ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Κυβερνοασφάλεια στη Ναυτιλιακή Βιομηχανία** **Cybersecurity in Maritime Industry**
Ονοματεπώνυμο Φοιτητή	**Καλφόπουλος Νικόλαος**
Πατρώνυμο	**Γρηγόριος**
Αριθμός Μητρώου	**ΜΠΠΛ18022**
Επιβλέπων	**Πατσάκης Κωνσταντίνος, Αναπλ. Καθηγητής**

Ημερομηνία Παράδοσης **Δεκέμβριος 2022**

Τριμελής Εξεταστική Επιτροπή

Πατσάκης Κ. Αναπλ. Καθηγητής	Αλέπης Ε. Αναπλ. Καθηγητής	Σακκόπουλος Ε. Αναπλ. Καθηγητής

(Blank page)

Πίνακας περιεχομένων

Πίνακας εικόνων 5
Περίληψη 7
Abstract 7
Εισαγωγή 8
Κεφάλαιο 1: Cyber Security – Κυβερνοασφάλεια 9
1.1 Ορισμός 9
1.2 Cyber Threats – Κυβερνοαπειλές 9
1.2.1 Κακόβουλο λογισμικό (malicious Software - malware) 12
1.2.2 Επιθέσεις από το διαδίκτυο (web based attacks) 13
1.2.3 Επιθέσεις ηλεκτρονικού ψαρέματος (Phishing) 13
1.2.4 Επιθέσεις σε διαδικτυακές εφαρμογές (Web Application Attacks) 14
1.2.5 Ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου (Spam) 14
1.2.6 Επιθέσεις κατανεμημένης άρνησης υπηρεσίας (Distributed Denial of Service) 15
1.2.7 Κλοπή ταυτότητας χρήστη (Identity Theft) 15
1.2.8 Παραβίαση Δεδομένων (Data Breach) 16
1.2.9 Εσωτερικές απειλές (Insider Threats) 16
1.2.10 Botnets 16
1.2.11 Φυσικές απειλές 17
1.2.12 Διαρροή Δεδομένων 17
1.2.13 Λογισμικό Λύτρων (ransomware) 17
1.2.14 Ηλεκτρονική κατασκοπία (Cyber Espionage) 17
1.2.15 Cryptojacking 18
1.2.16 Man-in-the-middle 18
1.2.17 HoneyPot 19
1.3 Μέτρα πρόληψης 19
1.4 Κανονισμοί και νομοθεσία 21
Κεφάλαιο 2: Ναυτιλία και Τεχνολογία 28
2.1 Εισαγωγικό Σημείωμα 28
2.2 Συστήματα γέφυρας / πλοήγησης 30
2.2.1 Global Navigation Satellite Systems 35
2.2.2 Global Positioning System 39
2.2.3 Automatic Identification System 41
2.2.4 Electronic Chart Display and Information System – ECDIS 46
2.2.5 Radar 48
2.3 Συστήματα επικοινωνίας 50
2.4 Άλλα συστήματα – ελέγχου, μηχανής, έρευνας 53
2.4.1 Συστήματα ελέγχου μηχανής 53
2.4.2 Συστήματα ελέγχου έρματος 56

2.4.3 Συστήματα φόρτωσης και ισορροπίας φορτίου 59
2.4.4 Συστήματα ασφαλείας 63
2.4.5 Καταγραφείς δεδομένων ταξιδιού 65
Κεφάλαιο 3: Περιστατικά στο Ναυτιλιακό Τομέα 68
3.1 Εισαγωγικό Σημείωμα 68
3.2 Περιστατικά στα συστήματα γέφυρας/πλοήγησης 71
3.2.1 GNSS 72
3.2.2 GPS 74
3.2.3 AIS 77
3.2.4 ECDIS 78
3.2.5 Radar 81
3.3 Περιστατικά στα συστήματα επικοινωνίας 82
3.4 Περιστατικά σε άλλα συστήματα 84
3.4.1 ECR 84
3.4.2 BMWS 86
3.4.3 Bay/Stowage Plan 87
3.4.4 Security Systems 88
3.4.5 VDR 89
3.5 Περιστατικά στο Σύστημα Θαλάσσιων Μεταφορών 90
3.5.1 Επιβατηγά πλοία 90
3.5.2 Ναυτιλιακές εταιρείες 91
3.5.3 Λιμάνια 92
3.5.4 Εξέδρες πετρελαίου 94
3.5.5 Emotet 95
Κεφάλαιο 4: Κυβερνοασφάλεια και Ναυτιλία 97
4.1 Ρυθμιστικό πλαίσιο στη Ναυτιλία 97
4.2 Λύσεις στον ναυτιλιακό τομέα 104
4.2.1 Πιστοποιητικά προμηθευτών 105
4.2.2 Εκτίμηση κινδύνου 105
4.2.3 Εκπαίδευση – Ανθρώπινο Δυναμικό 108
4.2.4 Λογισμικό προστασίας – Ενημερώσεις Ασφαλείας και εξωτερικά μέσα 109
4.2.5 Τοπολογία – Δίκτυο - Firewalls 110
4.2.6 Κωδικοί και κρυπτογράφηση 111
4.2.7 Jamming And Spoofing στην Πλοήγηση 111
4.2.8 Δορυφορικές Επικοινωνίες 114
4.3 Ναυτιλιακά Σεμινάρια για την Κυβερνοασφάλεια 114
4.4 Αναζητήσεις Shodan 116
Κεφάλαιο 5: Συμπεράσματα 128
Βιβλιογραφία 130

Πίνακας εικόνων

Εικόνα 1 - Άτομα και κίνητρα κυβερνοαπειλής ... 11
Εικόνα 2 - ENISA Threat Landscape Report 2020, 15 Top Cyberthreats and Trends ... 12
Εικόνα 3 - Παράδειγμα συμφόρησης από μη νόμιμα αιτήματα ... 15
Εικόνα 4 - Τεχνικές και τύποι επίθεσης MitM ... 18
Εικόνα 5 - Τρισδιάστατη ταξινόμηση ... 24
Εικόνα 6 - Ομάδες διεθνών / περιφερειακών οργανισμών ... 26
Εικόνα 7 - Σύστημα θαλάσσιων μεταφορών ... 28
Εικόνα 8 - Συστήματα κυβερνοχώρου στα πλοία ... 29
Εικόνα 9 - Τεχνολογικά συστήματα πάνω στο πλοίο ... 30
Εικόνα 10 - Σύνθεση ενός ολοκληρωμένου συστήματος πλοήγησης ... 31
Εικόνα 11 - Automatic Identifications System ... 31
Εικόνα 12 - ECDIS ... 32
Εικόνα 13 – Βυθόμετρο ... 32
Εικόνα 14 - GPS Receiver ... 32
Εικόνα 15 - Γυροσκοπική Πυξίδα ... 33
Εικόνα 16 - Μαγνητική πυξίδα ... 33
Εικόνα 17 - Αυτόματος πιλότος ... 33
Εικόνα 18 – a) Radar b) ARPA ... 34
Εικόνα 19 – Sound Reception System ... 34
Εικόνα 20 - a)Speed&Distance Log Device b)Rudder Angle Indicator c)Rate of turn indicator ... 35
Εικόνα 21 - Transmitting Heading Device ... 35
Εικόνα 22 - Τροχιά δορυφόρων GNSS ... 37
Εικόνα 23 - Satellite Based Augmentation System ... 38
Εικόνα 24 - Διαδικασία τριπλοποίησης (trillateration) ... 40
Εικόνα 25 - a) AIS950 Class A b) AIS350 Class B c) AIS350 Class C ... 43
Εικόνα 26 - Αρχιτεκτονική AIS ... 43
Εικόνα 27 - Απειλές που σχετίζονται με το AIS ... 44
Εικόνα 28 - Αρχιτεκτονική συστήματος ECDIS. ... 46
Εικόνα 29 - Τα βασικά στοιχεία του RADAR. ... 48
Εικόνα 30 - Μοντέλο επίθεσης σε σύστημα a) Radar, b) AIS/ECDIS ... 49
Εικόνα 31 - Ένα ECR σε ένα μεγάλο σύγχρονο κρουαζιερόπλοιο. ... 54
Εικόνα 32 – MOXA – case study - Ψηφιοποίηση συστημάτων ελέγχου κινητήρα για λειτουργική απόδοση ... 55
Εικόνα 33 - Ενδεικτική εικόνα ενός Human Machine Interface ελέγχου συστήματος έρματος. ... 57
Εικόνα 34 -Σενάριο επίθεσης στο σύστημα ελέγχου έρματος ... 58
Εικόνα 35 – Σενάριο επίθεσης στο BWMS ... 59
Εικόνα 36 - Πρόγραμμά διαχείρισης φορτίου σε εμπορευματοκιβώτια. ... 60
Εικόνα 37 - Sagging και Hogging ... 62
Εικόνα 38 - Λειτουργία Σύστηματος Προειδοποίησης Ασφάλειας Πλοίου ... 64
Εικόνα 39 - Voyage Data Recorder ... 65
Εικόνα 40 - Τυπική αρχιτεκτονική ενός συστήματος VR-3000 ... 66
Εικόνα 41 - Τεχνολογία πληροφορικής και λειτουργίας ... 68
Εικόνα 42 - Συμβάντα στον ναυτιλιακό κλάδο ... 68
Εικόνα 43 - Πληροφορίες για την φύση των περιστατικών από τους ερωτηθέντες της έρευνας. 69
Εικόνα 44 - Περιοχές που θεωρούνται πιο ευάλωτες σε επιθέσεις ... 69
Εικόνα 45 - Πίνακας αποτελεσμάτων ερευνών ... 70
Εικόνα 46 - Σύνθεση συλλεγόμενων στοιχείων τρωτότητας. ... 71
Εικόνα 47 - Black sea Spoofing Activity ... 72
Εικόνα 48 – Επισκόπηση γεγονότων πλαστογράφησης GNSS που επηρέασαν τη θαλάσσια κυκλοφορία μεταξύ των ετών 2008 και 2020 ... 73
Εικόνα 49 - GNSS Spoofing ... 73

Εικόνα 50 - Princess Janice από το Point Reyes στην ενδοχώρα, κυκλικές κινήσεις στη Γιούτα και πίσω στη Νιγηρία 75
Εικόνα 51 - Πέντε πλοία που «εκτοπίστηκαν» στο Point Reyes, από μέρη σε όλο τον κόσμο. . 76
Εικόνα 52 - Πλοία-φαντάσματα που κάνουν κύκλους ανοιχτά της Καλιφόρνιας..... 76
Εικόνα 53 - Δείγμα προτάσεων AIVDM για αναφορές θέσεις (πάνω) και στατικές (κάτω)..... 77
Εικόνα 54 - Πλαστογράφηση AIS..... 77
Εικόνα 55 - Επιθέσεις AIS και δημιουργία ψεύτικων a) πλοίων b) AtoN 78
Εικόνα 56 - a) Κανονικό b) Αλλαγή θέσης c) Αλλαγή μεγέθους..... 80
Εικόνα 57 - Πορεία Wakashio στον Ινδικό Ωκεανό 81
Εικόνα 58 - Αποτελέσματα ανάλυσης MITRE ATT&CK στα συστήματα επικοινωνίας..... 82
Εικόνα 59 - Σενάριο επίθεσης μέσω CVE..... 83
Εικόνα 60 - Κυβερνοεπίθεση εναντίον μιας γεννήτριας ενέργειας 85
Εικόνα 61 – Κλίση εξέδρας πετρελαίου..... 94
Εικόνα 62- Διαδικασία PDCA 98
Εικόνα 63 - Κύρια Δομή Πλαισίου 99
Εικόνα 64 - Προσέγγιση διαχείρισης κινδύνων στον κυβερνοχώρο όπως ορίζεται στις κατευθυντήριες γραμμές BIMCO. 106
Εικόνα 65 - Διάγραμμα ροής μεθόδου CYRA-MS 107
Εικόνα 66 - Αναζητήσεις με VSAT..... 118
Εικόνα 67 - Αναζήτηση VSAT 119
Εικόνα 68 - Εύρημα Sailor 900..... 119
Εικόνα 69 - Αναζήτηση CommBox..... 120
Εικόνα 70 - Γραφικός Ιχνηλάτης Shodan 120
Εικόνα 71 - Αναζήτηση Inmarsat..... 121
Εικόνα 72 - Αναζήτηση Thrane / Sailor 800 121
Εικόνα 73 – Fleet..... 122
Εικόνα 74 - Vessel..... 123
Εικόνα 75 - Passenger ship..... 123
Εικόνα 76 - Cobham Vessel..... 124
Εικόνα 77 – AIS Vessel..... 124
Εικόνα 78 – ECDIS..... 125
Εικόνα 79 - Ship GPS..... 125
Εικόνα 80 – EPIRB..... 126
Εικόνα 81 - Vessel SART..... 126
Εικόνα 82 - Ballast water..... 127

Περίληψη

Η παρούσα εργασία πραγματεύεται το ζήτημα της Κυβερνοασφάλειας στη Ναυτιλιακή Βιομηχανία. Σκοπός της είναι να αναδειχτεί η αναγκαιότητα τήρησης μέτρων ασφαλείας στα ναυτιλιακά συστήματα προκειμένου να εξασφαλιστεί η ομαλότητα ακόμη και η βελτίωση των υπηρεσιών τους. Κατ' αρχάς παρατίθεται μία αναφορά στο ρόλο που παίζει η ναυτιλία στην κοινωνία μας. Στο πρώτο κεφάλαιο αναλύεται ο όρος Κυβερνοασφάλεια και στη συνέχεια αναφέρονται οι πιο γνωστές περιπτώσεις απειλών στον κυβερνοχώρο. Μετέπειτα, μέσα από την παρουσίαση των σύγχρονων συστημάτων ψηφιοποίησης δεδομένων που χρησιμοποιούνται στη ναυτιλία οδηγούμαστε στο συμπέρασμα ότι η σπουδαιότητα καθώς και η εμπιστευτικότητα των δεδομένων αυτών καθιστούν απαραίτητη την ασφάλειά τους. Παρουσιάζονται περιστατικά επιθέσεων από τον ναυτιλιακό τομέα καθώς και το ρυθμιστικό πλαίσιο που υπάρχει. Τέλος, προτείνονται τρόποι αντιμετώπισης ή τουλάχιστον ελαχιστοποίησης των κινδύνων μαζί με ορισμένα ευρήματα στην διαδικτυακή πλατφόρμα αναζήτησης Shodan.

Abstract

This paper addresses the issue of Cybersecurity in the Shipping Industry. Its purpose is to highlight the need for safety measures in maritime systems in order to ensure the smoothness and even the improvement of their services. First, there is a reference to the role that shipping plays in our society. The first chapter analyzes the term Cybersecurity and then lists the most well-known cases of cyber threats. Then, through the presentation of modern data digitization systems used in shipping, we conclude that the importance as well as the confidentiality of this data make their security necessary. Incidents of attacks from the shipping sector as well as the existing regulatory framework are presented. Finally, ways to address or at least minimize the risks are suggested along with some findings on the Shodan online search platform.

Εισαγωγή

Η ναυτιλία στις μέρες μας διαδραματίζει πολύ σημαντικό ρόλο στη ζωή των ανθρώπων, καθώς αποτελεί το πιο αξιόλογο μέσο για την εκπλήρωση μεταφορών τόσο αγαθών όσο και ανθρώπων (με τις θαλάσσιες μεταφορές από μόνες τους να αντιπροσωπεύουν σχεδόν το 90% του παγκόσμιου εμπορίου). Είναι ζωτικής σημασίας καθώς είναι ένας από τους μεγαλύτερους τομείς στην οικονομία ενός κράτους. Για τον λόγο αυτό, κρίνεται αναγκαίο να τεθούν και θέματα ασφάλειας. Ήδη στον ναυτιλιακό κλάδο έχουν θεσπισθεί διάφοροι κανονισμοί για την ασφάλεια στη θάλασσα, όσον αφορά ατυχήματα, απώλεια ζωής και περιβαλλοντικές καταστροφές. Στον 21ο αιώνα που ζούμε, όμως, εγκυμονούν και άλλοι κίνδυνοι πέρα από την φυσική καταστροφή, όπως είναι τα τρωτά σημεία που προκύπτουν από την ραγδαία ανάπτυξη της τεχνολογίας. Ωστόσο, η τελευταία έχει σαφώς να επιδείξει και μεγάλα επιτεύγματα που αφορούν στην διευκόλυνση της καθημερινότητάς μας, όπως είναι η ρομποτική αλλά και η ψηφιοποίηση και η αποθήκευση των δεδομένων μας σε ένα νέφος (cloud) που όπως είναι φανερό ανταποκρίνονται και στον κλάδο της ναυτιλίας εφόσον προσφέρουν βελτίωση σε θέματα ταχύτητας και οικονομίας. Πράγματι στη ναυτιλία η τεχνολογία έχει αλλάξει θεαματικά. Μπορούμε να πάρουμε και ως παράδειγμα τα έξυπνα λιμάνια που πλέον δεν έχουν ανθρώπινο δυναμικό για την ταξινόμηση των εμπορευματοκιβωτίων στην ενδοχώρα, την λήψη αποφάσεων μέσα από την συλλογή ψηφιακών δεδομένων αλλά και τα έξυπνα πλοία που σιγά σιγά υιοθετούνται για την εξυπηρέτηση των μεταφορών. Τα παραπάνω καθιστούν αναγκαία την ένταξη ενός νέου τύπου ασφάλειας στη ναυτιλία που ονομάζεται κυβερνοασφάλεια.

