018

Κίνδυνος για τα δεδομένα

Η επίθεση μπορεί να αποτελεί απειλή

Ευαισθητοποίηση ανά τομέα

- Συστάσεις
- Πρόληψη



ΕΥΡΩΠΑΪΚΟ ΠΛΑΙΣΙΟ ΔΕΞΙΟΤΗΤΩΝ ΚΥΒΕΡΝΗΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ: ΠΡΟΦΙΛ ΘΕΣΕΩΝ ΕΡΓΑΣΙΑΣ

ECSF
EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

Διευθυντής Ασφάλειας Πληροφοριών CISO
Chief Information Security Officer (CISO)

Ανταποκριτής σε περιστατικά κυβερνοασφάλειας
Responder

Υπεύθυνος νομικών θεμάτων, πολιτικής και συμμόρφωσης στον κυβερνοχώρο
Cyber Legal, Policy and Compliance Officer

Ειδικός σε θέματα πληροφοριών για κυβερνοαπειλές
Cyber Threat Intelligence Specialist

Αρχιτέκτονας κυβερνοασφάλειας
Cybersecurity Architect

Ελεγκτής κυβερνοασφάλειας
Cybersecurity Auditor

Εκπαιδευτής στον τομέα της κυβερνοασφάλειας
Cybersecurity Educator

Υπεύθυνος εφαρμογής κυβερνοασφάλειας
Cybersecurity Implementer

Ερευνητής στον τομέα της κυβερνοασφάλειας
Cybersecurity Researcher

Διαχειριστής κινδύνων κυβερνοασφάλειας
Cybersecurity Risk Manager

Ερευνητής ψηφιακής εγκληματολογίας
Digital Forensics Investigator

Δοκιμαστής διείσδυσης
Penetration Tester

https://digital-skills-jobs.europa.eu/en/cyber-skills-academy-knowledge-and-training

https://cybersecpro-project.eu/

Περίπτωση χρήσης

Κρίσιμη υποδομή

Θαλάσσιο λιμάνι

ΛΙΜΑΝΙΑ ΚΑΙ ΝΑΥΤΙΛΙΑΚΟΙ ΕΝΔΙΑΦΕΡΟΜΕΝΟΙ

Ποιος είναι ο στόχος των επιτιθέμενων;

Διασφάλιση πληροφοριών

Λειτουργικές περιοχές

(Ταξινομία CYBERSECPRO)

Προστασία προσωπικών δεδομένων και δεδομένων

Διαχείριση κινδύνων στον τομέα της κυβερνοασφάλειας

Απειλές για την ασφάλεια στον κυβερνοχώρο

διαχείριση

Αντιμετώπιση συμβάντων στον κυβερνοχώρο

Αντιμετώπιση

Ανθρώπινη διάσταση της κυβερνοασφάλειας

Δοκιμές διείσδυσης

Ασφάλεια δικτύων και επικοινωνιών

Εργαλεία και τεχνολογία

Διαχείριση κυβερνοασφάλειας

Πολιτική, διαδικασία και συμμόρφωση στον τομέα της κυβερνοασφάλειας

Ναυτιλιακό πλαίσιο – Νομικά (διεθνή) ΨΗΦΙΣΜΑΤΑ ΤΟΥ ΔΝΟ

MSC.428(98) (16 Ιουνίου 2017) ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΤΑ ΣΥΣΤΗΜΑΤΑ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ:

ένα εγκεκριμένο σύστημα διαχείρισης ασφάλειας πρέπει να λαμβάνει υπόψη τη διαχείριση των κινδύνων στον κυβερνοχώρο

Διοικήσεις πρέπει να διασφαλίζουν ότι οι κίνδυνοι είναι αντιμετωπίζονται αντιμετωπίζονται σε συστήματα

01 Ιανουαρίου 2021 (Έρευνα ?)

Συγκεκριμένα συστήματα που πρέπει να ληφθούν υπόψη:

- Συστήματα γέφυρας
- Συστήματα διαχείρισης και χειρισμού φορτίου
- Συστήματα διαχείρισης πρόωσης και μηχανημάτων και συστήματα ελέγχου ισχύος
- Συστήματα ελέγχου πρόσβασης
- Συστήματα εξυπηρέτησης και διαχείρισης επιβατών
- Δημόσια δίκτυα εξυπηρέτησης επιβατών
- Συστήματα διοικητικής υποστήριξης και φροντίδας του πληρώματος
- Συστήματα επικοινωνίας

