Κυβερνοασφάλεια και εμπορικό πλοίο

Νικήτας Νικητάκος
Καθ. Πανεπιστημίου Αιγαίου
Κέντρο Μελετών Ασφάλειας

Στόχοι

- Έρευνα και αναλύσεις για την εσωτερική ασφάλεια
- Υποβοήθηση του Υπουργείου Προστασίας του Πολίτη σε πολιτικές προστασίας του πολίτη και πρόληψης εγκλήματος .
- Διαχείριση, εκμετάλευση και δίαχυση γνώσης και εμπειρίας σε εσωτερική ασφάλεια και σε θέματα διεθνούς ασφάλειας
- Συμμετοχή σε ερευνητικά προγράμματα και σε επιστημονικές μελέτες και αναλύσεις σε θέματα ασφάλειας
- Συμβουλευτικές Υπηρεσίες σε Υπουργεία σε θέματα ασφάλειας και προστασίας κρίσιμών υποδομών

Στρατηγικοί Πυλώνες

Διεθνείς συνεργασίες

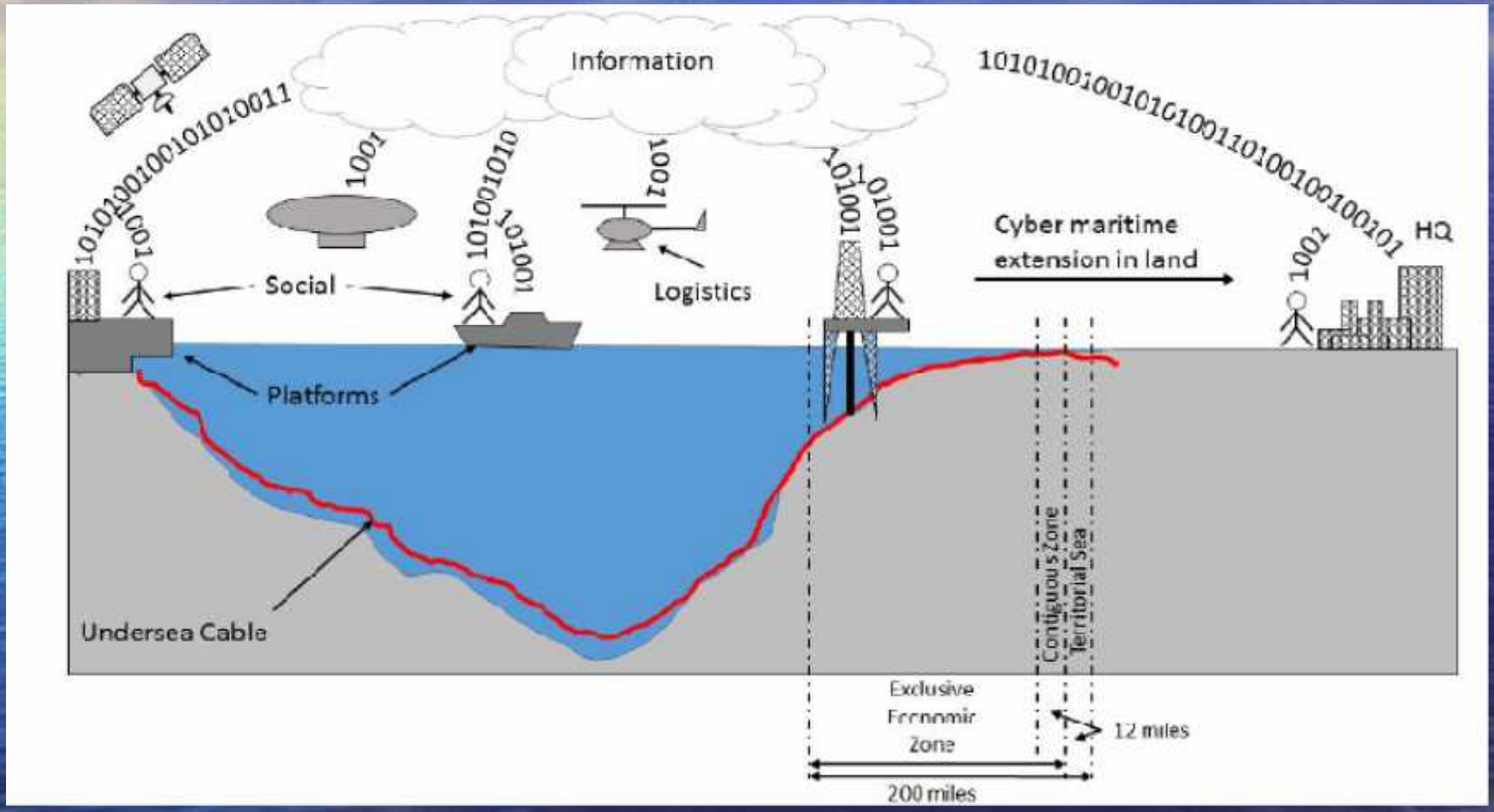
Έρευνα

Συμβουλευτικές Υπηρεσίες

Περίγραμμα Παρουσίασης

- Εισαγωγή
- Κυβερνοεπιθέσεις και πλοία
- Ευάλωτα συστήματα πλοίου
- Συμβάντα κυβερνοεπιθέσεων
- Αντιμετώπιση
- Σημερινή κατάσταση – Βελτιώσεις
- Το μέλλον

Πλαίσιο Εμπορικής ναυτιλιακής δραστηριότητας



Κυβερνοεπιθέσεις και πλοία

- Τα πλοία ναυλώνονται από τρίτους
- Ο πλοιοκτήτης δεν έχει πλήρη έλεγχο στα πληροφοριακά συστήματα που απαιτούν οι ναυλωτές.
- Τα πλοία λειτουργούν κυρίως offline. Η σημερινή κυβερνοασφάλεια δεν μπορεί να ελεγχθεί με αποφυγή διαδυνδεσιμότητας