Κεφάλαιο 1: Cyber Security – Κυβερνοασφάλεια

1.1 Ορισμός

Αρχικά, καλό είναι να ξεκινήσουμε με το να ορίσουμε τι είναι η κυβερνοασφάλεια και που δραστηριοποιείται. **Κυβερνοχώρος** (Cyber Space) λοιπόν είναι το περιβάλλον που δημιουργείται από δίκτυα επικοινωνιών που χρησιμοποιούν ηλεκτρονικούς υπολογιστές είτε αυτά είναι τοπικά δίκτυα (LAN) ή ευρείας εμβέλειας δίκτυα (WAN) όπως είναι το internet για ίδιες δραστηριότητες σε εθνικά και παγκόσμια δίκτυα. (Wikipedia, 2021). **Κυβερνοασφάλεια** είναι η διαδικασία κατά την οποία προσπαθούμε να αποτρέψουμε τυχόν ψηφιακές απειλές. Είναι η προστασία συστημάτων συνδεδεμένων στο Διαδίκτυο συμπεριλαμβανομένων υλικού, λογισμικού και δεδομένων από επιθέσεις σε αυτόν τον χώρο (Hub, 2020) . Ο ορισμός μπορεί να δοθεί και αντίστροφα, εξετάζοντας, δηλαδή, από τι θέλουμε να προστατευτούμε, δηλαδή από μία **κυβερνοεπίθεση**. Σε υπολογιστές και δίκτυα υπολογιστών, μια επίθεση είναι κάθε προσπάθεια έκθεσης, αλλαγής, απενεργοποίησης, καταστροφής, κλοπής ή απόκτησης πληροφοριών μέσω μη εξουσιοδοτημένης πρόσβασης ή χρήσης ενός περιουσιακού στοιχείου. Η επίθεση στον κυβερνοχώρο είναι κάθε επιθετικός ελιγμός που στοχεύει συστήματα πληροφορικής, υποδομές, δίκτυα υπολογιστών ή προσωπικές συσκευές υπολογιστή. Ένας εισβολέας είναι ένα δυνητικά κακόβουλο άτομο ή διαδικασία που επιχειρεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε δεδομένα, λειτουργίες ή άλλους περιορισμένους τομείς ενός συστήματος. Ανάλογα με το πλαίσιο, οι επιθέσεις στον κυβερνοχώρο μπορούν να αποτελούν μέρος του κυβερνοπολέμου (cyberwarfare) ή του κυβερνοτρομοκρατισμού (cyberterrorism). Μια διαδικτυακή επίθεση μπορεί να χρησιμοποιηθεί από κυρίαρχα κράτη, άτομα, ομάδες, κοινωνίες ή οργανισμούς και μπορεί να προέρχεται από μια ανώνυμη πηγή (Wikipedia, 2021).

Ο **Σκοπός της Κυβερνοασφάλειας** είναι να εξασφαλίσουμε για τα δεδομένα μας τα παρακάτω:

I. **Confidentiality (Εμπιστευτικότητα των δεδομένων)** : Πρέπει να σκεφτούμε τρόπους να εξασφαλίσουμε ότι τα αρχεία που θέλουμε να **παραμείνουν ιδιωτικά** ή εμπιστευτικά **δεν θα είναι διαθέσιμα σε κάποιον τρίτο**.
II. **Integrity (Ακεραιότητα των δεδομένων):** Τα δεδομένα μας θα πρέπει να **παραμένουν αναλλοίωτα** όχι μόνο με την πάροδο του χρόνου αλλά και από σκόπιμες ή μη καταστροφές ή άλλων ειδών ατυχήματα, όπως για παράδειγμα η καταστροφή ενός σκληρού δίσκου. Κρίνεται αναγκαία η εφαρμογή κατάλληλων μέτρων - εργαλείων που θα εξασφαλίζουν την ακεραιότητα των δεδομένων από κάποιον πιθανό κακόβουλο χρήστη.
III. **Availability (Διαθεσιμότητα των αρχείων):** Τα δεδομένα που αποθηκεύουμε θα πρέπει **να είναι πάντα στη διάθεσή μας**. Καλό είναι να υπάρχουν εφεδρικά μέσα αποθήκευσης (back up) για την εξασφάλιση της πρόσβασής μας σε αυτά ανεξαρτήτως χωροχρόνου. (tictac laboratories, 2021)

Οπότε, θα μπορούσαμε να θέσουμε την κυβερνοασφάλεια ως ένα μέσο προστασίας από μία επίθεση που εξαπολύεται από έναν υπολογιστή εναντίον ενός ιστοτόπου, ενός υπολογιστικού συστήματος ή μεμονωμένου υπολογιστή που στοχεύει την **ακεραιότητα, την εμπιστευτικότητα ή την διαθεσιμότητα** του στόχου και των πληροφοριών που είναι αποθηκευμένα σε αυτό (The Windows Club, 2021)

1.2 Cyber Threats – Κυβερνοαπειλές

Υπάρχουν πολλές ψηφιακές απειλές που έχουν ως σκοπό την παράνομη πρόσβαση σε πληροφορίες, ώστε να καταστραφούν ευαίσθητου περιεχομένου ή υψηλής σημασίας δεδομένα για διάφορους λόγους, όπως είναι η απόσπαση χρημάτων ή η διακοπή ροής ενεργειών. Στην ουσία η παράνομη πρόσβαση έχει ως απώτερο σκοπό την στοχοποίηση ενός συστήματος κατά την οποία ο εισβολέας επωφελείται είτε από πληροφορίες ή ακόμη και από τον έλεγχο του ίδιου του συστήματος. (The Windows Club, 2021) Ο παγκοσμιοποιημένος χαρακτήρας του Διαδικτύου επιτρέπει σε αυτούς τους απειλητικούς παράγοντες να βρίσκονται φυσιολογικά οπουδήποτε στον

κόσμο και να εξακολουθούν να επηρεάζουν την ασφάλεια των συστημάτων πληροφοριών (Canadian Center for Cyber Security, 2021).

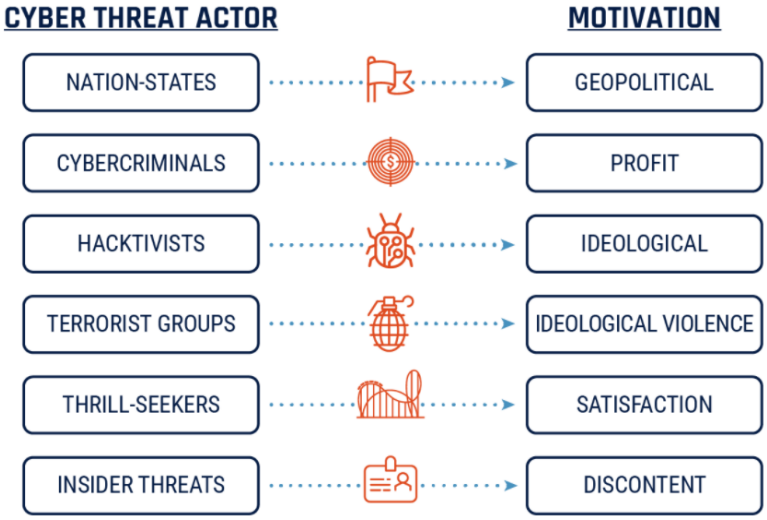
Οι απειλές στον κυβερνοχώρο γίνονται με ποικίλους τρόπους που θα παρουσιαστούν αναλυτικότερα και στη συνέχεια. Αναφορικά, πάντως, κάποιες απειλές είναι η απόκτηση ή απόπειρα απόκτησης μη εξουσιοδοτημένης πρόσβασης σε ένα σύστημα υπολογιστή ή στα δεδομένα του, η άρνηση παροχής υπηρεσιών (DDoS), η παραβίαση ιστοτόπου, η εγκατάσταση ιών και κακόβουλου λογισμικού, καθώς και η ακατάλληλη χρήση υπολογιστών ή εφαρμογών από υπαλλήλους μιας εταιρείας με τρόπο που βλάπτει την εταιρεία (The Windows Club, 2021).

Πρώτα από όλα, πρέπει να εξεταστούν τα άτομα ή οι ομάδες που βρίσκονται πίσω από αυτήν την επίθεση καθώς και τα πιθανά κίνητρα τους στην απόκτηση πρόσβασης σε τέτοιου είδους πόρους. Οι παράγοντες απειλής στον κυβερνοχώρο είναι κράτη, ομάδες ή άτομα που, με κακόβουλη πρόθεση, στοχεύουν να εκμεταλλευτούν τις ευπάθειες για να επηρεάζουν τα δεδομένα, τις συσκευές, τα συστήματα και τα δίκτυα των θυμάτων (Canadian Center for Cyber Security, 2021). Πιο συγκεκριμένα:

- **Εχθρικά έθνη-κράτη:** Τα εθνικά προγράμματα κυβερνοπολέμου παρέχουν αναδυόμενες απειλές που κυμαίνονται από **προπαγάνδα, καταστροφή ιστοτόπων, κατασκοπεία, διακοπή βασικών υποδομών έως απώλεια ζωής**. Τα εχθρικά έθνη-κράτη ενέχουν τον υψηλότερο κίνδυνο λόγω της ικανότητάς τους να χρησιμοποιούν αποτελεσματικά την τεχνολογία ενάντια στους πιο δύσκολους στόχους, όπως διαβαθμισμένα δίκτυα και κρίσιμες υποδομές, ηλεκτρικά δίκτυα και βαλβίδες ελέγχου αερίου.
- **Τρομοκρατικές ομάδες:** Οι τρομοκρατικές ομάδες χρησιμοποιούν όλο και περισσότερο κυβερνοεπιθέσεις για να **βλάψουν τα εθνικά συμφέροντα**. Είναι λιγότερο αναπτυγμένες κυβερνοεπιθέσεις αλλά είναι πιθανό να παρουσιάσουν σημαντικές απειλές στον κυβερνοχώρο καθώς όλο και πιο τεχνικά ικανές γενιές εντάσσονται στις τάξεις τους.
- **Εταιρικοί κατάσκοποι και οργανώσεις οργανωμένου εγκλήματος:** Διαπράττουν βιομηχανική κατασκοπεία για την κλοπή εμπορικών πληροφοριών ή μεγάλης κλίμακας χρηματοοικονομικής κλοπής. Γενικά, αυτά τα μέρη ενδιαφέρονται για δραστηριότητες που βασίζονται στο **κέρδος,** είτε να αποκομίσουν κέρδος είτε να διαταράξουν την ικανότητα μιας επιχείρησης να αποκομίσει κέρδος. Επιτίθονται σε βασικές υποδομές ανταγωνιστών, κλέβουν εμπορικές πληροφορίες ή αποκτούν πρόσβαση σε υλικό εκβιασμού.
- **Hacktivists:** Οι δραστηριότητες των Hacktivists ανάγονται σε **πολιτικά ιδανικά** και αξίες. Οι περισσότερες ομάδες ασχολούνται με την εξάπλωση προπαγάνδας προκειμένου να υποστηρίξουν τις πολιτικές τους πεποιθήσεις και όχι τόσο να προκαλέσουν τη μέγιστη ζημιά σε έναν οργανισμό.
- **Δυσαρεστημένοι εσωτερικοί:** Οι εσωτερικοί χρήστες συχνά δεν χρειάζονται υψηλό βαθμό γνώσεων υπολογιστών για να εκθέσουν ευαίσθητα δεδομένα, επειδή ενδέχεται να έχουν ήδη άδεια πρόσβασης σε αυτά. Οι απειλές εσωτερικών πληροφοριών περιλαμβάνουν επίσης τρίτους προμηθευτές και υπαλλήλους που ενδέχεται κατά λάθος να εισάγουν κακόβουλα προγράμματα σε συστήματα ή ενδέχεται να συνδεθούν, να κατεβάσουν και να μοιραστούν στο διαδίκτυο τα περιεχόμενά ενός σημαντικού φακέλου με αποτέλεσμα την **παραβίαση δεδομένων**.
- **Χάκερ:** Οι κακόβουλοι εισβολείς θα μπορούσαν να εκμεταλλευτούν μια ευπάθεια λογισμικού για να αποκτήσουν **μη εξουσιοδοτημένη πρόσβαση σε δεδομένα**. Οι χάκερ ενδέχεται να εισέλθουν σε συστήματα πληροφοριών για μια **πρόκληση ή υπερηφάνεια**.
- **Τυχαίες ενέργειες εξουσιοδοτημένων χρηστών:** Ένας εξουσιοδοτημένος χρήστης μπορεί να ξεχάσει να ρυθμίσει σωστά την ασφάλεια του συστήματος και τα διαπιστευτήρια, προκαλώντας πιθανή **διαρροή δεδομένων**. (upguard, 2021)

Ως κύριο κίνητρο των επιθέσεων αυτών θεωρείται η πρόκληση βλάβης στο σύστημα με απώτερο σκοπό όλων την απόκτηση πρόσβασης σε εμπιστευτικού περιεχομένου πληροφορίες προς όφελος του επιτιθέμενου ατόμου ή ομάδας. Τα **κίνητρα** θα μπορούσαν να χωριστούν σε τέσσερις κατηγορίες :

1. **Πολιτικά – εθνικά:** Ως τέτοιο κίνητρο μπορεί να θεωρηθεί μία επίθεση που αποσκοπεί στην προώθηση ενός μηνύματος με στόχο την ανάδειξη ενός ατόμου ή μιας ομάδας στην πολιτική σκηνή. Άλλο κίνητρο μπορεί να απορρέει από την επεκτατική πολιτική μιας χώρας (πόλεμος) ή την επικράτησή της έναντι μιας άλλης ή και για γεωπολιτικούς λόγους, κ.ά.
2. **Οικονομικά:** Στην περίπτωση αυτή η επίθεση γίνεται μέσω εγκατάστασης κακόβουλου λογισμικού (ransomware) και αποσκοπεί στην απόσπαση χρηματικού ποσού – λύτρα από το θύμα.
3. **Προσωπικά:** Προσωπικά κίνητρα θα μπορούσαν να θεωρηθούν η επίδειξη δύναμης, ο φθόνος ή η εκδίκηση προς ένα άλλο άτομο ή ακόμη και η προσωπική ικανοποίηση του επιτιθέμενου.



Εικόνα 1 - Άτομα και κίνητρα κυβερνοαπειλής. (Canadian Center for Cyber Security, 2021)

Όσον αφορά στις απειλές ποικίλλουν ανάλογα με τον σκοπό που υπηρετούν. Αυτές μπορεί να είναι οι ιοί των υπολογιστών, τα Ransomware, τα Malware, οι παραβιάσεις ηλεκτρονικών συστημάτων από κακόβουλους χρήστες (Hackers), η παραβίαση ηλεκτρονικής ταυτότητας, οι ηλεκτρονικές απάτες σε επίπεδο οργανισμών ή ιδιωτών κλπ. (insurance quality, 2021). Άλλες μορφές επιθέσεων στον κυβερνοχώρο αποτελούν η έγχυση κακόβουλου λογισμικού, το ηλεκτρονικό ψάρεμα (phishing), το social engineering. Άλλες προηγμένες αλλά κοινές μορφές είναι DDoS επιθέσεις και επιθέσεις Brute Force (The Windows Club, 2021).

Ο ENISA (Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια), είναι ένα ευρωπαϊκό κέντρο εμπειρογνωσίας για την ασφάλεια στον κυβερνοχώρο που βοηθά την ΕΕ και τα κράτη μέλη της να εξοπλίζονται και να προετοιμάζονται καλύτερα ώστε να προλαμβάνουν, να εντοπίζουν και να αντιμετωπίζουν προβλήματα που αφορούν την ασφάλεια των πληροφοριών (europa.eu, 2021). Στις 20 Οκτώβριου του 2020 δημοσίευσε τις top 15 κυβερνοαπειλές καθώς και

τις τάσεις που έχουν από το 2019 με 2020 όπως φαίνεται και στην παρακάτω εικόνα. (ENISA Threat Landscape - The year in review, 2021).

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	---	---
2	Web-based Attacks	---	↗
3	Phishing	↗	↗
4	Web application attacks	---	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	---	---
9	Insider threat	↗	---
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	---	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Legend: Trends: ↙ Declining, --- Stable, ↗ Increasing **Ranking**: ↗ Going up, --- Same, ↙ Going down

Εικόνα 2 - ENISA Threat Landscape Report 2020, 15 Top Cyberthreats and Trends (ENISA Threat Landscape - The year in review, 2021)

1.2.1 Κακόβουλο λογισμικό (malicious Software - malware)

Λογισμικό το οποίο έχει σχεδιαστεί ειδικά για να προκαλέσει ζημιά, όπως καταστροφή δεδομένων, ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα υπολογιστή. Περιλαμβάνει ιούς, worms, trojan horses κ.λπ. Σε αυτή την κατηγορία ανήκει και το λογισμικό λύτρων (ransomware) και η ηλεκτρονική κατασκοπία (Spyware) (Chroni, 2021). Το κακόβουλο λογισμικό παραβιάζει ένα δίκτυο μέσω μιας ευπάθειας. Συνήθως, όταν ένας χρήστης κάνει κλικ σε έναν επικίνδυνο σύνδεσμο ή σε ένα συνημμένο αρχείο στο email εγκαθιστά επικίνδυνο λογισμικό. Μόλις μπει στο σύστημα το κακόβουλο λογισμικό μπορεί να κάνει τα εξής:

1) Αποκλείει την πρόσβαση σε βασικά στοιχεία του δικτύου (ransomware),
2) Εγκαθιστά κακόβουλο λογισμικό ή πρόσθετο επιβλαβές λογισμικό,
3) Λαμβάνει κρυφά πληροφορίες διαβιβάζοντας δεδομένα από τον σκληρό δίσκο (spyware),
4) Διασπά ορισμένα στοιχεία και καθιστά το σύστημα μη λειτουργικό (cisco, 2021).