Incident notification requirements

- Specific criteria/thresholds for incident notification

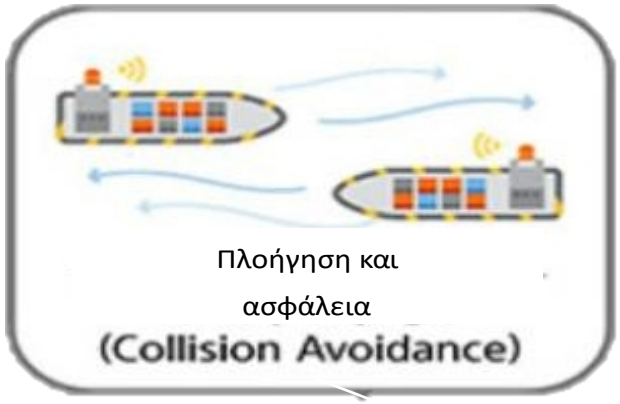
Ναυτιλιακό πλαίσιο – Νομικά (ΕΕ) – Υπενθύμιση

	Αναφορά	Χρήστης	Δίκτυο	SI	Ποιοι ενδιαφερόμενοι	Προληπτικά μέτρα	Ικανότητα άμυνας	Ανακατάληψη (δικαστική)
C I (Εθνη: μετά το 2013) 	Οδηγία 2005/65/ΕΚ Εθνική νομοθεσία	+++	++	++ +	Λιμάνια Καλώδια Πετρέλαιο και φυσικό αέριο HAZMAT και τα κρίσιμα συστήματά τους	Η ΕΕ έχει αναγνωρίσει τα λιμάνια ως κρίσιμη υποδομή» Λιμάνι = συγκεκριμένη περιοχή ξηράς και θάλασσας, με όρια που ορίζονται από τα κράτη μέλη, η οποία περιλαμβάνει έργα και εξοπλισμό που έχουν σχεδιαστεί για τη διευκόλυνση των μεταφορικών δραστηριοτήτων	Καταγραφή συμβάντων και δυνατότητα ανάλυσης αρχείων καταγραφής Δοκιμές συστημάτων (κράτος ή εξειδικευμένος πάροχος υπηρεσιών. ANSSI permalink Διαχείριση κρίσεων	Διατήρηση τεχνικών αρχείων για 6 μήνες
OES (NIS – 2018 - 22) 	Dir (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (6/07/16 - μέτρα για τη διασφάλιση ενός επιπέδου ασφάλειας Συστήματα και δίκτυα	0	+++	++	Κατάλογος **OES** που παρέχεται από τα κράτη μέλη (λιμάνια, ναυτιλιακές εταιρείες)	Κατάλογος βασικών υπηρεσιών Πολιτική και τεχνική διακυβέρνηση. Προστασία δικτύων και πληροφοριακών συστημάτων. Έλεγχοι αποφάσεων PM, πρότυπα Κανόνες παρόχων υπηρεσιών cloud	Άμυνα δικτύων και συστημάτων πληροφοριών Χρήση συσκευών υλικού/λογισμικού ή υπηρεσιών πληροφορικής που έχουν πιστοποιηθεί για την ασφάλειά τους. Αναφορά περιστατικών στην Εθνική Υπηρεσία Ασφαλείας.	Επιχειρησιακή ανθεκτικότητα.
Δεδομένα (GDPR-2018) 	Κανονισμός της ΕΕ 2016/679 - 27/04/16 Δεδομένα - Προστασία φυσικών προσώπων Κανονισμός	+++	0	++	Οντότητα που διαχειρίζεται προσωπικά δεδομένα (πράκτορας μεταφοράς με πλοίο)	Προστασία των θεμελιωδών ελευθεριών στον ψηφιακό κόσμο (διαγραφή και φορητότητα δεδομένων).	Προστατευμένα συστήματα και δίκτυα σε επίπεδο που αποτρέπει την απώλεια ελέγχου των προσωπικών πληροφοριών	Πιθανή προσφυγή σε CERT σε περίπτωση απώλειας/διαρροής δεδομένων.