- Κρίσιμα δεδομένα σχετικά με το φορτίο περνούν από μεγάλο αριθμό συστημάτων ξηράς και κάνει ποιό εύκολη την διείσδυση
- Υψηλής αξιοπιστίας ηλεκτρονικά συστήματα ασφαλείας όπως ECDIS και δορυφορικοί δέκτες κάνουν το πλοίο ποιο ευάλωτο σε κυβερνοεπειθέσεις

Κυβερνοεπιθέσεις και πλοία

- Το πλοίο είναι μια ανεξάρτητη μονάδα και μια κυβερνοεπίθεση μπορεί να δημιουργήσει κινδύνους στην ασφάλεια του στο περιβάλλον και στην συνέχεια της επιχειρηματικής δραστηριότητας της πλοιοκτήτριας εταιρείας
- Σε μεγάλο ποσοστό το πλήρωμα έχει τις ίδιες διαδικασίες αντιμετώπισης όπως σε κάθε άλλο κίνδυνο

Ευάλωτα συστήματα πλοίου

- Συστήματα Ελέγχου Πλοίου και Πρόωσης ;
- Συστήματα ναυσιπλοΐας περιλαμβανομένων GPS, AIS, ECDIS, αυτόματο πιλότο, radar, gyrocompass, dynamic positioning, VDR;
- Βιομηχανικά συστήματα ελέγχου πλοίου όπως πρόωσης, πηδαλιουχίας, ballast-water management, ηλεκτρικά συστήματα, κλιματισμός, συστήματα ευστάθειας, φορτίου, εντοπισμού πυρκαιάς και
- Επικοινωνίες και συστήματα παρακολούθησης όπως κάμερες ασφάλειας, συστήματα ειδοποίησης, επικίνδυνων αερίων και ελέγχου ρύπανσης περιβάλλοντος .

Ευάλωτα συστήματα πλοίου

Έλλειψη παρακολούθησης λογισμικού και συστημάτων

Μη ελεγχόμενη πρόσβαση σε υπολογιστές και δίκτυα

Εισαγωγή κακόβουλου λογισμικού από το εσωτερικό του πλοίου .