Πιο συγκεκριμένα, ένας ιός ενός υπολογιστή (virus) προσκολλάται σε ένα πρόγραμμα ή αρχείο, ώστε να μπορεί να εξαπλωθεί από έναν υπολογιστή σε άλλο, αφήνοντας λοιμώξεις καθώς μεταφέρεται. Ορισμένοι ιοί προκαλούν μόνο ελαφρώς ενοχλητικά αποτελέσματα, ενώ άλλοι μπορεί να προκαλέσουν βλάβη στο υλικό, το λογισμικό ή τα αρχεία. Σχεδόν όλοι οι ιοί είναι συνδεδεμένοι σε ένα εκτελέσιμο αρχείο, πράγμα που σημαίνει ότι ο ιός μπορεί να υπάρχει στον

υπολογιστή, αλλά δεν μπορεί να τον μολύνει εκτός εάν εκτελεστεί το κακόβουλο πρόγραμμα. Είναι σημαντικό να σημειωθεί ότι ένας ιός δεν μπορεί να εξαπλωθεί χωρίς ανθρώπινη δράση για να συνεχίσει να λειτουργεί. Αυτό γίνεται κατά κόρον εν αγνοία των χρηστών μοιράζοντας μολυσμένα αρχεία ή στέλνοντας email με ιούς.

Ένα σκουλήκι (computer worm) μοιάζει με έναν ιό στο σχεδιασμό του και θεωρείται υποκατηγορία του. Τα σκουλήκια εξαπλώνονται από υπολογιστή σε υπολογιστή, αλλά σε αντίθεση με έναν ιό, έχουν τη δυνατότητα να μεταφέρονται χωρίς βοήθεια από κάποιο άτομο, εκμεταλλεύοντας τις δυνατότητες μεταφοράς αρχείων ή πληροφοριών στο σύστημα. Ο μεγαλύτερος κίνδυνος με ένα σκουλήκι είναι η ικανότητά του να αναπαράγεται στο σύστημα, με αποτέλεσμα να στείλει εκατοντάδες ή χιλιάδες αντίγραφα του εαυτού του, δημιουργώντας ένα τεράστιο καταστροφικό αποτέλεσμα. Λόγω της φύσης αντιγραφής ενός worm και της ικανότητάς του να ταξιδεύει σε δίκτυα, το τελικό αποτέλεσμα στις περισσότερες περιπτώσεις είναι ότι το worm καταναλώνει πάρα πολύ μνήμη συστήματος (ή εύρος ζώνης δικτύου), με αποτέλεσμα οι διακομιστές Web, οι διακομιστές δικτύου και οι μεμονωμένοι υπολογιστές να σταματήσουν να ανταποκρίνονται. Το worm έχει σχεδιαστεί για να διοχετεύεται στο σύστημα και επιτρέπει σε κακόβουλους χρήστες να ελέγχουν τον υπολογιστή από απόσταση.

Ένα Δούρειο άλογο (trojan horse) είναι ένα καταστρεπτικό πρόγραμμα που μοιάζει με μια πραγματική εφαρμογή. Σε αντίθεση με τους ιούς, το Δούρειο άλογο δεν αναπαράγεται, αλλά μπορεί να είναι εξίσου καταστροφικό. Οι Trojans ανοίγουν επίσης μια είσοδο πίσω πόρτας στον υπολογιστή, η οποία παρέχει σε κακόβουλους χρήστες πρόσβαση στο σύστημα, επιτρέποντας την κλοπή εμπιστευτικών και προσωπικών πληροφοριών. (digicert, 2021)

1.2.2 Επιθέσεις από το διαδίκτυο (web based attacks)

Αυτές οι απειλές στοχεύουν άμεσα χρήστες εκμεταλλευόμενες ευπάθειες σε προγράμματα περιήγησης (browsers), και συστήματα διαχείρισης περιεχομένου (content management systems). Κυριότερα είδη επιθέσεων αυτής της κατηγορίας αποτελούν τα browser exploits[1], drive-by downolads[2], watering hole attacks[3], zero-day exploits[4] κ.α. (Chroni, 2021)

1.2.3 Επιθέσεις ηλεκτρονικού ψαρέματος (Phishing)

Το ηλεκτρονικό ψάρεμα (phishing) είναι ένας τύπος επίθεσης social engineering που χρησιμοποιείται συχνά για την κλοπή δεδομένων χρήστη, συμπεριλαμβανομένων των διαπιστευτηρίων σύνδεσης και των αριθμών πιστωτικών καρτών. Η επίθεση συνήθως λαμβάνει τη μορφή αλληλογραφίας SPAM, κακόβουλων ιστοτόπων, μηνυμάτων email ή άμεσων μηνυμάτων, που φαίνεται να προέρχονται από νόμιμη πηγή όπως τράπεζα ή κοινωνικό δίκτυο. Ο παραλήπτης στη συνέχεια κάνει κλικ σε έναν κακόβουλο σύνδεσμο, ο οποίος μπορεί να οδηγήσει στην εγκατάσταση κακόβουλου λογισμικού, στο πάγωμα του συστήματος ή την αποκάλυψη ευαίσθητων πληροφοριών.

---

[1] Η εκμετάλλευση προγράμματος περιήγησης είναι μια μορφή κακόβουλου κώδικα που εκμεταλλεύεται ένα ελάττωμα ή μια ευπάθεια σε ένα λειτουργικό σύστημα ή ένα κομμάτι λογισμικού με σκοπό να παραβιάσει την ασφάλεια του προγράμματος περιήγησης για να αλλάξει τις ρυθμίσεις του προγράμματος περιήγησης ενός χρήστη χωρίς να το γνωρίζει. (wikipedia, 2021)

2 Όταν γίνονται λήψεις τις οποίες έχει εξουσιοδοτήσει ένα άτομο, αλλά χωρίς κατανόηση των συνεπειών ή γίνονται λήψης που συμβαίνει εν αγνοία του ατόμου, συχνά ιούς υπολογιστών , λογισμικό υποκλοπής spyware, malware , ή crimeware (wikipedia, 2021)

3 Μια στρατηγική επίθεση στον υπολογιστή όπου ένας εισβολέας μαντεύει ή παρατηρεί ποιες ιστοσελίδες χρησιμοποιεί ένας οργανισμός και μολύνει μία ή περισσότερες από αυτές με κακόβουλο λογισμικό ώσπου κάποιο μέλος της στοχευμένης ομάδας θα μολυνθεί. (wikipedia, 2021)

[4] Η εκμετάλλευση μηδενικής ημέρας είναι ένα ελάττωμα σε λογισμικό, υλικό ή υλικολογισμικό που είναι άγνωστο στο συμβαλλόμενο μέρος ή τα μέρη που είναι υπεύθυνα για την αποκατάσταση του. Ο εισβολέας εντοπίζει την ευπάθεια του λογισμικού και δημιουργεί γρήγορα ένα exploit και το χρησιμοποιεί για επίθεση. (Zero-day (0day) exploit, 2022)

Επίσης υπάρχει και το Spear phishing που είναι μια πιο εξελιγμένη και περίπλοκη έκδοση του ηλεκτρονικού ψαρέματος. Στοχεύει συγκεκριμένους οργανισμούς ή άτομα και επιδιώκει μη εξουσιοδοτημένη πρόσβαση σε εμπιστευτικά δεδομένα. Οι εισβολείς ενδέχεται να χρησιμοποιούν δημόσιες πληροφορίες που βρίσκονται σε ιστοτόπους κοινωνικών μέσων όπως το LinkedIn ή το Facebook. (Enisa, 2021). Αυτά χρησιμοποιούνται συχνά για να κερδίσουν θέση σε εταιρικά ή κυβερνητικά δίκτυα ως μέρος μιας μεγαλύτερης επίθεσης, όπως ένα συμβάν προχωρημένης επίμονης απειλής (APT- advanced persistent threat[5]), που συνήθως επιφέρει σοβαρές κυρώσεις τόσο οικονομικές όσο και στην φήμη, την εμπιστοσύνη και στο μερίδιο αγοράς (imperva, 2021) .

1.2.4 Επιθέσεις σε διαδικτυακές εφαρμογές (Web Application Attacks)

Πρόκειται για απειλές που στοχεύουν απευθείας στο χρήστη μέσω εκμετάλλευσης αδυναμιών στους διακομιστές (servers) ή στη βάση δεδομένων. Οι διαδικτυακές εφαρμογές είναι ιδιαίτερα ευαίσθητες σε hacking, επειδή είναι διαθέσιμες 24 ώρες την ημέρα, 365 ημέρες το χρόνο για παροχή συνεχών υπηρεσιών στο κοινό και ως εκ τούτου δεν μπορούν να προστατευτούν από τείχη προστασίας (firewalls). Πολλά από αυτά τα προγράμματα έχουν πρόσβαση, άμεσα ή έμμεσα, σε ιδιαίτερα επιθυμητά δεδομένα πελατών. Οι χάκερ καθιστούν δική τους δουλειά να αναζητούν τρωτά σημεία, ώστε αυτές οι πληροφορίες να μπορούν να κλαπούν ή να ανακατευθυνθούν. Κυριότερα είδη επιθέσεων αυτής της κατηγορίας αποτελούν τα SQL Injection (SQLI), Path traversal, Cross-site scripting (XSS), Local File Inclusion κλπ. (TrustNet, 2021)

Μια επίθεση στην εφαρμογή (application level attack) προκύπτει όταν οι επιτιθέμενοι αποκτούν πρόσβαση σε μη εξουσιοδοτημένες περιοχές, αναζητώντας τρωτά σημεία εφαρμογών γραμμένα στον κώδικα (contrast security, 2021). Περιλαμβάνει χαμηλές και αργές επιθέσεις, GET / POST πλημμύρες, επιθέσεις που στοχεύουν ευπάθειες Apache, Windows ή OpenBSD και άλλα. Αποτελούμενη από φαινομενικά νόμιμα και αθώα αιτήματα, ο στόχος αυτών των επιθέσεων είναι να καταρρεύσει ο διακομιστής ιστού και το μέγεθος μετράται σε αιτήσεις ανά δευτερόλεπτο (Rps). (imperva, 2021)

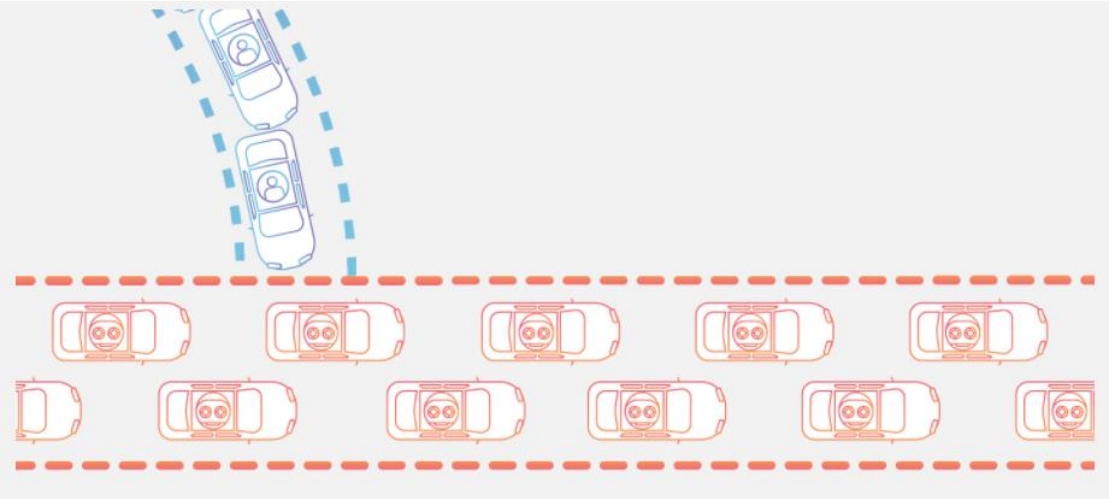
1.2.5 Ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου (Spam)

Spam (ή αλλιώς Sending and Posting Advertisement in Mass) είναι τα ανεπιθύμητα μηνύματα που αποστέλλονται μαζικά για την προώθηση ενός προϊόντος ή μιας ιδέας. Η αποστολή γίνεται σε μεγάλο αριθμό παραληπτών λόγω χαμηλού κόστους αποστολής. Τα περισσότερα είναι εμπορικής φύσης, αλλά πολλά είναι επικίνδυνα επειδή μπορεί να περιέχουν συνδέσμους που οδηγούν σε απειλές phishing ή σε ιστοτόπους ή συνημμένα με κακόβουλο λογισμικό. (wikipedia, 2021)

5Προχωρημένες επίμονες απειλές: Μια προηγμένη επίμονη απειλή είναι όταν ένας μη εξουσιοδοτημένος χρήστης αποκτά πρόσβαση σε ένα σύστημα ή δίκτυο και παραμένει εκεί χωρίς να εντοπιστεί για μεγάλο χρονικό διάστημα. (upguard, 2021)

1.2.6 Επιθέσεις κατανεμημένης άρνησης υπηρεσίας (Distributed Denial of Service)

Οι κατανεμημένες επιθέσεις άρνησης υπηρεσίας αποσκοπούν στη διακοπή ενός δικτύου υπολογιστών πλημμυρίζοντας το δίκτυο με περιττές αιτήσεις για υπερφόρτωση του συστήματος και αποτρέποντας την εκπλήρωση νόμιμων αιτημάτων (upguard, 2021). Ουσιαστικά, εκμεταλλεύονται την πεπερασμένη χωρητικότητα συστημάτων και δικτύων, ώστε να καταστήσουν αδύνατη την παροχή υπηρεσιών (απώλεια διαθεσιμότητας) (Chroni, 2021). Οι επιθέσεις DDoS επιτυγχάνονται αποτελεσματικά χρησιμοποιώντας πολλαπλά παραβιασμένα συστήματα υπολογιστών ή άλλους δικτυακούς πόρους ως μέσα επιθέσεων για αύξηση της επισκεψιμότητας (CloudFlare, 2021). Ένας τύπος DDoS είναι και το Protocol Attack που καταναλώνει πραγματικούς πόρους διακομιστή ή αυτούς του ενδιάμεσου εξοπλισμού επικοινωνίας, όπως τείχη προστασίας και εξισορρόπησης φορτίου, και μετράται σε πακέτα ανά δευτερόλεπτο (Pps). (imperva, 2021)



Εικόνα 3 - Παράδειγμα συμφόρησης από μη νόμιμα αιτήματα. (CloudFlare, 2021)

1.2.7 Κλοπή ταυτότητας χρήστη (Identity Theft)

Η κλοπή ταυτότητας είναι το έγκλημα της απόκτησης των προσωπικών ή οικονομικών πληροφοριών άλλου ατόμου για χρήση της ταυτότητάς του για διάπραξη απάτης, όπως η πραγματοποίηση μη εξουσιοδοτημένων συναλλαγών ή αγορών. Υπάρχουν πολλών ειδών ταυτότητες άρα και κλοπές αντίστοιχα. Πιο συγκεκριμένα:

a) Οικονομική: κάποιος χρησιμοποιεί την ταυτότητα ή τις πληροφορίες άλλου ατόμου για να λάβει πίστωση, αγαθά, υπηρεσίες ή οφέλη.
b) Κοινωνική Ασφάλιση: μπορούν να την χρησιμοποιήσουν για να υποβάλουν αίτηση για πιστωτικές κάρτες, δάνεια, φάρμακα, αναπηρία κα.
c) Ιατρική: για να λάβει δωρεάν ιατρική περίθαλψη
d) Συνθετική κλοπή ταυτότητας: συνδυασμός πληροφοριών για δημιουργία μιας νέας ταυτότητας, η οποία χρησιμοποιείται για το άνοιγμα δόλιων λογαριασμών και την πραγματοποίηση δόλιων αγορών.
e) Κλοπή ταυτότητας παιδιών: χρησιμοποιεί την ταυτότητα ενός παιδιού για να αποκτήσει προνόμια, όπως κατοικία, να βρει εργασία, να πάρει δάνεια ή να αποφύγει τη σύλληψη.
f) Φορολογική: για να υποβάλει μία ψευδή φορολογική δήλωση και να εισπράξει επιστροφή χρημάτων.
g) Ποινική ταυτότητα: για να αποφύγει μια κλήση, να αποτρέψει την έκδοση εντάλματος ή να αποφύγει ένα αρχείο καταδίκης. (Investopedia, 2021)

Το παραπάνω μπορεί να επιτευχθεί με την κλοπή διαπιστευτηρίων (theft of credentials) που είναι ένα έγκλημα στον κυβερνοχώρο που περιλαμβάνει την παράνομη επίτευξη του κωδικού πρόσβασης ενός οργανισμού ή ενός ατόμου με σκοπό την πρόσβαση και την κατάχρηση / την αποβολή κρίσιμων δεδομένων και πληροφοριών. Η κλοπή διαπιστευτηρίων επιτρέπει στους εισβολείς να λειτουργούν χωρίς ανίχνευση σε ένα δίκτυο, να επαναφέρουν τους κωδικούς πρόσβασης και να καταστρέφουν τον οργανισμό (awake , 2021).

1.2.8 Παραβίαση Δεδομένων (Data Breach)

Μια παραβίαση δεδομένων εκθέτει εμπιστευτικές, ευαίσθητες ή προστατευμένες πληροφορίες σε μη εξουσιοδοτημένο άτομο. Τα αρχεία σε μια παραβίαση δεδομένων προβάλλονται ή / και κοινοποιούνται χωρίς άδεια. Επίσης, εκτός από την διαρροή των προσωπικών δεδομένων μπορεί να γίνει και καταστροφή ή αλλοίωση τους με αποτέλεσμα να μην είναι διαθέσιμα προς χρήση. Η παραβίαση δεδομένων μπορεί να γίνει είτε με μορφή ηλεκτρονικής απειλής όπως είναι το phishing και το brute force[6] ή τυχαία. Δηλαδή όταν ένα υπάλληλος έχει στα χέρια του μια ηλεκτρονική συσκευή (φορητός υπολογιστής, εξωτερικός σκληρός δίσκος) ενός συναδέλφου του, και με αυτόν τον τρόπο αποκτά πρόσβαση σε αρχεία στα οποία δεν έχει την εξουσιοδότηση. (kaspersky, 2021).