Συστήματα ελέγχου λιμένων (PCS)

Λειτουργίες λιμένων

Ποια συστήματα;



Πλοήγηση και ασφάλεια

(Collision Avoidance)

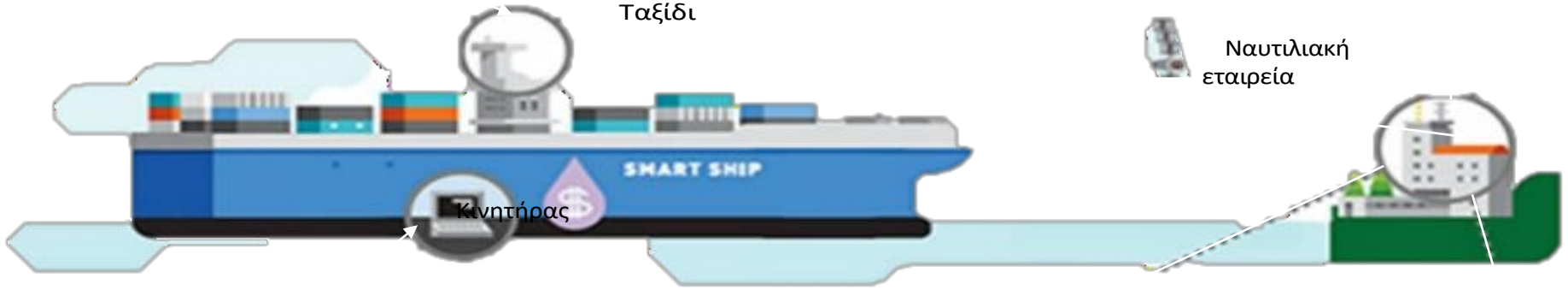
Ειδικά εργαλεία (επιβατών & επιβάτες)