Μη ενημερωμένο λογισμικό

Έλεγχος από απόσταση

Συμβάντα κυβερνοεπιθέσεων (1/2)

- Κλοπή χρημάτων με κυβερνοεπίθεση
- Λαθρεμπόριο ναρκωτικών και διαγραφή εμπορευματοκιβωτίων από λιμάνι
- Zombie Zero: Με χρήση barcode scanners πρόσβαση στο λογιστικό σύστημα
- Icefog: backdoor πρόσβαση σε Ιαπωνικές και Κορεάτικες εταιρείες και ναυπηγεία (extract documents, gain email access, obtain passwords)

- Παράκαμψη των Αυστραλιανών τελωνείων

Συμβάντα κυβερνοεπιθέσεων (2/2)

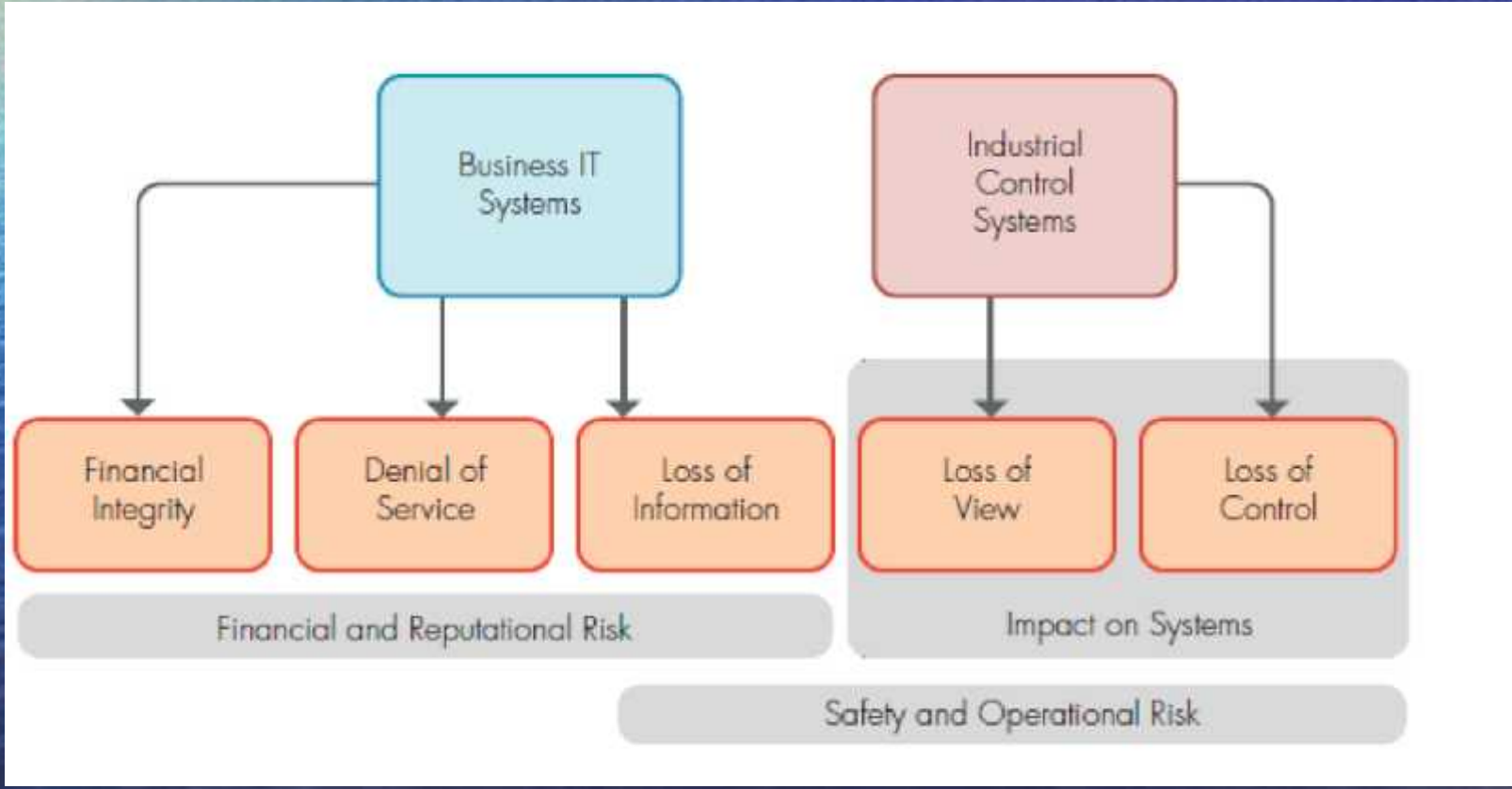
- Απώλεια ευστάθειας πλατφόρμας εξαγωγής πετερλαίου
- Διακοπή λειτουργίας πλωτής πλατφόρμας από κακόβουλο λογισμικό
- Υποκλοπή και πλαστογράφηση του AIS
- GPS Jamming
- Παρεμβολή στα δεδομένα του ECDIS
- Πλοήγηση από απομακρυσμένη θέση ενός 80 εκατ. $ yacht με χρήση συσκευών αξίας 3000 USD
- Facebook πηγη πληροφορίων για πειρατές