Με αυτήν την πρόσβαση μπορεί να επιτευχθεί η χειραγώγηση των δεδομένων (data manipulation). Αυτές οι επιθέσεις αποσκοπούν στην κλοπή προσωπικών αρχείων, υγείας, εκπαίδευσης και οικονομικών αρχείων. Επιπλέον, στοχεύουν να σαρώσουν τις πολύτιμες μετοχές μεγάλων εταιρειών άμυνας, τεχνολογίας και παραγωγής. Για παράδειγμα, φανταστείτε ότι ένας εισβολέας καταφέρνει να παραβιάσει το σύστημα πληροφορικής και να εκτελεί μια επίθεση χειραγώγησης δεδομένων οποιασδήποτε εταιρείας, όπως η Amazon ή η Uber. Αυτό θα προκαλούσε άμεσο πανικό στο χρηματιστήριο, με ζημίες στις ίδιες και στους μετόχους τους. (Brooke, 2022)

1.2.9 Εσωτερικές απειλές (Insider Threats)

Οι απειλές μπορεί να προέρχονται από στελέχη που εργάζονται ή έχουν εργαστεί για τον οργανισμό, καθώς και εξωτερικούς υπαλλήλους που έχουν εσωτερικές πληροφορίες σχετικά με τις πρακτικές ασφαλείας, τα συστήματα υπολογιστών και τα δεδομένα του οργανισμού. Αυτές οι απειλές μπορούν να οδηγήσουν σε πολλές από τις επιθέσεις που περιγράφονται σε αυτήν την ενότητα. Συχνά, έχουν πολύ μεγάλο αντίκτυπο στον φορέα και είναι εξαιρετικά δύσκολο να διαγνωστούν και να αντιμετωπιστούν (Chroni, 2021).

1.2.10 Botnets

Το botnet είναι ένα σύνολο υπολογιστών που έχει μολυνθεί από bots. Το bot είναι ένα κακόβουλο λογισμικό το όποιο δέχεται εντολές από μία κύρια μηχανή του επιτιθέμενου. Ένας υπολογιστής μολύνεται είτε όταν ένα worm ή ένας ιός εγκαθιστά το bot ή όταν ο χρήστης επισκέπτεται έναν κακόβουλο ιστότοπο που εκμεταλλεύεται μια ευπάθεια στο πρόγραμμα περιήγησης. Όταν το κακόβουλο λογισμικό bot εκτελείται σε έναν υπολογιστή, έχει μεγάλη πρόσβαση στους πόρους του υπολογιστή όπως και ο κάτοχός του. Στη συνέχεια, τα bots μπορούν να διαβάζουν και να γράφουν αρχεία, να εκτελούν προγράμματα, να παρακολουθούν πλήκτρα, να έχουν πρόσβαση στην κάμερα, να στέλνουν email, να πλημμυρίζουν δίκτυα (DDoS) κ.λπ. (βλέπε Zeus Botnet). (enisa, 2021)

---

[6] **Brute Force (password guessing):** είναι πολύ συχνή μορφή επίθεσης σε ιστοτόπους και διακομιστές ιστού για να τους θέσουν σε κίνδυνο. Η διαδικασία είναι πολύ απλή και οι εισβολείς δοκιμάζουν βασικά πολλαπλούς συνδυασμούς ονομάτων χρήστη και κωδικών πρόσβασης μέχρι να βρουν έναν που λειτουργεί. Μόλις έχουν την πρόσβαση οι κίνδυνοι είναι μεγάλοι όπως κακόβουλο λογισμικό, ανεπιθύμητο περιεχόμενο, ηλεκτρονικό ψάρεμα (phishing) ή οτιδήποτε άλλο θέλουν. (sucuri, 2021)

1.2.11 Φυσικές απειλές

Μια φυσική απειλή είναι μια πιθανή αιτία ενός συμβάντος που μπορεί να οδηγήσει σε απώλεια ή φυσική βλάβη στο σύστημα με σοβαρές επιπτώσεις όπως η καταστροφή δεδομένων ή η άρνηση της υπηρεσίας. Τέτοιου είδους απειλές προκαλούνται είτε από το εσωτερικό περιβάλλον όπως είναι η πυρκαγιά, η ασταθής τροφοδοσία, ή από το εξωτερικό δηλαδή κεραυνούς, πλημμύρες και σεισμούς. Επίσης, σε αυτήν την απειλή υπολογίζεται και η κλοπή καθώς και τυχαίοι ή εκ προθέσεως βανδαλισμοί της υποδομής. (guru99, 2021)

1.2.12 Διαρροή Δεδομένων

Η διαρροή πληροφοριών επιτρέπει σε μια εφαρμογή να αποκαλύπτει ευαίσθητα δεδομένα, όπως τεχνικές λεπτομέρειες της εφαρμογής, σχόλια προγραμματιστή, περιβάλλον ή δεδομένα ειδικά για το χρήστη. Ένας εισβολέας μπορεί να χρησιμοποιήσει αυτά τα ευαίσθητα δεδομένα για να εκμεταλλευτεί την εφαρμογή στόχου, το δίκτυο φιλοξενίας ή τους χρήστες του. Στην πιο συνηθισμένη μορφή του, η διαρροή πληροφοριών είναι το αποτέλεσμα μίας ή περισσοτέρων από τις ακόλουθες συνθήκες: a) αποτυχία εξαγωγής σχολίων HTML/script που περιέχουν ευαίσθητες πληροφορίες b) ακατάλληλες ρυθμίσεις εφαρμογής ή διακομιστή c) ή διαφορές στις απαντήσεις σελίδας για έγκυρα έναντι μη έγκυρων δεδομένων. Το Information Leakage δεν αντιπροσωπεύει απαραίτητα παραβίαση ασφαλείας, παρέχει στον εισβολέα χρήσιμη καθοδήγηση για μελλοντική εκμετάλλευση. (White Hat Security, 2021)

1.2.13 Λογισμικό Λύτρων (ransomware)

Αυτός ο τύπος κακόβουλου λογισμικού χρησιμοποιείται για εκβιασμό και μπορεί να κλειδώσει συσκευές ή να κρυπτογραφήσει δεδομένα που είναι αποθηκευμένα σε δίσκους. Στη συνέχεια, εμφανίζει την αξίωση λύτρων με λεπτομέρειες για την πληρωμή. Οι δημιουργοί Ransomware χρησιμοποιούν διάφορες τεχνικές:

- Το **ransomware Diskcoder** κρυπτογραφεί όλο το δίσκο και εμποδίζει την πρόσβαση στο λειτουργικό σύστημα.
- Το **Screen locker** αποκλείει την πρόσβαση στην οθόνη της συσκευής.
- Το **Crypto-ransomware** κρυπτογραφεί τα δεδομένα που είναι αποθηκευμένα στο δίσκο του θύματος.
- Το **PIN locker** επιτίθεται σε συσκευές Android αλλάζοντας τους κωδικούς πρόσβασης κλειδώνοντας το χρήστη απ' έξω.

Όλα τα παραπάνω ransomware απαιτούν λύτρα, συνήθως σε **Bitcoin ή άλλα ψηφιακά νομίσματα**, καθιστώντας αδύνατο τον εντοπισμό τους συναλλαγής. Σε αντάλλαγμα, ο εισβολέας υπόσχεται να αποκρυπτογραφήσει τα δεδομένα ή να επαναφέρει την πρόσβαση στη μολυσμένη συσκευή – χωρίς καμία εγγύηση (eset, 2021).

1.2.14 Ηλεκτρονική κατασκοπία (Cyber Espionage)

Η κατασκοπεία είναι μια μορφή επίθεσης στον κυβερνοχώρο που κλέβει ευαίσθητα δεδομένα ή πνευματική ιδιοκτησία για να αποκτήσει πλεονέκτημα έναντι μιας ανταγωνιστικής εταιρείας ή κυβερνητικής οντότητας. Στον κυβερνοχώρο οι κατάσκοποι είναι στρατοί από κακόβουλους χάκερ από όλο τον κόσμο που έχουν την τεχνογνωσία για να κλείσουν οτιδήποτε, από κυβερνητικές υποδομές μέχρι χρηματοοικονομικά συστήματα. Χρησιμοποιούν τον κυβερνοπόλεμο (cyber warfare) για οικονομικό, πολιτικό ή στρατιωτικό όφελος. Έχουν επηρεάσει το αποτέλεσμα των πολιτικών εκλογών, έχουν δημιουργήσει χάος σε διεθνή γεγονότα και έχουν βοηθήσει εταιρείες να πετύχουν ή να αποτύχουν. (vmware, 2021)

1.2.15 Cryptojacking

Το Cryptojacking είναι τους τύπος επίθεσης στον κυβερνοχώρο στον οποίο τους χάκερ επιλέγει την υπολογιστική δύναμη τους στόχου για να εξαγάγει παράνομα χρήματα από τους στόχους του με την μορφή κρυπτονομισμάτων για λογαριασμό του χάκερ. Οι παραλλαγές κακόβουλου λογισμικού που εμπλέκονται στο cryptojacking επιβραδύνουν τους μολυσμένους υπολογιστές, καθώς η διαδικασία εξόρυξης έχει προτεραιότητα έναντι άλλων νόμιμων δραστηριοτήτων. (investopedia, 2021)

1.2.16 Man-in-the-middle

Μια επίθεση **man-in-the-middle (MitM)** είναι μια μορφή επίθεσης στον κυβερνοχώρο όπου σημαντικά δεδομένα παρεμποδίζονται από έναν εισβολέα χρησιμοποιώντας μια τεχνική για να αναμιχθούν στη διαδικασία επικοινωνίας. Ο εισβολέας μπορεί να είναι ένας παθητικός ακροατής στη συνομιλία ή ένας ενεργός συμμετέχων που αλλάζει το περιεχόμενο των μηνυμάτων ή πλαστοπροσωπεί το άτομο / σύστημα. Ορισμένες τεχνικές που χρησιμοποιούνται είναι:

Εικόνα 4 - Τεχνικές και τύποι επίθεσης MitM (Buckbee, 2021)

a) ARP[7] Cache Poisoning: Οι εισβολείς εισάγουν ψευδείς πληροφορίες στο σύστημα, λαμβάνοντας όλη την κυκλοφορία του δικτύου, για να εξαπατήσουν τον υπολογιστή, ώστε να πιστεύει ότι ο υπολογιστής του εισβολέα είναι η πύλη δικτύου (αντί για την πραγματική) και μεταφέρει την κυκλοφορία στον πραγματικό του προορισμό.
b) Δηλητηρίαση προσωρινής μνήμης DNS[8]: είναι όταν ο εισβολέας δίνει μια ψεύτικη καταχώρηση DNS που οδηγεί σε διαφορετικό ιστότοπο. Μπορεί να μοιάζει με Google, αλλά δεν είναι και ο εισβολέας καταγράφει ό,τι δεδομένα εισαχθούν στον πλαστό ιστότοπο, όπως όνομα χρήστη και κωδικός πρόσβασης.
c) Πλαστογράφηση (spoofing) HTTPS[9]: Οι εισβολείς δημιουργούν ιστοτόπους HTTPS που μοιάζουν με νόμιμους με έγκυρα πιστοποιητικά ελέγχου ταυτότητας, αλλά η διεύθυνση URL είναι διαφορετική. Για παράδειγμα, θα καταχωρήσουν έναν ιστότοπο με χαρακτήρα unicode[10] που μοιάζει με "a" αλλά να είναι ένα κυριλλικό "a", που είναι έγκυρος

7 Το Address Resolution Protocol (ARP) είναι μια διαδικασία χαμηλού επιπέδου που μεταφράζει τη διεύθυνση του μηχανήματος (MAC) στη διεύθυνση IP του τοπικού δικτύου.

8 Το Domain Name System (DNS) είναι ένα ιεραρχικό και αποκεντρωμένο σύστημα ονομάτων για υπολογιστές, υπηρεσίες ή άλλους πόρους που είναι συνδεδεμένοι στο Διαδίκτυο ή σε ιδιωτικό δίκτυο. Παρέχοντας μια παγκόσμια, κατανεμημένη υπηρεσία καταλόγου, αποτελεί ουσιαστικό στοιχείο της λειτουργικότητας του Διαδικτύου από το 1985. (wikipedia, 2021)

9 Το HyperText Transfer Protocol Secure (HTTPS) χρησιμοποιείται για ασφαλή επικοινωνία μέσω δικτύου υπολογιστών και χρησιμοποιείται ευρέως στο Διαδίκτυο. (wikipedia, 2021)

10 Το Unicode είναι ένα πρότυπο τεχνολογίας πληροφοριών για τη συνεπή κωδικοποίηση , αναπαράσταση και χειρισμό κειμένου που εκφράζεται στα περισσότερα συστήματα γραφής του κόσμου. (wikipedia, 2021)

χαρακτήρας. Ο επιτιθέμενος δρομολογεί τον χρήστη στην πλαστή ιστοσελίδα με αποτέλεσμα να κάνει λήψη και αποθήκευση του πιστοποιητικού με το ιδιωτικό κλειδί[11] CA[12] για τον ψεύτικο ιστότοπο.

d) Παρακολούθηση (Eavesdropping) Wi-Fi: Οι εισβολείς ακούνε την κυκλοφορία σε δημόσια ή μη ασφαλή δίκτυα Wi-Fi ή δημιουργούν δίκτυα Wi-Fi με κοινά ονόματα για να εξαπατήσουν τους ανθρώπους να συνδεθούν, ώστε να μπορούν να κλέψουν διαπιστευτήρια ή αριθμούς πιστωτικών καρτών ή οποιεσδήποτε άλλες πληροφορίες στέλνουν οι χρήστες σε αυτό το δίκτυο.
e) Παραβίαση συνεδρίας (Session Hijacking): είναι μια επίθεση MitM όπου ο εισβολέας κλέβει το cookie περιόδου σύνδεσης ενός χρήστη για να συνδεθεί στον ίδιο λογαριασμό από το πρόγραμμα περιήγησής του. Αυτό μπορεί να του επιτρέψει να κάνει ό,τι και ο χρήστης σε αυτόν τον ιστότοπο. (Buckbee, 2021)

1.2.17 HoneyPot

Ένα cyber honeypot είναι ένα θυσιαστικό σύστημα υπολογιστών που προορίζεται να προσελκύσει επιθέσεις στον κυβερνοχώρο, όπως ένα δόλωμα. Μιμείται έναν στόχο για χάκερ και χρησιμοποιεί τις προσπάθειές τους για εισβολή για να αποκτήσουν πληροφορίες σχετικά με εγκληματίες στον κυβερνοχώρο και τον τρόπο λειτουργίας τους ή για να τους αποσπάσουν από άλλους στόχους. Μπορούν όμως να αποτελέσουν κίνδυνο αν δεν είναι εξοπλισμένα με ένα «τείχος» προστασίας. Ένας έμπειρος χάκερ θα μπορούσε να χρησιμοποιήσει ένα honeypot υψηλής αλληλεπίδρασης για να επιτεθεί σε άλλους οικοδεσπότες του διαδικτύου ή να στείλει ανεπιθύμητο περιεχόμενο από έναν παραβιασμένο υπολογιστή. Επιπλέον, μόλις ένα honeypot έχει «δακτυλικό αποτύπωμα», ένας εισβολέας μπορεί να δημιουργήσει πλαστογραφημένες επιθέσεις για να αποσπάσει την προσοχή από μια πραγματική εκμετάλλευση που στοχεύει στα συστήματα παραγωγής. (kaspersky, 2021)

1.3 Μέτρα πρόληψης

Παραπάνω είδαμε τους δημοφιλέστερες απειλές που μπορεί να κρύβονται στον κυβερνοχώρο. Οι περισσότερες από αυτές έχουν λάβει χώρα κιόλας και για αυτόν τον λόγο έχουν ληφθεί ποικίλα μέτρα πρόληψης. Ένα από τα κύρια μέτρα που λαμβάνουν ορισμένες επιχειρήσεις είναι η **πρόσληψη έμπειρων ανθρώπων ή εταιριών** για να ελέγξουν τα συστήματα και να προτείνουν βελτιώσεις στην ασφάλεια τους. Άλλα μέτρα πρόληψης που συμβάλλουν στην άμβλυνση του κινδύνου των κυβερνοεπιθέσεων είναι τα παρακάτω: (the capacity group, 2021)

1. **Εκπαίδευση προσωπικού:** Τους από τους πιο αποτελεσματικούς τρόπους προστασίας από κυβερνοεπιθέσεις και όλων των τύπων παραβιάσεων δεδομένων είναι η εκπαίδευση των υπαλλήλων σχετικά με την πρόληψη τους επίθεσης στον κυβερνοχώρο και η ενημέρωσή τους για τους τρέχουσες επιθέσεις στον κυβερνοχώρο. Τους, ωφέλιμο θα ήταν να μάθει το προσωπικό να ελέγχει τους συνδέσμους, τους διευθύνσεις των ληφθέντων email και να μην στέλνει αφιλτράριστά ευαίσθητες πληροφορίες κα.
2. **Ενημερωμένο λογισμικό:** Η εγκατάσταση τους κώδικα (patch management system) που θα διαχειρίζεται τους τους ενημερώσεις του λογισμικού διατηρεί το σύστημά

11 Το δημόσιο και το ιδιωτικό κλειδί δεν είναι πραγματικά κλειδιά αλλά μάλλον είναι πολύ μεγάλοι πρωταρχικοί αριθμοί που σχετίζονται μαθηματικά μεταξύ τους. Η σχέση σε αυτήν την περίπτωση σημαίνει ότι ό, τι κρυπτογραφείται από το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο από το σχετικό ιδιωτικό κλειδί. Ένα άτομο δεν μπορεί να μαντέψει το ιδιωτικό κλειδί με βάση το να γνωρίζει το δημόσιο κλειδί. Εξαιτίας αυτού, ένα δημόσιο κλειδί μπορεί να κοινοποιηθεί ελεύθερα. Το ιδιωτικό κλειδί ωστόσο ανήκει μόνο σε ένα άτομο. (preveil, 2021)

12 Στην κρυπτογραφία, μια αρχή έκδοσης πιστοποιητικών ή μια αρχή πιστοποίησης (CA) είναι μια οντότητα που εκδίδει ψηφιακά πιστοποιητικά . Ένα ψηφιακό πιστοποιητικό πιστοποιεί την κυριότητα ενός δημόσιου κλειδιού από το όνομα του πιστοποιητικού. Αυτό επιτρέπει σε άλλους (εξαρτώμενα μέρη) να βασίζονται σε υπογραφές ή σε ισχυρισμούς που έγιναν για το ιδιωτικό κλειδί που αντιστοιχεί στο πιστοποιημένο δημόσιο κλειδί. Η CA ενεργεί ως αξιόπιστο τρίτο μέρος - εμπιστεύεται τόσο το αντικείμενο (κάτοχος) του πιστοποιητικού όσο και το μέρος που βασίζεται στο πιστοποιητικό. (wikipedia, 2021)

ανθεκτικό και ενημερωμένο. Αυτό θα αποτρέψει τους κακόβουλους χρήστες από το να εκμεταλλευτούν αδυναμίες του συστήματος για να αποκτήσουν πρόσβαση.