Optimum route planning

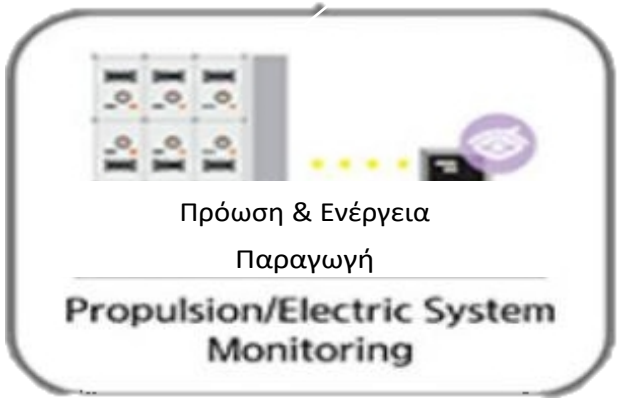
Παρακολούθηση στόλου

Fleet Management

Ταξίδι



Ναυτιλιακή εταιρεία



Πρόωση & Ενέργεια

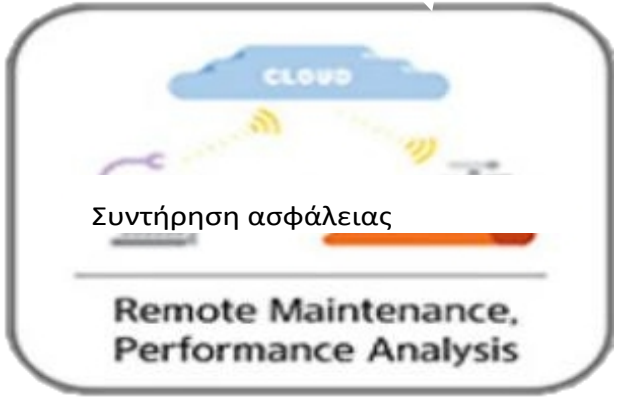
Παραγωγή

Propulsion/Electric System Monitoring

Λειτουργία

Συντήρηση

Preventive Maintenance, Part Replacement Guide



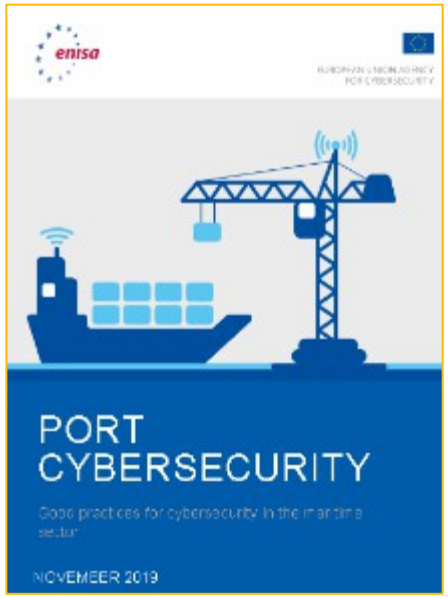
Συντήρηση ασφάλειας

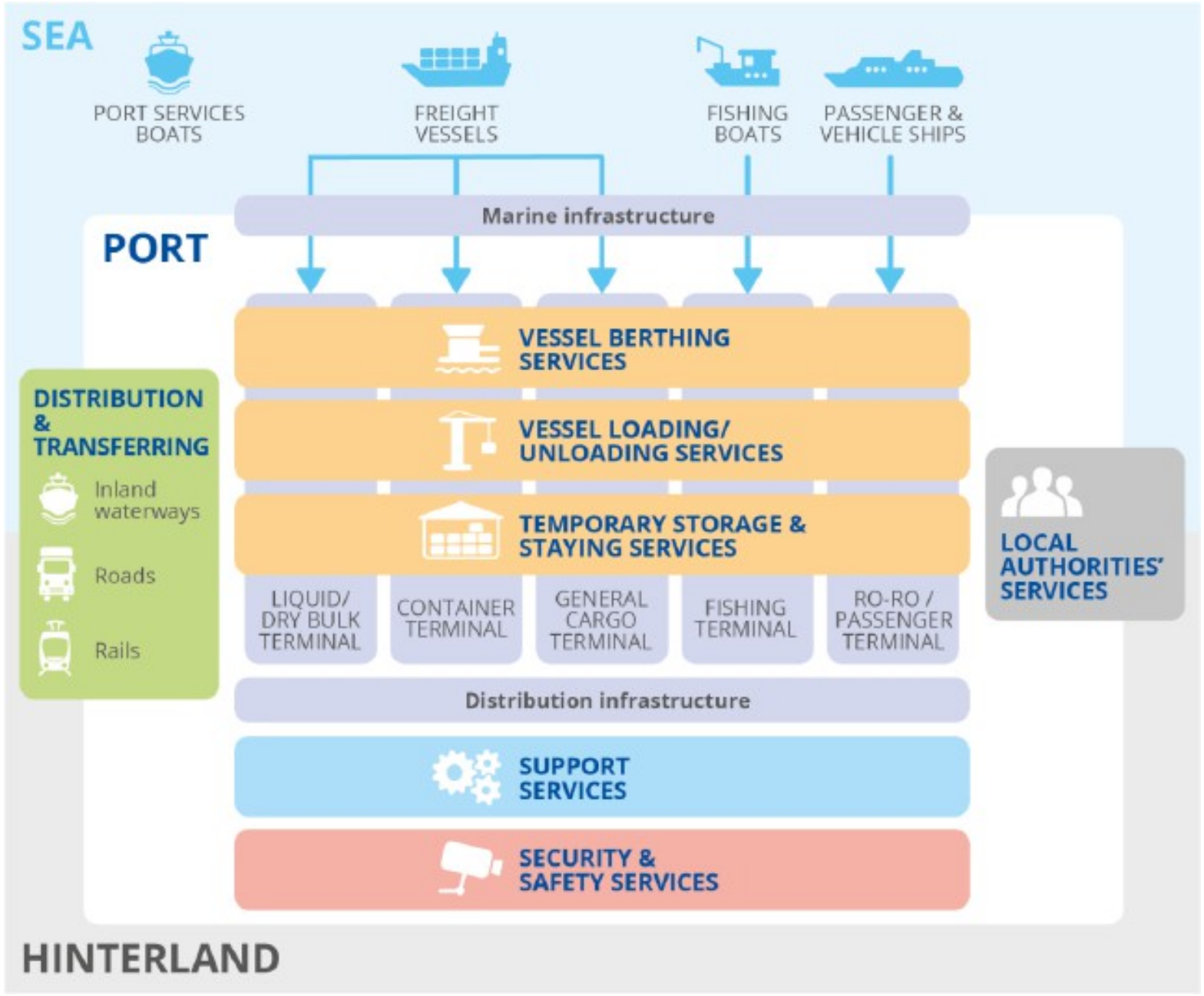
Remote Maintenance, Performance Analysis