Συστήματα Βιομηχανικού Ελέγχου

SCADA (Supervisory Control and Data Acquisition)

Συστήματα Βιομηχανικού Ελέγχου στα πλοία

Shodan is the world's first search engine for Internet-connected devices. https://www.shodan.io/



Κατηγορίες επιτιθέμενων

3 κύριες κατηγορίες:

Ποινικοί

Κίνητρο: Χρήματα

Δραστηριότητες: κλοπή χρημάτων με απάτη, διευκόλυνση λαθρεμπορίου, λύτρα

Hacktivists

Κίνητρο: πολιτικά, δημιουργία αναταραχής Ι

Δραστηριότητες: Καταστροφή/ υποβάθμιση υποδομών , δημοσιοποίηση ευαίσθητων πληροφοριών , έλεγχος διάυλων επικοινωνίας

Κυβερνήσεις (ή κυβερνητικοί οργανισμοί)

Κίνητρο: Κατασκοπεία , κρίσιμες υποδομές

Αντιμετώπιση (1/2)

- Οι τεχνικές κυβερνοεπιθέσεων βελτιώνονται συνεχώς οπότε η αντιμετώπιση τους χρειάζεται συνέχεια προσαρμογές
- Η διαδικασία έγκρισης κανονισμών του IMO είναι πολύ αργή
- Η έγκριση τύπου του λογισμικού δεν είναι αρκετή καθόσον είναι στατική διαδικασία
- Υπάρχουν καλές πρακτικές από άλλους τομείς

Αντιμετώπιση (2/2)

- Θέματα κυβερνοασφάλειας σε νέες κατασκευές ή σε αγορές μεταχειρισμένων
- Ειδικότερα στις νέες κατασκευές θα πρέπει να υπάρχει διασφάλιση ποιότητας λογισμικού με ιδιαίτερη έμφαση στην κυβερνοασφάλεια και κατάλληλη σχεδίαση ηλεκτρονικών δικτύων
- Συνδυασμός με την συντήρηση λογισμικού πάνω στο πλοίο
- Σε περιπτώσεις συνεχούς σύνδεσης on-line

Σημερινή κατάσταση

- Χαμηλό το επίπεδο κυβερνοασφάλειας στην ναυτιλία
- Τεχνολογία: χαμηλό επίπεδο ασφάλειας ναυτιλιακών ιστοτόπων (cyberkeel survey)
- Οργάνωση και ευρύτερη ενημέρωση βασικά προβλήματα.
- Η διαχείριση των ηλεκτρονικών συστημάτων πλοίου γίνεται κύρια από ξηρά
- Εκπαίδευση, καθήκοντα, διαδικασίες

Βελτίωση της κατάστασης

- Έμφαση στους εσωτερικούς κινδύνους
- Συχνός έλεγχος εφαρμογών λογισμικού και συσκευών
- Ανθρώπινος παράγων
- Οργάνωση ώστε να υπάρχει cyber-resilient
- Εκπαίδευση

Το μέλλον

- Μη γραμμική τεχνολογική ανάπτυξη
- Εκθετική ανάπτυξη σε χωρητικότητα
- Αυτοματισμοί και Ολοκλήρωση
- Ανοικτό λογισμικό και Standards
- Μεγάλη ποσότητα πληροφοριών (Big Data)
- Ασύμμετρες επιθέσεις
- Διαθεσιμότητα πληροφοριών
- Διασυνδεσιμότητα

KEMEA
ΚΕΝΤΡΟ ΜΕΛΕΤΩΝ ΑΣΦΑΛΕΙΑΣ
CENTER FOR SECURITY STUDIES

UNIVERSITY OF THE AEGEAN
Department of Shipping
Trade and Transport

Ευχαριστώ για την προσοχή σας

nnik@aegean.gr