3. **Τείχος προστασίας (firewall):** Η τοποθέτηση του δικτύου πίσω από ένα τείχος προστασίας είναι τους από τους πιο αποτελεσματικούς τρόπους για την προστασία από οποιαδήποτε επίθεση στον κυβερνοχώρο, καθώς αποκλείει τυχόν βίαιες επιθέσεις προτού να προκαλέσει ζημιά.
4. **Τελικό σημείο (endpoint):** Η προστασία Endpoint προστατεύει δίκτυα που συνδέονται από απόσταση. Οι φορητές συσκευές, τα tablet και οι φορητοί υπολογιστές που συνδέονται με εταιρικά δίκτυα παρέχουν διαδρομές πρόσβασης οι οποίες πρέπει να προστατεύονται με συγκεκριμένο λογισμικό προστασίας τελικού σημείου για να μην τεθεί κάποιο ζήτημα ασφάλειας.
5. **Αντίγραφα ασφαλείας (Back ups):** Σε περίπτωση καταστροφής πρέπει να υπάρχουν αντίγραφα ασφαλείας για τα δεδομένα, ώστε να αποφευχθούν σοβαρές διακοπές λειτουργίας, απώλεια δεδομένων και σοβαρή οικονομική ζημία.
6. **Φυσική πρόσβαση τους υπολογιστές:** Είναι σημαντικό να ελέγχεται ποιος έχει πρόσβαση τους υπολογιστές. Η εγκατάσταση τους περιμετρικού συστήματος ασφαλείας είναι τους πολύ καλός τρόπος για να σταματήσει το έγκλημα στον κυβερνοχώρο καθώς κάποιος μπορεί απλώς να εισέλθει στο γραφείο ή την επιχείρησή και να συνδέσει ένα USB που περιέχει μολυσμένα αρχεία σε έναν από τους υπολογιστές επιτρέποντάς τους να έχουν πρόσβαση σε ολόκληρο το δίκτυό ή να το μολύνουν.
7. **Δίκτυα Wi-Fi:** Η ασφάλεια των δικτύων Wi-Fi και η απόκρυψή τους είναι ένα από τα ασφαλέστερα πράγματα που μπορούν να εφαρμοστούν για τα συστήματά των επιχειρήσεων αφού ολόκληρο το σύστημά διατρέχει σοβαρό κίνδυνο αν μια μολυσμένη συσκευή συνδεθεί με το επιχειρηματικό δίκτυο.
8. **Προσωπικοί λογαριασμοί εργαζομένων:** Έχοντας ξεχωριστές συνδέσεις για κάθε μέλος του προσωπικού επιτυγχάνεται η μείωση του αριθμού των επιθετικών μετώπων. Εκτός από την ασφάλεια που παρέχει αυτό το μέτρο, έχει τους και βελτιωμένη χρηστικότητα.
9. **Διαχείριση πρόσβασης:** Ενδείκνυται ο περιορισμός τους πρόσβασης των εργαζομένων σε δεδομένα και πληροφορίες καθώς και τους δυνατότητας εγκατάστασης λογισμικού σε συσκευές που ανήκουν στην επιχείρηση και θα μπορούσαν να θέσουν σε κίνδυνο τα συστήματά.
10. **Κωδικοί πρόσβασης:** Η ρύθμιση διαφορετικών κωδικών πρόσβασης για κάθε εφαρμογή αποτελεί πραγματικό όφελος για την ασφάλειά των συστημάτων τους και η συχνή αλλαγή τους θα διατηρήσει υψηλό επίπεδο προστασίας από εξωτερικές και εσωτερικές απειλές. (leaf, 2021)

Όπως αναφέρθηκε και στην αρχή, τα παραπάνω μέτρα καθώς και η εγκατάσταση λογισμικού προστασίας από κακόβουλο λογισμικό ή φίλτρα για spam αλληλογραφία αποτελούν τα ελάχιστα που μπορεί να λάβει μια επιχείρηση για να αποτρέψει τις πιο συχνές επιθέσεις. Για πιο προχωρημένες κυβερνοεπιθέσεις καλό θα ήταν να υπάρχει μια ομάδα εξειδικευμένων ατόμων που θα δοκιμάζουν και θα ελέγχουν τα λογισμικά περιβάλλοντα μέσω α) αξιολογήσεων ευπαθειών, β) διεξαγωγής δοκιμών διείσδυσης ρουτίνας, γ) εφαρμογής πληροφοριών ασφαλείας και διαχείρισης συμβάντων (SIEM), δ) ανάπτυξης λογισμικού εντοπισμού και πρόληψης εισβολής (IDS και IPS) και ε) δημιουργίας προγράμματος πρόληψης απώλειας δεδομένων (DLP)[13] (PURPLESEC, 2021)

13 Για περισσότερες πληροφορίες μπορείτε να ανατρέξετε στην ιστοσελίδα https://purplesec.us/prevent-cyber-attacks/ όπου αναφέρονται διάφορες κυβερνοεπιθέσεις καθώς και τα μέτρα πρόληψης κάθε μιας ξεχωριστά.

1.4 Κανονισμοί και νομοθεσία

Οι κυβερνοεπιθέσεις αφορούν όχι μόνο την χώρα μας αλλά είναι ένα παγκόσμιο πλέον φαινόμενο, και για αυτό τον λόγο έχουν δημιουργηθεί ανάλογοι φορείς όπως και κανονισμοί που συνδράμουν στον περιορισμό τέτοιων επιθέσεων. Τέτοιοι φορείς στον ελλαδικό χώρο είναι οι Γενική Διεύθυνση Κυβερνοασφάλειας (National Cybersecurity Authority), Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων, Διεύθυνση Κυβερνοάμυνας (Υπουργείο Εθνικής Άμυνας) (ΓΕΕΘΑ/ΔΙΚΥΒ), Δίωξη Ηλεκτρονικού Εγκλήματος, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.), Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.), Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (Α.Δ.Α.Ε), Κέντρο Μελετών Ασφαλείας (ΚεΜεΑ) και λοιποί εμπλεκόμενοι φορείς. Πιο συγκεκριμένα:

Η **Γενική Διεύθυνση Κυβερνοασφάλειας**, τμήμα ας Γενικής Γραμματείας Τηλεπικοινωνιών & Ταχυδρομείων του υπουργείου Ψηφιακής Διακυβέρνησης, καταρτίζει την Εθνική Στρατηγική Κυβερνοασφάλειας, στην οποία προσδιορίζονται οι στρατηγικοί στόχοι, οι προτεραιότητες και τα ρυθμιστικό πολιτικό πλαίσιο με στόχο τη διασφάλιση υψηλού επιπέδου ασφάλειας στα συστήματα τηλεπικοινωνιών και πληροφορικής διεθνώς. Η Γενική Διεύθυνση Κυβερνοασφάλειας διατυπώνει την πολιτική ασφάλειας συστημάτων, ορίζει απαιτήσεις και κανόνες ασφάλειας, συνεργάζεται με αρμόδιες αρχές και ακαδημαϊκούς φορείς για την υιοθέτηση ενιαίων πολιτικών ασφαλείας και προωθεί εκπαιδευτικές ενέργειες του προσωπικού που διαχειρίζεται και υποστηρίζει κρίσιμα συστήματα και υποδομές του δημοσίου. (Ελληνική Δημοκρατία, 2022)

Η **Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων** (Εθνικό CERT) είναι μια υπηρεσία ασφαλείας που συνιστά μέρος της Εθνικής Υπηρεσίας Πληροφοριών της Ελλάδας (National Intelligence Service). Καθήκον της είναι η μέριμνα για την πρόληψη και τη στατική καθώς και για τη δραστική αντιμετώπιση ηλεκτρονικών επιθέσεων κατά δικτύων επικοινωνιών, εγκαταστάσεων αποθήκευσης πληροφοριών και συστημάτων πληροφορικής. Επιπλέον, είναι αρμόδια για τη συγκέντρωση, την επεξεργασία δεδομένων και την ενημέρωση των αρμόδιων φορέων (IGuru, 2022).

Η **Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ** αποτελεί την Ελληνική Αρμόδια Ομάδα Απόκρισης Κυβερνοπεριστατικών (Computer Security Incident Response Team – CSIRT) σχετικά με την ανταπόκριση σε περιστατικά που εμπίπτουν στον στρατιωτικό τομέα – κυβερνοάμυνα (military CSIRT), στο πεδίο εφαρμογής του ν. 4577/2018 (Φ.Ε.Β.Υ., Π.Ψ.Υ.) και την επιχειρησιακή ολοκλήρωση. Ο ρόλος της ανωτέρω Υπηρεσίας είναι η σμίκρυνση του κινδύνου εθνικών προκλήσεων στον τομέα της ασφάλειας του κυβερνοχώρου και των επικοινωνιών. (Ελληνική Δημοκρατία - Υπουργείο Ψηφιακής Διακυβέρνησης, 2022)

Στις αρμοδιότητες της **Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος** συμπεριλαμβάνονται η πρόληψη, η έρευνα και η καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που πραγματοποιούνται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος υπάγεται απευθείας στον Αρχηγό της Ελληνικής Αστυνομίας. Αποτελείται από πέντε αναβαθμισμένα τμήματα που αφορούν όλο το φάσμα της προστασίας του χρήστη και της ασφάλειας του Κυβερνοχώρου, και είναι τα εξής: α) Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών, β) Τμήμα Καινοτόμων Δράσεων και Στρατηγικής, γ) Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων, δ) Τμήμα Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης και ε) Τμήμα Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων. (Ελληνική Αστυνομία, 2022)

Η **Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα** έχει κατοχυρωθεί συνταγματικά ως ανεξάρτητη δημόσια Αρχή, η οποία έχει ως αρμοδιότητά της την έλεγχο της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων, του ν. 4624/2019, του ν. 3471/2006 και άλλων διατάξεων που σχετίζονται με την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και την εκτέλεση των εκάστοτε καθηκόντων της (Αρχή Προστατίας Δεδομένων, 2022)

Η **Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)** είναι ανεξάρτητος φορέας με διοικητική αρχή. Στην ουσία πρόκειται για τον Εθνικό Ρυθμιστή που εποπτεύει και ελέγχει: (α) το εμπόριο ηλεκτρονικών επικοινωνιών, που αφορά τις εταιρίες σταθερής και κινητής

τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου και (β) την ταχυδρομική αγορά, στην οποία δραστηριοποιούνται οι εταιρίες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφοράς. Η αποστολή της είναι η παρακολούθηση των εξελίξεων σε ευρωπαϊκό και παγκόσμιο επίπεδο, η συνεργασία με την Ελληνική Πολιτεία, η συμμετοχή στην χάραξη μακροχρόνιων πολιτικών και σχεδίων επενδύσεων ευρυζωνικότητας, η εποπτεία στις αγορές φάσματος, τηλεπικοινωνιών και ταχυδρομείων, ώστε να υπάρχει υγιής ανταγωνισμός και άλλα πολλά. (ΕΕΤΤ, 2022)

Η **Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών** στοχεύει στην προστασία του απορρήτου της αλληλογραφίας, της ελεύθερης επικοινωνία και της ασφάλειας των δικτύων και των πληροφοριών. Η έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνει τον έλεγχο της συμμόρφωσης με της όρους και της διαδικασίες που απαιτούνται από το νόμο για την απουσία εμπιστευτικότητας. Η ΑΔΑΕ είναι ανεξάρτητος φορέας με διοικητική αυτονομία. Οι κύριες αρμοδιότητες της είναι: 1) η διενέργεια ελέγχων σε εγκαταστάσεις που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή της υπηρεσίες, 2) ο έλεγχος από πλευράς νομιμότητας, 3) η διενέργεια ακροάσεων για πιθανές παραβάσεις της κείμενης νομοθεσίας για το απόρρητο των επικοινωνιών, 4) η επιβολή κυρώσεων, 5) η έκδοση κανονιστικών και άλλων αναγκαίων πράξεων αναφορικά με τα εφαρμοστέα μέτρα για την τήρηση του απορρήτου, 6) η έκδοση γνωματεύσεων, συστάσεων και υποδείξεων για θέματα που εντάσσονται στα καθήκοντά της και 7) η διερεύνηση καταγγελιών για τυχόν παραβίαση του απορρήτου τηλεφωνικών και διαδικτυακών επικοινωνιών. (ΑΔΑΕ, 2022)

Το **ΚΕ.ΜΕ.Α**. είναι ένα επιστημονικό, ερευνητικό και συμβουλευτικό όργανο που σκοπό έχει τη διεξαγωγή θεωρητικής και εφαρμοσμένης έρευνας και τη διεξαγωγή έρευνας σε θέματα που σχετίζονται με την πολιτική ασφάλειας, ιδίως σε στρατηγικό επίπεδο, και την παροχή υπηρεσιών, συμβουλών και συμβουλών σε θέματα ασφάλειας. γενικά. Είναι νομικό πρόσωπο ιδιωτικού δικαίου που εδρεύει στην Αθήνα, με διοικητική και οικονομική αυτοτέλεια, που λειτουργεί προς το δημόσιο συμφέρον και υπό την εποπτεία του Υπουργού Πολιτικής Άμυνας.. (ΚΕΜΕΑ, 2022)

Επειδή, οι κυβερνοεπιθέσεις και τα κυβερνοεγκλήματα πολλαπλασιάζονται σε ολόκληρη την Ευρώπη, ακόμα και μέθοδοι που χρησιμοποιούνται στις ενέργειες αυτές εξελίσσονται διαρκώς, και πρόκειται να ενισχυθούν περαιτέρω στο μέλλον, η ΕΕ αναπτύσσει δράση σε διάφορα μέτωπα, προκειμένου:

- να ενισχύσει την κυβερνοανθεκτικότητα
- να καταπολεμήσει το κυβερνοέγκλημα
- να ενισχύσει την κυβερνοδιπλωματία
- να ενδυναμώσει την κυβερνοάμυνα
- να τονώσει την έρευνα και την καινοτομία
- να προστατεύσει τις υποδομές ζωτικής σημασίας

Δύο σημαντικές ημερομηνίες για την Ευρωπαϊκή Επιτροπή είναι ο Μάιος και ο Ιούνιος του 2019. Τον Μάιο του 2019, το Συμβούλιο ενέκρινε ένα πλαίσιο που επιτρέπει στην ΕΕ να επιβάλλει κυρώσεις για την πρόληψη και την απάντηση σε κυβερνοεπιθέσεις που αποτελούν εξωτερική απειλή για την ίδια ή τα κράτη μέλη της. Ειδικότερα, για πρώτη φορά, το πλαίσιο επιτρέπει στην ΕΕ να επιβάλλει κυρώσεις σε άτομα ή οντότητες που είναι υπεύθυνες για επιθέσεις στον κυβερνοχώρο ή απόπειρες κυβερνοεπιθέσεων ή στην εμπλοκή τους μέσω παροχής οικονομικής, τεχνικής ή υλικής υποστήριξης. Τα περιοριστικά μέτρα περιλαμβάνουν απαγόρευση ταξιδιού προς την ΕΕ και δέσμευση περιουσιακών στοιχείων προσώπων και οντοτήτων.

Και στις 27 Ιούνιου του 2019 τέθηκε σε ισχύ ευρωπαϊκή πράξη για την κυβερνοασφάλεια (Cybersecurity Act) που θέσπιζε ένα κοινό σύστημα πιστοποίησης και μια νέα και ισχυρότερη εντολή για τον Οργανισμό της ΕΕ. Μέσω του νόμου αυτού, η ΕΕ δημιούργησε ένα ενιαίο πλαίσιο πιστοποίησης για την οικοδόμηση εμπιστοσύνης, τη διευκόλυνση της ανάπτυξης της αγοράς κυβερνοασφάλειας και του εμπορίου σε ολόκληρη την ΕΕ. Το πλαίσιο θα παρέχει ένα ολοκληρωμένο σύνολο κανόνων, τεχνικών απαιτήσεων, προτύπων και διαδικασιών (Ευρωπαϊκό Συμβούλιο, 2021).

Όσον αφορά την Ευρωπαϊκή Ένωση οι φορείς που απαρτίζουν την Cyber κοινότητα είναι οι European Union Agency for Network and Information Security (ENISA), Information Sharing and Analysis Centres (ISAC), Joint Research Center (JRC), Computer Security Incident Response Teams (CSIRTs), European Cybersecurity Organisation (ECSO) και Women4Cyber Registry.