Ναυτιλιακό πλαίσιο – Τεχνική

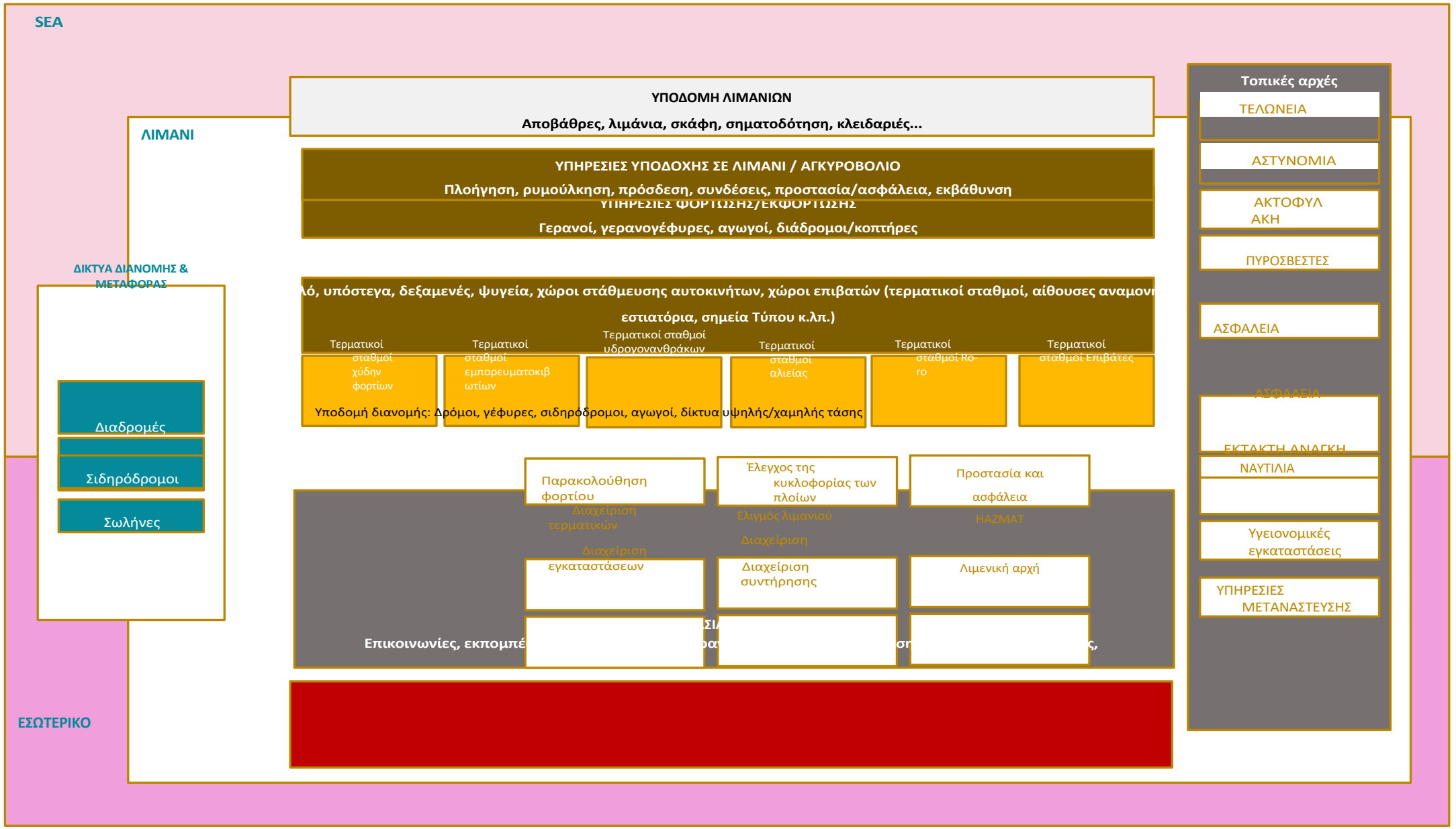
Ψηφιοποιημένο λιμάνι

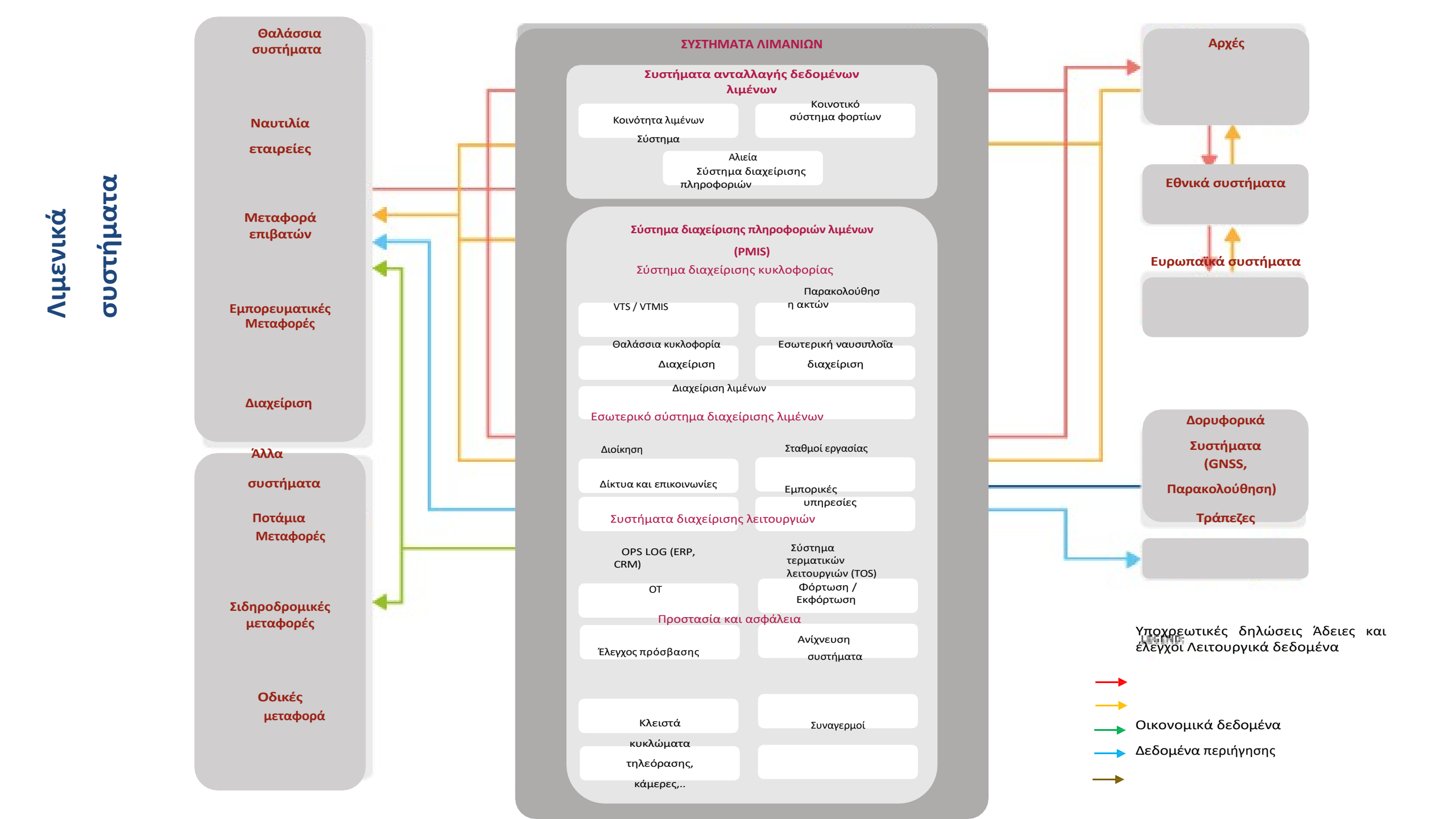
Χαρτογραφία





Ναυτιλιακό πλαίσιο – Λιμενική υποδομή

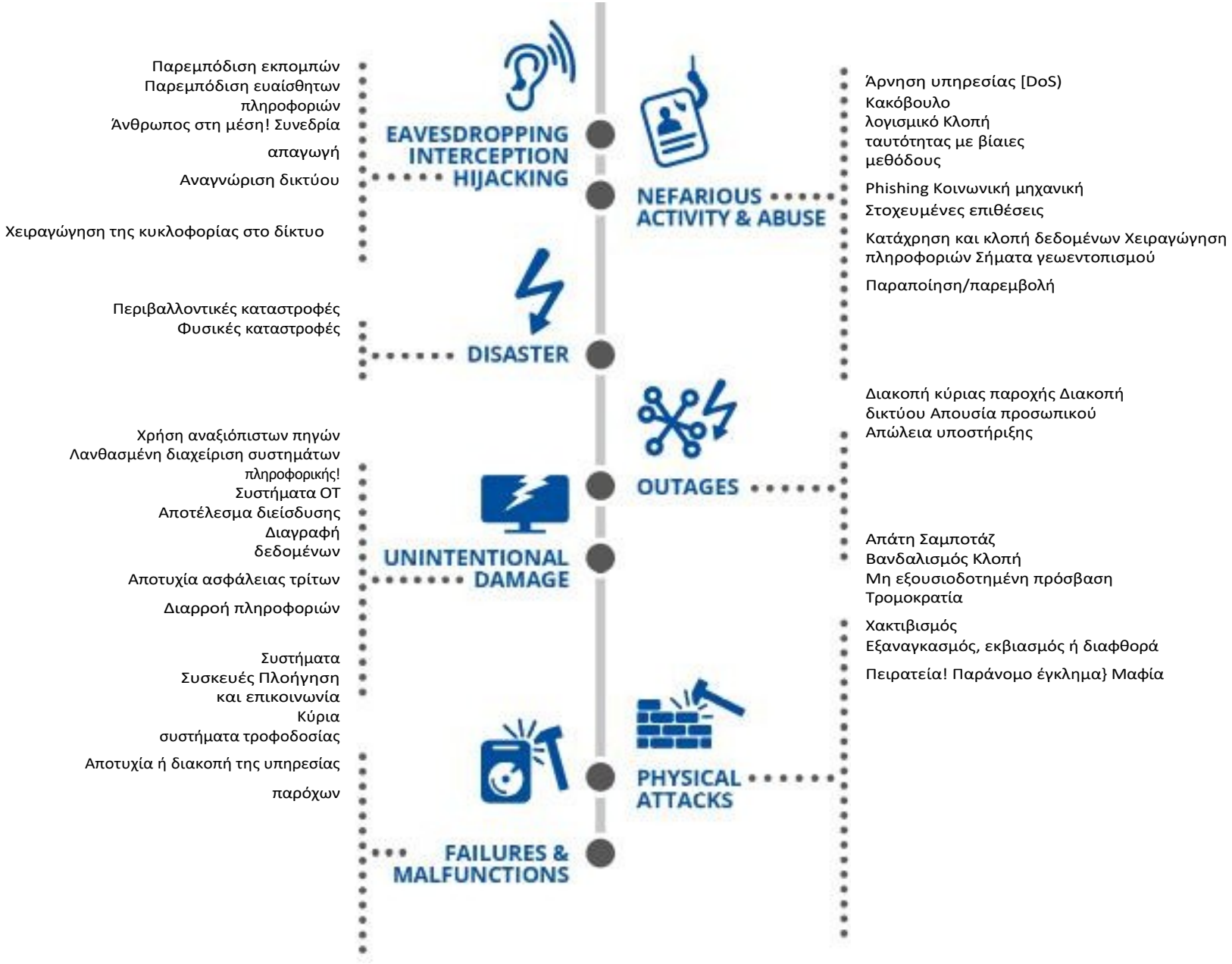



Λιμενικά συστήματα
Θαλάσσια συστήματα
Ναυτιλία
εταιρείες
Μεταφορά επιβατών
Εμπορευματικές Μεταφορές
Διαχείριση
Άλλα συστήματα
Ποτάμια Μεταφορές
Σιδηροδρομικές μεταφορές
Οδικές μεταφορά
ΣΥΣΤΗΜΑΤΑ ΛΙΜΑΝΙΩΝ