Ο **ENISA** είναι ο οργανισμός της ΕΕ που ασχολείται με την ασφάλεια στον κυβερνοχώρο. Παρέχει υποστήριξη σε κράτη μέλη, σε θεσμικά όργανα και σε επιχειρήσεις της ΕΕ σε βασικούς τομείς, συμπεριλαμβανομένης της εφαρμογής της οδηγίας NIS. Το πρώτο κομμάτι νομοθεσίας είναι η οδηγία για την ασφάλεια των δικτύων και των συστημάτων πληροφοριών **(Network and Information Systems Directive)** που παρέχει νομικά μέτρα για την ενίσχυση του συνολικού επιπέδου ασφάλειας στον κυβερνοχώρο διασφαλίζοντας:

- Ετοιμότητα των κρατών μελών, απαιτώντας τους να είναι κατάλληλα εξοπλισμένοι.
- Συνεργασία μεταξύ όλων των κρατών μελών, με τη σύσταση ομάδας για τη στήριξη και τη διευκόλυνση της στρατηγικής συνεργασίας και της ανταλλαγής πληροφοριών μεταξύ των κρατών μελών.
- Μια κουλτούρα ασφάλειας μεταξύ τομέων που είναι ζωτικής σημασίας για την οικονομία και την κοινωνία και επιπλέον βασίζονται σε μεγάλο βαθμό στις τεχνολογίες πληροφοριών. (European Commission, 2021)

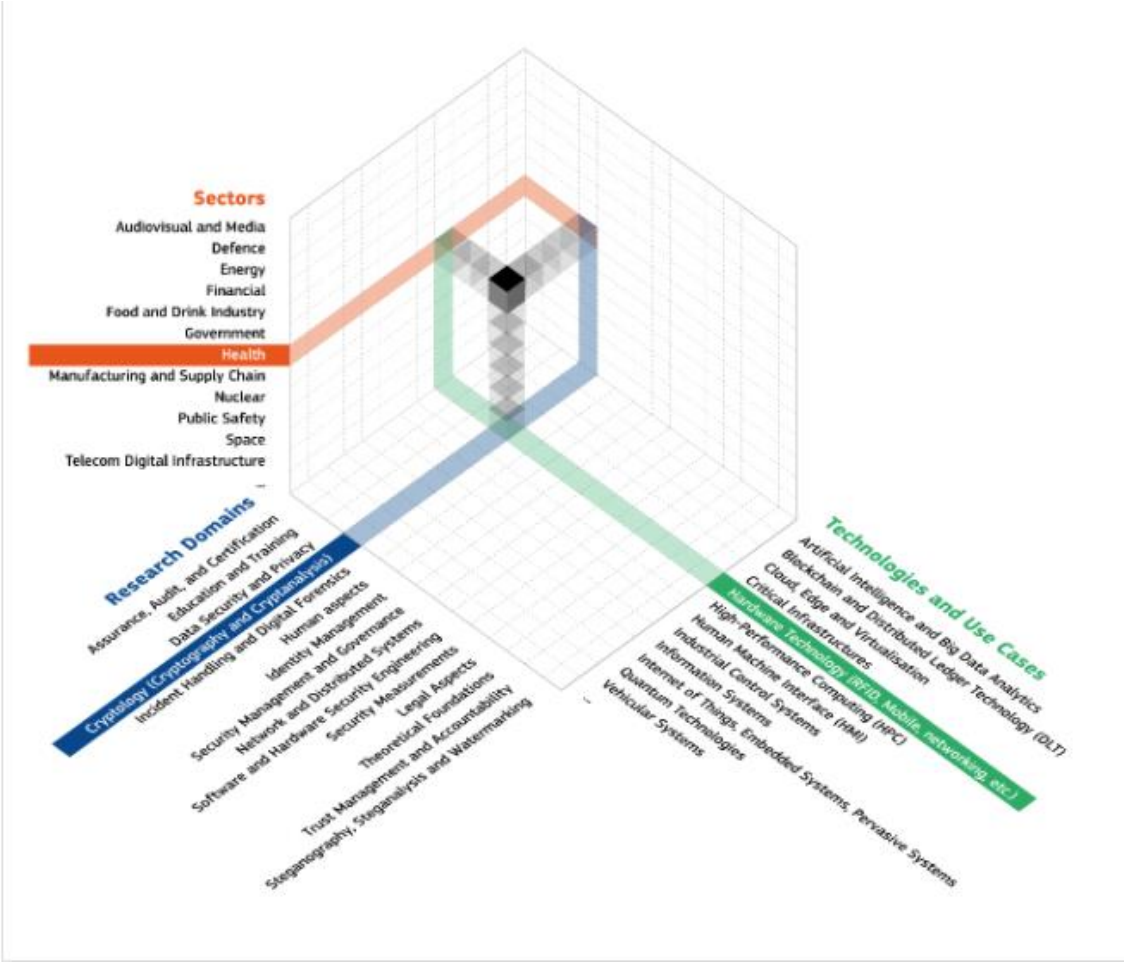
Ο ρόλος του ENISA ενισχύεται από τον νόμο περί ασφάλειας στον κυβερνοχώρο (**Cybersecurity Act**) που πλέον έχει μόνιμη εντολή και εξουσία να συμβάλει στην ενίσχυση τόσο της επιχειρησιακής συνεργασίας όσο και της διαχείρισης κρίσεων σε ολόκληρη την ΕΕ, θεσπίζοντας ένα πλαίσιο πιστοποίησης κυβερνοασφάλειας για προϊόντα και υπηρεσίες (European Commision, 2021). Ο παραπάνω νόμος περιγράφει τη διαδικασία που πρέπει να ακολουθηθεί και στη συνέχεια ο οργανισμός, ως κύριο μέλος της Ευρωπαϊκής Επιτροπής, εξετάζει την έκδοση πιστοποίησης. Η ύπαρξη ενός κοινού συστήματος πιστοποίησης θα ήταν χρήσιμη σε όλους ώστε να μην υπάρχουν διαφορές στον έλεγχο και στην πιστοποίηση των προϊόντων για συμμόρφωση με υψηλά πρότυπα ασφάλειας στον κυβερνοχώρο. (European Commission, 2021)

Οι απειλές για την ασφάλεια στον κυβερνοχώρο είναι σχεδόν πάντα διασυνοριακές και μια επίθεση στον κυβερνοχώρο στις κρίσιμες εγκαταστάσεις μιας χώρας μπορεί να επηρεάσει την ΕΕ στο σύνολό της. Τα κράτη μέλη της ΕΕ πρέπει να διαθέτουν ισχυρούς κυβερνητικούς φορείς που εποπτεύουν την ασφάλεια στον κυβερνοχώρο στη χώρα τους, να συνεργάζονται με τους ομολόγους τους σε άλλα κράτη μέλη, κοινοποιώντας πληροφορίες. Αυτό έρχεται να διασφαλίσει η εν λόγω οδηγία, την οποία έχουν πλέον εφαρμόσει όλες οι χώρες, δηλαδή τη δημιουργία και τη συνεργασία τέτοιων κυβερνητικών φορέων.

Σε συνέχεια, τα Κέντρα Ανταλλαγής και Ανάλυσης Πληροφοριών (**ISAC**) προωθούν τη συνεργασία μεταξύ της κοινότητας ασφάλειας στον κυβερνοχώρο σε διάφορους τομείς της οικονομίας. Σε συνεργασία με τον ENISA, η Επιτροπή προωθεί επίσης τη δημιουργία νέων ISAC σε τομείς που δεν καλύπτονται. Η «ενδυνάμωση κοινοπραξίας ISAC της ΕΕ», υπό την εποπτεία της Επιτροπής, παρέχει νομική, τεχνική και οργανωτική υποστήριξη για τις ISAC.

Το Κοινό Κέντρο Ερευνών (**JRC**) της Επιτροπής συμβάλλει ενεργά στην ασφάλεια στον κυβερνοχώρο έχοντας αναπτύξει μια Ταξινόμηση (**Cybersecurity Taxonomy**). Αυτό ευθυγραμμίζει την ορολογία που χρησιμοποιείται στην ασφάλεια στον κυβερνοχώρο, έτσι ώστε να μπορούμε να έχουμε μια σαφέστερη επισκόπηση των δυνατοτήτων της κυβερνοασφάλειας. Πιο συγκεκριμένα, αυτή η ταξινόμηση γίνεται προκειμένου α) να ενθαρρυνθεί δραστηριότητες διαχείρισης γνώσης, β) να καταστεί δυνατή η αποτελεσματική επικοινωνία μεταξύ των θεσμικών οργάνων, γ) να χρησιμεύει ως ακρογωνιαίος λίθος στις μελλοντικές προσπάθειες συνεργασίας μεταξύ των εμπλεκόμενων και δ) να υποστηρίξει τη διακυβέρνηση των μελλοντικών πρωτοβουλιών. Το παρακάτω σχήμα απεικονίζει οπτικά πώς μπορεί να εφαρμοστεί η

τρισδιάστατη ταξινόμηση για την ταξινόμηση γνώσεων στον κυβερνοασφάλεια (European Commission, 2021).



Εικόνα 5 - Τρισδιάστατη ταξινόμηση (European Commission, 2021)

Σύμφωνα με την οδηγία NIS, τα κράτη μέλη της ΕΕ οφείλουν να διασφαλίζουν ότι διαθέτουν ομαλές ομάδες απόκρισης σε περιστατικά ασφάλειας υπολογιστών (**CSIRTs**), γνωστές και ως ομάδες αντιμετώπισης έκτακτης ανάγκης σε υπολογιστές (**CERTs**). Αυτές οι ομάδες προσφέρουν στην πράξη για συμβάντα και κινδύνους στον κυβερνοχώρο, με συνεργασία του ιδιωτικού τομέα και των μελών τους σε επίπεδο ΕΕ. Όλοι οι τύποι χειριστών βασικών υπηρεσιών και παρόχων ψηφιακών υπηρεσιών πρέπει να καλύπτονται από καθορισμένους CSIRT. Τα κύρια καθήκοντα των CSIRT είναι:

- παρακολούθηση των περιστατικών σε εθνικό επίπεδο
- παροχή έγκαιρης προειδοποίησης, ειδοποιήσεων, ανακοινώσεων και άλλων πληροφοριών σχετικά με κινδύνους και συμβάντα σε σχετικούς ενδιαφερόμενους
- απάντηση σε περιστατικά
- παρέχοντας δυναμική ανάλυση κινδύνου και συμβάντων και επίγνωση κατάστασης
- συμμετοχή στο δίκτυο CSIRTs

Ο Ευρωπαϊκός Οργανισμός Cybersecurity (**ECSO**) δημιουργήθηκε το 2016 προκειμένου να ενεργήσει ως ομόλογος της Επιτροπής σε μια συμβατική σύμπραξη δημόσιου-ιδιωτικού τομέα που καλύπτει το πρόγραμμα «Ορίζοντας 2020» από τα έτη 2016 έως 2020. Η πλειοψηφία των 250 μελών της ECSO ανήκουν είτε στον κλάδο της Cybersecurity είτε σε ερευνητικά και ακαδημαϊκά ιδρύματα στον τομέα. Σε μικρότερο βαθμό, τα μέλη του ECSO περιλαμβάνουν επίσης

παράγοντες του δημόσιου τομέα και βιομηχανίες από τη ζήτηση. Εκτός από την υποβολή συστάσεων για το πρόγραμμα «Ορίζοντας 2020», το ECSO πραγματοποιεί διάφορες δραστηριότητες με στόχο την οικοδόμηση της κοινότητας και τη βιομηχανική ανάπτυξη σε ευρωπαϊκό επίπεδο.

Είναι επίσης σημαντικό να τονιστεί ο ρόλος των γυναικών στην κοινότητα της ασφάλειας στον κυβερνοχώρο, οι οποίες υποεκπροσωπούνται. Αυτός είναι ο λόγος για τον οποίο η Επιτροπή δημιούργησε το Women4Cyber Registry , σε συνεργασία με την πρωτοβουλία Women4Cyber του ECSO. Διευκολύνει τα μέσα μαζικής ενημέρωσης, τους διοργανωτές εκδηλώσεων και άλλους να βρουν τις πολλές ταλαντούχες γυναίκες που εργάζονται στην ασφάλεια στον κυβερνοχώρο, οπότε αυτές οι γυναίκες γίνονται πιο ορατές και εξέχουσες στην κοινότητα αυτή και στη δημόσια συζήτηση (European Commission, 2021).

Η ΕΕ για να ενισχύσει την κυβερνοασφάλεια διαθέτει πλέον πληθώρα μέσων για την προστασία των δικτύων ηλεκτρονικών επικοινωνιών, όπως για παράδειγμα, την οδηγία για την ασφάλεια συστημάτων δικτύου και πληροφοριών (οδηγία NIS). Η Οδηγία εισάγει νέους μηχανισμούς συνεργασίας και μέτρα με στόχο την ενίσχυση της εθνικής ικανότητας σε επίπεδο ΕΕ. Οι φορείς εκμετάλλευσης βασικών υπηρεσιών και οι πάροχοι ψηφιακών υπηρεσιών πρέπει επίσης να εφαρμόζουν πρακτικές διαχείρισης κινδύνου και να αναφέρουν σημαντικά συμβάντα στις εθνικές αρχές.

Ο νόμος για την κυβερνοασφάλεια εισάγει, για πρώτη φορά σε επίπεδο ΕΕ, κανόνες πιστοποίησης κυβερνοασφάλειας για προϊόντα, διαδικασίες και υπηρεσίες. Επιπλέον, ο νόμος για την κυβερνοασφάλεια προβλέπει μια νέα μόνιμη εντολή για τον Οργανισμό Κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης (ENISA), ο οποίος ταυτόχρονα έχει πρόσβαση σε πρόσθετους πόρους για την επίτευξη των στόχων του. Σύμφωνα με τους νέους κανονισμούς τηλεπικοινωνιών (Ευρωπαϊκό Κώδικα Ηλεκτρονικών Επικοινωνιών), τα κράτη μέλη πρέπει να εγγυώνται την ακεραιότητα και την ασφάλεια των δημόσιων δικτύων επικοινωνιών και είναι υποχρεωμένα να διασφαλίζουν ότι οι εμπλεκόμενοι φορείς λαμβάνουν τεχνικά και οργανωτικά μέτρα για σωστή διαχείριση τυχόν κινδύνων

Οι αρμόδιες εθνικές ρυθμιστικές αρχές θα πρέπει επίσης να έχουν εξουσίες, συμπεριλαμβανομένης της εξουσίας να εκδίδουν δεσμευτικές οδηγίες και να διασφαλίζουν τη συμμόρφωση σε αυτές. Επιπλέον, για την προστασία του απορρήτου των επικοινωνιών, τα κράτη μέλη μπορούν να επισυνάψουν όρους στη γενική άδεια του φορέα εκμετάλλευσης σχετικά με την προστασία των δημόσιων δικτύων από μη εξουσιοδοτημένη πρόσβαση.

Τέλος, τον Μάιο του 2019 θεσπίστηκε ένα καθεστώς κυρώσεων από το Συμβούλιο , το οποίο δίνει στην Ε.Ε. την αξίωση της επιβολής στοχευμένων μέτρων με σκοπό την πρόληψη και την διαχείριση κυβερνοεπιθέσεων που αποτελούν εξωτερική απειλή για την Ε.Ε. ή τα κράτη μέλη της. Το νέο καθεστώς κυρώσεων περιλαμβάνεται στην εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο και παρέχει ένα πλαίσιο για την ανάληψη κοινής διπλωματικής δράσης σε επίπεδο ΕΕ με σκοπό την αντιμετώπιση κακόβουλων κυβερνοδραστηριοτήτων.

Τα κύρια καθήκοντα του οργανισμού της ΕΕ για την κυβερνοασφάλεια βάσει της νέας εντολής είναι:

- **Στήριξη της εφαρμογής πολιτικής**, ιδίως της οδηγίας NIS, καθώς και άλλων κανονισμών σε διαφορετικούς τομείς ‘όπως είναι η ενέργεια, οι μεταφορές και τα χρηματοοικονομικά. Και παροχή βοήθειας προς τα κράτη μέλη για την εφαρμογή της ενωσιακής πολιτικής και νομοθεσίας που αφορά την προστασία των δεδομένων και την ιδιωτική ζωή.
- **Διαμόρφωση δεξιοτήτων,** η οποία θα επιτευχθεί με εκπαιδευτικό υλικό που θα συμβάλει στην τεχνογνωσία όλων των αρμόδιων φορέων, ώστε να είναι εμπράκτως σε θέση να αντιμετωπίσουν τυχόν απειλές.
- **Μέτρα που αφορούν την αγορά**, όπως ανάλυση των σχετικών τάσεων στην αγορά κυβερνοασφάλειας με στόχο την καλύτερη αντιστοίχιση ζήτησης και προσφοράς, και στήριξη της χάραξης κοινής πολιτικής στους τομείς της τυποποίησης και πιστοποίησης της κυβερνοασφάλειας ΤΠΕ.

- **Συνεργασία των επιχειρήσεων και αντιμετώπιση κρίσεων.** Συγκεκριμένα, εστίαση στις επιχειρησιακές ικανότητες που θα στηρίξουν την επιχειρησιακή συνεργασία στο πλαίσιο της γραμματείας του δικτύου CSIRT και τη διαχείριση περιστατικών διασυνοριακών κυβερνοεπιθέσεων.
- **Συντονισμένη δημοσιοποίηση τρωτών σημείων**: Αρωγή και προσπάθεια βελτίωσης συνεργασίας των κρατών-μελών και των λοιπών θεσμικών οργάνων της Ε.Ε. στο πλαίσιο του ενστερνισμού και της τήρησης πολιτικών δημοσιοποίησης τρωτών σημείων (lawspot, 2021)

Όμως, επειδή η κυβερνοασφάλεια αποτελεί διεθνές ζήτημα, επιβάλλεται να γίνει μια μικρή αναφορά σχετικά με το τι ισχύει σε παγκόσμιο επίπεδο. Με βάση μια παρουσίαση το Νομικό πλαίσιο για την ασφάλεια στον κυβερνοχώρο αποτελείται από Διεθνείς και Διμερείς Συμφωνίες, από τις Νομοθετικές Ρυθμίσεις της ΕΕ, το Εθνικό δίκαιο και τους Εσωτερικούς κανονισμούς.

Μέσα στις Διεθνείς Δραστηριότητες/ΟΗΕ είναι τα ψηφίσματα γενικής Συνέλευσης για:

1. Εξελίξεις στον Τομέα της Πληροφορίας και των Τηλεπικοινωνιών στο Πλαίσιο της Διεθνούς Ασφάλειας
2. Καταπολέμηση της Εγκληματικής Κατάχρησης της Πληροφορικής
3. Δημιουργία Παγκόσμιας Κουλτούρας Κυβερνοασφάλειας
4. Προστασία Κρίσιμων Πληροφοριακών Υποδομών.

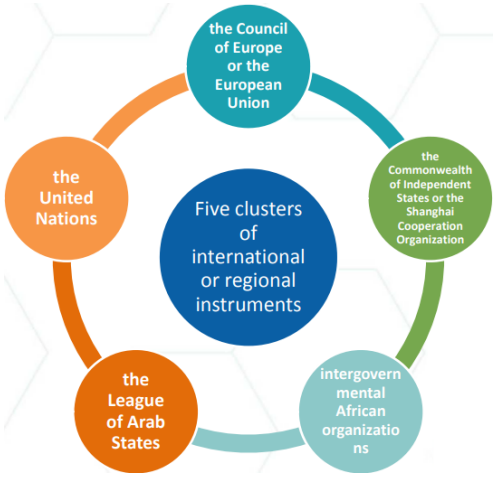
Αλλά και άλλες διεθνείς δραστηριότητες όπως είναι:

1. International Telecommunication Union: Παγκόσμια Ατζέντα Κυβερνοασφάλειας (GCA)
2. INTERPOL: Συντονίζει τις υπηρεσίες επιβολής του νόμου και τη νομοθεσία
3. NATO: Πολιτική και Έννοια Κυβερνοάμυνας
4. Ομάδα υψηλής τεχνολογίας G8: Συστάσεις και βέλτιστες πρακτικές
5. OECD, αρκετοί περιφερειακοί οργανισμοί (Cyber Security International Legislation, 2022)

Αναφορικά με την Διεθνή Ένωση Τηλεπικοινωνιών (ITU) είναι η εξειδικευμένη υπηρεσία των Ηνωμένων Εθνών για τις τεχνολογίες πληροφοριών και επικοινωνιών. Κεντρικά εργαλεία και υπηρεσίες που προσφέρει η ITU είναι

1. η από κοινού αναπτυγμένη εργαλειοθήκη για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο
2. η θεματική συνεργασία με το Γραφείο των Ηνωμένων Εθνών για τα Ναρκωτικά και το Έγκλημα (UNODC) σχετικά με τον μετριασμό των κινδύνων που ενέχει το έγκλημα στον κυβερνοχώρο και την ασφαλή χρήση των ΤΠΕ μέσω διαφόρων κοινών πρωτοβουλιών και δημιουργίας ικανοτήτων προς όφελος χωρών σε όλο τον κόσμο καθώς και
3. εξατομικευμένη υποστήριξη και τεχνική βοήθεια για τα μέλη της ITU που έχουν σχεδιαστεί για να ανταποκρίνονται στις επιμέρους απαιτήσεις της χώρας. (ITU, 2022)

Σε μία παρουσίαση που έγινε από ITRC σχετικά με το Cyber Crime Legislation αναφέρθηκαν 5 ομάδες διεθνών / περιφερειακών οργανισμών που καταπολεμούν το κυβερνοέγκλημα όπως φαίνεται και στην παρακάτω εικόνα.



Εικόνα 6 - Ομάδες διεθνών / περιφερειακών οργανισμών (Iran Telecommunication Research Center - Cyber Crime Legislation, 2022)

Επίσης, σημειώθηκε ότι από διεθνή καθεστώτα νομικής συνδρομής υπάρχουν διάφορες συνθήκες στη διεθνή συνεργασία όπως:

1. Συνθήκες «έκδοσης»: η έκδοση μπορεί να οριστεί ως η επίσημη διαδικασία κατά την οποία ένα κράτος ζητά την αναγκαστική επιστροφή ενός ατόμου που κατηγορείται ή έχει καταδικαστεί για έγκλημα για να δικαστεί ή να εκτίσει ποινή στο αιτούν κράτος.
2. Αμοιβαία νομική συνδρομή: τα βασικά εργαλεία της διεθνούς συνεργασίας περιλαμβάνουν την παροχή βοήθειας στη συλλογή αποδεικτικών στοιχείων για χρήση σε ποινικές υποθέσεις και ρυθμίσεις για τη διεθνή μεταφορά καταδίκων. Η διαδικασία που πρέπει να ακολουθείται για την επεξεργασία τόσο των εισερχόμενων όσο και των εξερχόμενων αιτημάτων ορίζεται συχνά στην εθνική νομοθεσία.
3. Άτυπη επικοινωνία αστυνομίας με αστυνομία: μέρη της διαδικασίας εξωεδαφικών ερευνών επιβολής του νόμου μπορεί να αναληφθούν από άτυπη επικοινωνία αστυνομίας-αστυνομίας ή υπηρεσίας-υπηρεσίας. Αυτή η επικοινωνία μπορεί να χρησιμοποιηθεί πριν από την επίσημη αίτηση αμοιβαίας νομικής συνδρομής σε αρμόδια αρχή ή για να διευκολυνθεί ένα επίσημο αίτημα.

Επίσης, σχολιάστηκε ότι υπάρχει ένας Παγκόσμιος Δείκτης Κυβερνοασφάλειας (GCI) ο οποίος στοχεύει να μετρήσει το επίπεδο δέσμευσης κάθε χώρας στην ασφάλεια στον κυβερνοχώρο σε πέντε βασικούς τομείς:

a) Νομικά Μέτρα
b) Τεχνικά Μέτρα
c) Οργανωτικά Μέτρα
d) Ανάπτυξη ικανοτήτων
e) Εθνική και Διεθνής Συνεργασία (Iran Telecommunication Research Center - Cyber Crime Legislation, 2022)

Η προοπτική του United Nations Office on Drugs and Crime[14] στη Διεθνή Συνεργασία αναφέρει για τα διεθνή νομικά πλαίσια σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο ότι:

- Τα εγκλήματα που αφορούν ηλεκτρονικά στοιχεία αποτελούν μοναδικές προκλήσεις για τη διεθνή συνεργασία.
- Λόγω της ασταθούς φύσης των ηλεκτρονικών αποδεικτικών στοιχείων, η διεθνής συνεργασία για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο απαιτεί έγκαιρη ανταπόκριση και δυνατότητα αίτησης εξειδικευμένων διερευνητικών ενεργειών, συμπεριλαμβανομένης της διατήρησης και παραγωγής δεδομένων από παρόχους του ιδιωτικού τομέα.
- Οι χρόνοι απόκρισης σε αιτήματα αμοιβαίας νομικής συνδρομής που περιλαμβάνουν τη διερεύνηση του εγκλήματος στον κυβερνοχώρο μπορεί συχνά να είναι εκτός των περιόδων διατήρησης δεδομένων των παροχών υπηρεσιών ή μπορεί να επιτρέψουν στους δράστες να καταστρέψουν μόνιμα βασικά ψηφιακά στοιχεία.
- Η αποτελεσματική διεθνής συνεργασία σε υποθέσεις που αφορούν ηλεκτρονικά αποδεικτικά στοιχεία απαιτεί επομένως μηχανισμούς για την ταχεία διατήρηση των δεδομένων εν αναμονή της εξέτασης περαιτέρω ερευνητικών μέτρων.
- (OAS - International legal frameworks for combating cybercrime: the UNODC perspective, 2022)

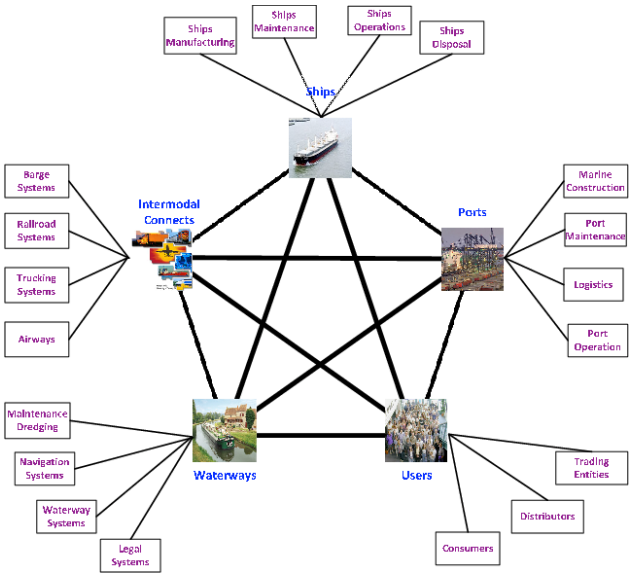
[14] Για περισσότερες πληροφορίες σχετικά με μία Ολοκληρωμένη μελέτη για το έγκλημα στον κυβερνοχώρο η οποία έγινε από το UNODC μπορείτε να ανατρέξετε στο παρακάτω site https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf

Επίσης μία ιστοσελίδα που περιέχει βάση δεδομένων σχετικά με τις νομοθεσίες είναι η SHERLOC (Sharing Electronic Resources and Laws on Crime) αναπτύσσεται και διατηρείται από το Γραφείο των Ηνωμένων Εθνών για τα Ναρκωτικά και το Έγκλημα (UNODC) για τη διευκόλυνση της διάδοσης πληροφοριών. https://sherloc.unodc.org/cld/v3/sherloc/legdb/index.html?lng=en

Κεφάλαιο 2: Ναυτιλία και Τεχνολογία

2.1 Εισαγωγικό Σημείωμα

Στο σημείο αυτό διαπιστώνουμε ότι η ναυτιλία είναι μία συνάρτηση από συστήματα που είναι μοναδικά και ανεξάρτητα μεταξύ τους, αλλά ταυτόχρονα συνεξαρτώμενα και αλληλένδετα. Όπως φαίνεται και στην παρακάτω εικόνα, το σύστημα θαλάσσιων μεταφορών αποτελείται κυρίως από τα πλοία, τις ναυτιλιακές γραμμές, τα λιμάνια, τους ανθρώπους (είτε αυτοί είναι πελάτες είτε πωλητές) αλλά και από τις μεταφορές στην ενδοχώρα. Η ζωή ενός πλοίου διασταυρώνεται με τη ζωή ενός λιμανιού και είναι μόνο ένα μέρος της ζωής της ναυτιλιακής γραμμής. Οι άνθρωποι και τα φορτία διασταυρώνονται με το ταξίδι και τη διέλευση του πλοίου μέσω λιμένων, διατροπικών μεταφορών και εσωτερικών πλωτών οδών. Οπότε γίνεται αντιληπτό ότι, εφόσον πρόκειται για μια αλυσίδα συστημάτων εφοδιασμού, μία επίθεση σε ένα από τα παραπάνω συστήματα θα μπορούσε να επιφέρει ζημία και σε όλα τα υπόλοιπα. Έτσι, λοιπόν συνειδητοποιούμε την ανάγκη ύπαρξης ασφάλειας σε όλα τα εμπλεκόμενα συστήματα.

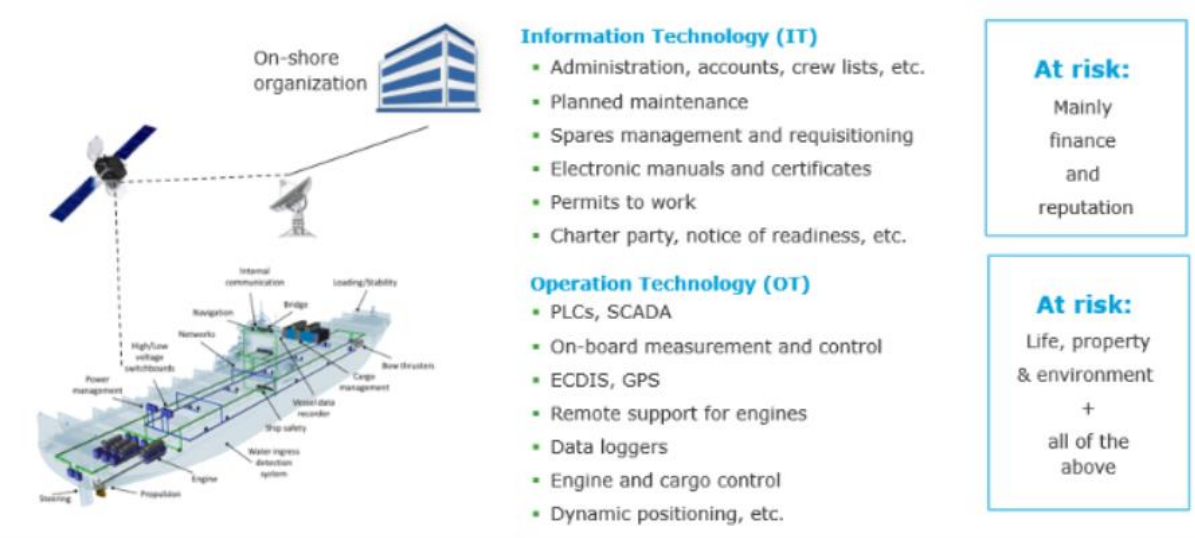


Εικόνα 7 - Σύστημα θαλάσσιων μεταφορών (Semantic Scholar, 2022)

Για να εξασφαλίσουμε μια ομαλή λειτουργία των παραπάνω, σαφώς και πρέπει να υπάρχει ανταλλαγή πληροφοριών μεταξύ τους. Η τεχνολογία ρυθμίζει τις επικοινωνίες, τον έλεγχο και τη διαχείριση του φορτίου των πλοίων. Σήμερα, υπάρχει καθημερινή επικοινωνία μεταξύ πλοίων, εταιρειών, λιμενικών εγκαταστάσεων και ναυτιλιακών πρακτόρων. Όπως είναι κατανοητό, η ανάγκη βελτιστοποίησης διαφορετικών επιχειρηματικών μοντέλων σχετίζεται άμεσα με την εφαρμογή νέων ψηφιακών τεχνολογιών που παρέχουν αυτοματοποίηση των διαδικασιών και των λειτουργιών των σκαφών. Τα δορυφορικά συστήματα χρησιμοποιούνται όλο και περισσότερο για διάφορους λειτουργικούς και εμπορικούς σκοπούς, καθώς και για αναψυχή και ψυχαγωγία. Υπάρχει πληθώρα δεδομένων για τα πλοία σήμερα, από πολλές διαφορετικές πηγές.

Πολλά ενσωματωμένα συστήματα έχουν σχεδιαστεί για να συλλέγουν δεδομένα και να τα καθιστούν διαθέσιμα σε εταιρείες, στο πλήρωμα, σε προμηθευτές και σε κατασκευαστές για τη διαδικασία λήψης αποφάσεων κατά την καθημερινή λειτουργία του σκάφους. Όπως είχε πει και ο κος. Μ. Σέρβος, Head of Energy Efficiency της Minerva Marine Inc., στη συνέντευξή του από την Isalos net, μακροπρόθεσμα οδηγούμαστε σε μια έξυπνη ναυτιλία, που προϋποθέτει πλοία εφοδιασμένα με κατάλληλο εξοπλισμό, που επιτρέπει την αυτόματη καταγραφή δεδομένων από όλα τα κύρια μηχανήματα του πλοίου. Και στη συνέχεια αυτά προωθούνται σε πραγματικούς χρόνους στη στεριά, όπως για παράδειγμα πληροφορίες για τον καιρό και τις θαλάσσιες διαδρομές, ώστε να επιλέγονται αυτόματα οι καλύτερες δυνατές πορείες με γνώμονα την

ασφάλεια και την εξοικονόμηση ενέργειας. Αυτά τα δεδομένα θα επεξεργάζονται και θα συντελούν στη λήψη αποφάσεων οι οποίες μπορεί να σχετίζονται είτε με τη συντήρηση είτε με την εμπορική διαχείριση των πλοίων (Isalos.net, 2022).



Εικόνα 8 - Συστήματα κυβερνοχώρου στα πλοία (DNV, 2021)

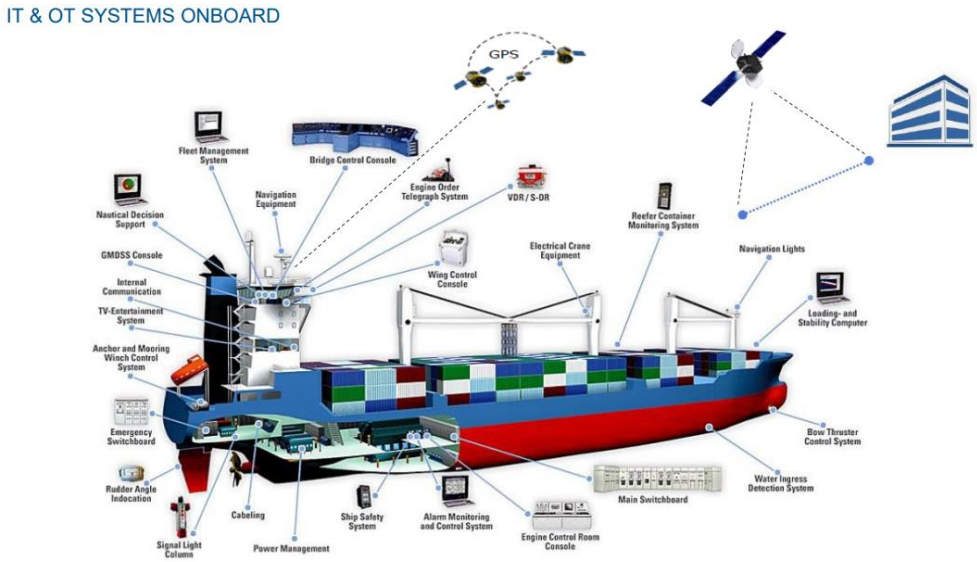
Τα συστήματα κυβερνοχώρου για πλοία και κινητές μονάδες ταξινομούνται είτε ως IT (τυπικά συστήματα πληροφοριών) είτε ως OT (συστήματα λειτουργίας και ελέγχου). Τα συστήματα πληροφορίων είναι συνήθως πιο αναβαθμισμένα όσον αφορά την ασφάλεια στον κυβερνοχώρο, με καθιερωμένες διαδικασίες, τεχνολογία και εκπαίδευση που εφαρμόζονται χρησιμοποιώντας ένα σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) - τουλάχιστον στην ξηρά. Η παραβίαση των συστημάτων πληροφορικής μπορεί να έχει σημαντικό αντίκτυπο στην οικονομία και στη φήμη. Ωστόσο, συνήθως δεν επηρεάζει την ασφαλή λειτουργία των πλοίων και των μονάδων. Το OT, αντίθετα, είναι λιγότερο εξελιγμένο όσον αφορά στην ασφάλεια στον κυβερνοχώρο και μια επίθεση στα συστήματα αυτά επί του σκάφους μπορεί να θέσει σε κίνδυνο την ασφάλεια του πλοίου, του πληρώματος και του περιβάλλοντος (DNV, 2021).