Συστήματα ανταλλαγής δεδομένων λιμένων
Κοινότητα λιμένων Σύστημα
Κοινοτικό σύστημα φορτίων
Αλιεία
Σύστημα διαχείρισης πληροφοριών
Σύστημα διαχείρισης πληροφοριών λιμένων (PMIS)
Σύστημα διαχείρισης κυκλοφορίας
VTS / VTMIS
Παρακολούθηση ακτών
Θαλάσσια κυκλοφορία Διαχείριση
Εσωτερική ναυσπλοΐα διαχείριση
Διαχείριση λιμένων
Εσωτερικό σύστημα διαχείρισης λιμένων
Διοίκηση
Σταθμοί εργασίας
Δίκτυα και επικοινωνίες
Εμπορικές υπηρεσίες
Συστήματα διαχείρισης λειτουργιών
OPS LOG (ERP, CRM)
Σύστημα τερματικών λειτουργιών (TOS)
OT
Φόρτωση / Εκφόρτωση
Προστασία και ασφάλεια
Έλεγχος πρόσβασης
Ανίχνευση συστήματα
Κλειστά κυκλώματα τηλεόρασης, κάμερες,..
Συναγερμοί
Αρχές
Εθνικά συστήματα
Ευρωπαϊκά συστήματα
Δορυφορικά Συστήματα (GNSS, Παρακολούθηση)
Τράπεζες
Υποχρεωτικές δηλώσεις Άδειες και έλεγχοι Λειτουργικά δεδομένα
Οικονομικά δεδομένα
Δεδομένα περιήγησης

Απειλές

Απειλές στον θαλάσσιο τομέα

Ταξινόμηση απειλών

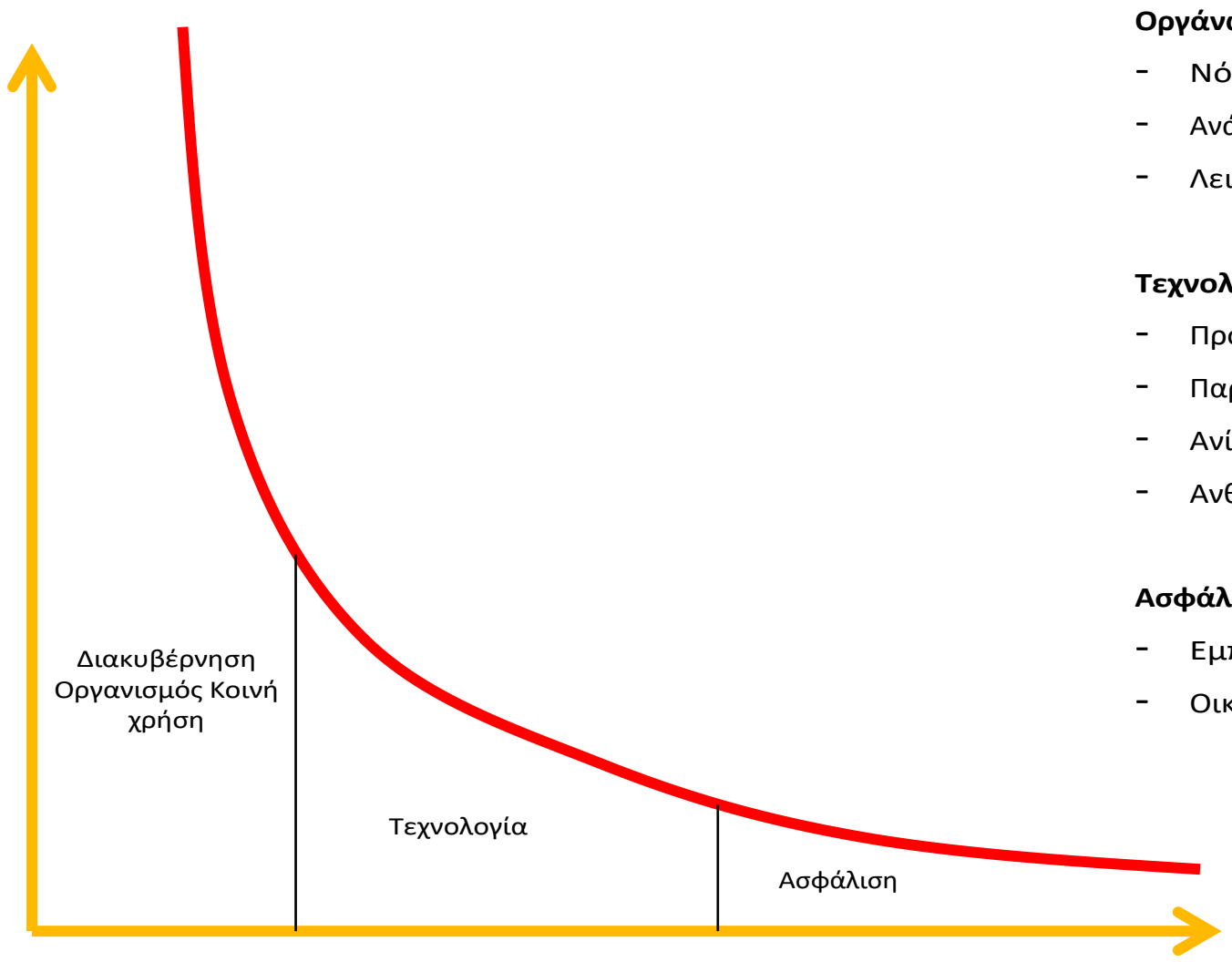


Μείωση των κινδύνων για κρίσιμες υποδομές

Ναυτιλία

ΛΙΜΑΝΙΑ ΚΑΙ ΝΑΥΤΙΛΙΑΚΟΙ ΕΝΔΙΑΦΕΡΟΜΕΝΟΙ

Στρατηγικές και αποτελέσματα μείωσης των κινδύνων για την ασφάλεια στον κυβερνοχώρο



Οργάνωση

- Νόμος / Διακυβέρνηση
- Ανάλυση κινδύνου
- Λειτουργική / τομεακή ανθεκτικότητα

Τεχνολογική

- Πρόληψη
- Παρακολούθηση / επιτήρηση
- Ανίχνευση & ανταλλαγή πληροφοριών για περιστατικά
- Ανθεκτικότητα

Ασφάλιση

- Εμπιστοσύνη
- Οικονομική υποστήριξη / ανασυγκρότηση

ΕΡΩΤΗΣΕΙΣ - ΔΙΑΛΕΙΜΜΑ