Ως πλοίο με δυνατότητα κυβερνοχώρου («Cyber enabled ships») νοείται το πλοίο που αποτελείται από συστήματα τα οποία κατά κύριο λόγο ελέγχονται από το πλήρωμα. Ωστόσο, μέσω της ραγδαίας εξέλιξης στον τομέα της πληροφορικής (IT) και της επιχειρησιακής τεχνολογίας (OT), έχει πλέον δοθεί η δυνατότητα παρακολούθησης και ελέγχου είτε εξ αποστάσεως είτε αυτόνομα με ή χωρίς πλήρωμα επί του πλοίου. Η λειτουργικότητα που παρέχεται από αυτά τα συστήματα μπορεί να κυμαίνεται από μία απλή απομακρυσμένη παρακολούθηση με το πλήρωμα επί του σκάφους έως ένα πλήρως αυτόνομο σκάφος χωρίς πλήρωμα (Lloyd's Register, 2022). Επειδή ένα πλοίο με δυνατότητα κυβερνοχώρου αποτελείται από πολλαπλά, διασυνδεδεμένα συστήματα και λόγω του γρήγορου ρυθμού ανάπτυξης της τεχνολογίας, η διασφάλιση ότι ένα τέτοιο πλοίο θα είναι ασφαλές δεν μπορεί να είναι δεσμευτική και δεν μπορεί να βασίζεται στη γνώση που αποκτήθηκε από προηγούμενα συστήματα. Αντίθετα, απαιτεί μια προσέγγιση «συνολικών συστημάτων» – μια προσέγγιση που λαμβάνει υπόψη όλα τα διαφορετικά συστήματα στο πλοίο και στην ξηρά, πώς σχεδιάζονται και εγκαθίστανται, πώς συνδέονται και πώς θα διαχειρίζονται.

Με τον όρο cyber systems ή αλλιώς ICT (information communication technology) ορίζουμε όλα εκείνα τα τεχνολογικά συστήματα τα οποία χρησιμοποιούνται σε προηγμένα πλοία που δραστηριοποιούνται σε διάφορους τομείς, από υπεράκτια, πλοία έρευνας έως κρουαζιερόπλοια και προσαρμοσμένα γιοτ. Τα συστήματα που βασίζονται σε πλοία περιλαμβάνουν:

a) συστήματα πλοήγησης, συμπεριλαμβανομένων ηλεκτρονικών χαρτών, συστημάτων παγκόσμιας τοποθεσίας (GPS) και συστήματα δυναμικού εντοπισμού θέσης (DPS)

b) συστήματα ραντάρ και αυτόματης αναγνώρισης (AIS)
c) συστήματα επικοινωνιών, συμπεριλαμβανομένων των ραδιοεπικοινωνιών (επίγεια και δορυφορικά) και επικοινωνίες δεδομένων (ευρυζωνική, Voice over IP (VOIP), πρόσβαση στο διαδίκτυο και e-mail)
d) ολοκληρωμένα συστήματα γεφυρών
e) συστήματα ελέγχου για το ευρύ φάσμα ηλεκτρομηχανικών συστημάτων επί των πλοίων, όπως κύρια μηχανή, γεννήτριες, δεξαμενές έρματος, υποστήριξη ζωής, αντλίες καυσίμου και λαδιού, υδατοστεγείς πόρτες, συναγερμοί πυρκαγιάς και χειριστήρια, ανεμιστήρες συγκράτησης φορτίου και περιβαλλοντικοί έλεγχοι
f) εξοπλισμός που χρησιμοποιείται από ναυλωτές, όπως εξοπλισμός έρευνας (για παράδειγμα, σόναρ και συστήματα σεισμικής έρευνας) σημεία ασύρματης πρόσβασης, θύρες IP και ασύρματα τηλέφωνα. (Lloyd's Register, 2022)

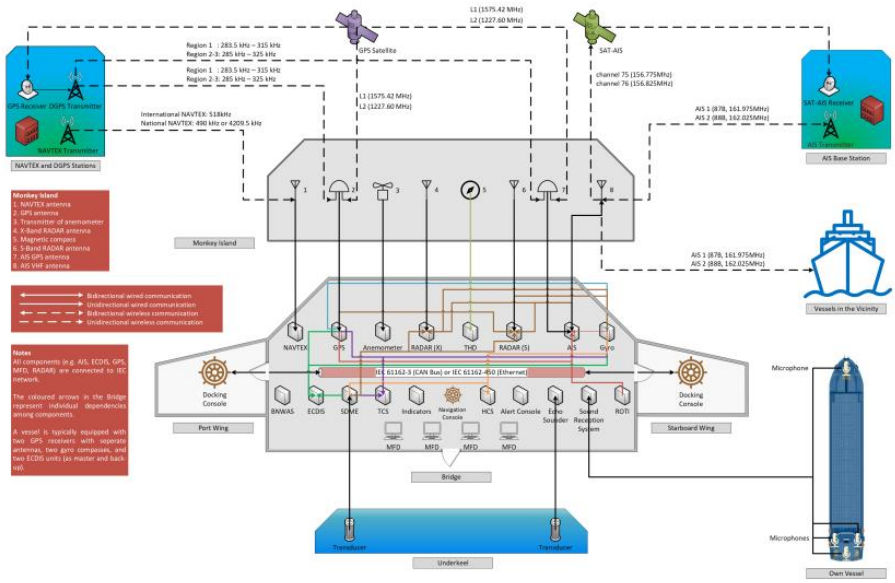


Εικόνα 9 - Τεχνολογικά συστήματα πάνω στο πλοίο (Gard, 2022)

2.2 Συστήματα γέφυρας / πλοήγησης

Τα συστήματα θαλάσσιας πλοήγησης που συνδέονται μέσω δικτύων επί του σκάφους αναφέρονται συνήθως ως ολοκληρωμένα συστήματα πλοήγησης (Integrated Navigation Systems - INS). Ο σκοπός τους είναι να βελτιώσουν την ασφάλεια της πλοήγησης παρέχοντας ολοκληρωμένες και επαυξημένες λειτουργίες για την αποφυγή γεωγραφικών, κυκλοφοριακών και περιβαλλοντικών κινδύνων. Περιλαμβάνει εργασίες πλοήγησης όπως «Σχεδιασμός διαδρομής», «Παρακολούθηση διαδρομής», «Αποφυγή σύγκρουσης», «Δεδομένα ελέγχου πλοήγησης», «Κατάσταση και εμφάνιση δεδομένων πλοήγησης» και «Διαχείριση ειδοποιήσεων»,

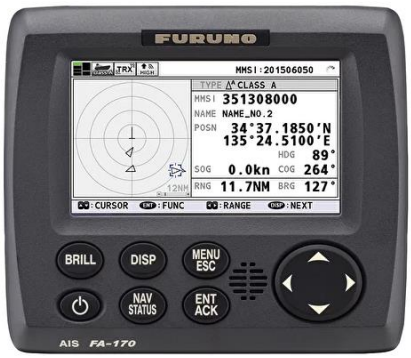
συμπεριλαμβανομένων των αντίστοιχων πηγών, δεδομένων και οθονών που είναι ενσωματωμένες σε ένα σύστημα πλοήγησης. (RESOLUTION MSC.252(83), 2022)



Εικόνα 10 - Σύνθεση ενός ολοκληρωμένου συστήματος πλοήγησης (MDPI, 2022)

Ένα τέτοιο σύστημα περιλαμβάνει το υλικό και το λογισμικό της γέφυρας όπου όλες οι λειτουργίες που σχετίζονται με την πλοήγηση και την ασφαλή λειτουργία του πλοίου ενοποιούνται σε μια ενιαία κονσόλα, ενσωματώνοντας την είσοδο από πολλά από τα υποσυστήματα του πλοίου, συμπεριλαμβανομένων:

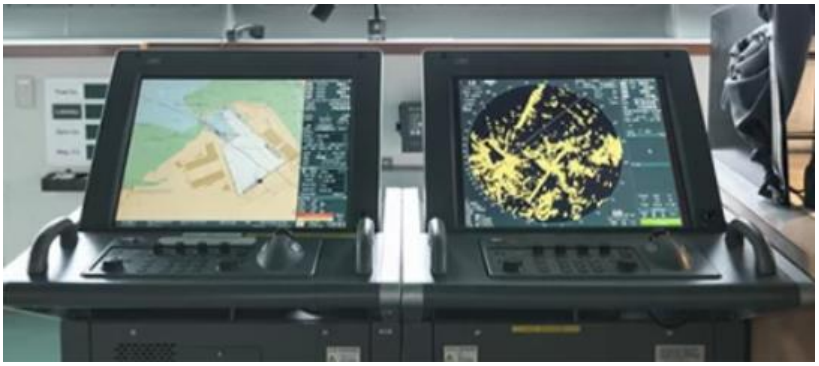
I. **AIS:** βοηθά στην ασφαλή πλοήγηση. Μεταδίδει τρεις τύπους δεδομένων και μηνύματα που σχετίζονται με την ασφάλεια σε άλλα σκάφη και σταθμούς στην ακτή. Εκτελεί τις ακόλουθες τέσσερις λειτουργίες 1) αναγνώριση πλοίων, 2) βοήθεια στην παρακολούθηση στόχων, 3) ανταλλαγή πληροφοριών και 4) παροχή πρόσθετων πληροφοριών για την επίγνωση της κατάστασης.



Εικόνα 11 - Automatic Identifications System (Marine Digital, 2022)

II. Σύστημα συναγερμού πλοήγησης γέφυρας (BNWAS): έχει τρεις επιλογές (μόνιμα κλειστό, μόνιμα ανοιχτό ή αυτόματο) και λειτουργεί για την αποφυγή ναυτικού ατυχήματος – δίνοντας προειδοποιήσεις σε περίπτωση ανικανότητας του αξιωματικού βάρδιας παρακολούθησης, λόγω ατυχήματος, ασθένειας ή σε περίπτωση παραβίασης της ασφάλειας (Marine Insight, 2022).
III. Human Machine Interface: έχει εξίσου 3 κατηγορίες (“συναγερμός”, “προειδοποίηση” και “προσοχή”) και ενημερώνει το πλήρωμα με οπτικοακουστικά ερεθίσματα.

IV. **Κύρια Μηχανή:** παρέχει ισχύ για το κύριο σύστημα πρόωσης του σκάφους.
V. Συστήματα ελέγχου κύριου πηδαλίου: Το βασικό μέρος για τον έλεγχο του πηδαλίου είναι το τιμόνι ή ο μοχλός του τιμονιού.
VI. Συστήματα ελέγχου προωθητή (thruster controls): είναι για την καλύτερη δυνατότητα ελιγμών.
VII. **Ηλεκτρονικά Συστήματα Εμφάνισης Χαρτών και Πληροφοριών (ECDIS):** είναι η υποστήριξη της ασφαλούς πλοήγησης, επιτρέπει τον προγραμματισμό και την παρακολούθηση διαδρομής.



Εικόνα 12 - ECDIS (Marine Digital, 2022)

VIII. Βυθόμετρο: έχει σχεδιαστεί για να μετράει και να παρουσιάζει γραφικά το βάθος του νερού.

Εικόνα 13 – Βυθόμετρο (Marine Digital, 2022)

IX. **GPS/GNSS:** προσφέρει πληροφορίες εντοπισμού θέσης, ταχύτητας και χρόνου βάσει δορυφόρου.

Εικόνα 14 - GPS Receiver (Marine Digital, 2022)

X. Γυροσκοπική πυξίδα: χρησιμοποιείται για να ανιχνεύσει την κατεύθυνση της κεφαλής του σκάφους σε σχέση με τον πραγματικό (γεωγραφικό) βορρά χρησιμοποιώντας φυσικούς νόμους, επιρροές της βαρύτητας και την περιστροφή της Γης. Τα μαγνητικά πεδία δεν επηρεάζουν τις γυροσκοπικές πυξίδες για αυτό χρησιμοποιούνται ευρέως σε σκάφη ως κύρια συσκευή για την ανίχνευση του αληθινού βορρά.

Εικόνα 15 - Γυροσκοπική Πυξίδα (Marine Digital, 2022)

XI. Μαγνητική πυξίδα: είναι εγκατεστημένη στα πλοία για τον προσδιορισμό και την εμφάνιση πληροφοριών κατεύθυνσης χωρίς παροχή ρεύματος. Όμως, επειδή δημιουργούνται πολλά σφάλματα, θα πρέπει να είναι τοποθετημένη σε κατάλληλο κάδο με διορθωτικές συσκευές.

Εικόνα 16 - Μαγνητική πυξίδα (Marine Digital, 2022)

XII. **Σύστημα Ελέγχου Κατεύθυνσης (Heading Control System):** ή αλλιώς αυτόματος πιλότος, διατηρεί το σκάφος σε μια προκαθορισμένη κατεύθυνση χρησιμοποιώντας τις πληροφορίες κατεύθυνσης. Θα πρέπει να παρέχει αξιόπιστη λειτουργία κάτω από διάφορες ταχύτητες, καιρικές συνθήκες και συνθήκες φόρτωσης.

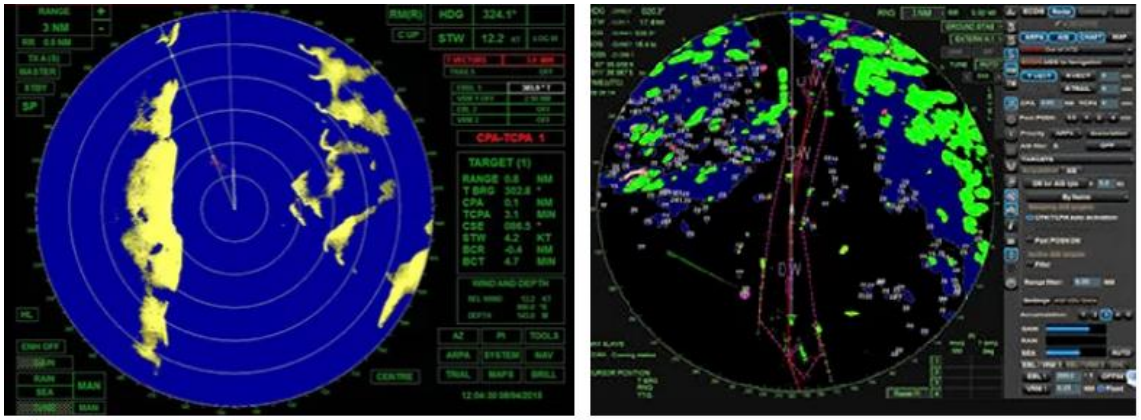
Εικόνα 17 - Αυτόματος πιλότος (Marine Digital, 2022)

XIII. Πολυλειτουργική Οθόνη (MFD): ορίζεται από τον IMO ως «Μια ενιαία μονάδα οπτικής απεικόνισης που μπορεί να παρουσιάσει, είτε ταυτόχρονα είτε μέσω μιας σειράς επιλέξιμων σελίδων, πληροφορίες από περισσότερες από μία λειτουργίες ενός INS». Ένας σταθμός εργασιών στη γέφυρα αποτελείται από το MFD με ειδικά χειριστήρια για την εμφάνιση και τη λειτουργία οποιασδήποτε εργασίας πλοήγησης, έτσι ώστε

μεμονωμένα στοιχεία (π.χ. RADAR και ECDIS) να μπορούν να συνδυαστούν σε μία μονάδα.

XIV. **Navigational Telex (NavTex):** είναι μια συσκευή επικοινωνίας για σκάφη. Λαμβάνει και εκτυπώνει αυτόματα ή εμφανίζει την ανακοίνωση των Πληροφοριών Θαλάσσιας Ασφάλειας (MSI) που είναι προειδοποιήσεις ναυσιπλοΐας και μετεωρολογικές προβλέψεις και άλλα επείγοντα μηνύματα που σχετίζονται με την ασφάλεια στα παράκτια ύδατα.

XV. Ραντάρ (Radio Detection And Ranging): Τα θαλάσσια σκάφη βασίζονται σε ένα σύστημα ραντάρ S-band και X-band για πλοήγηση, καθώς μπορεί να ανιχνεύσει στόχους και να εμφανίσει πληροφορίες στην οθόνη, όπως η απόσταση του πλοίου από το έδαφος, τυχόν επιπλέοντα αντικείμενα (νησί, βράχοι, παγόβουνο κ.λπ.), άλλα σκάφη και εμπόδια για την αποφυγή σύγκρουσης. Είναι μια περιστρεφόμενη κεραία που ανιχνεύει τη γύρω περιοχή του πλοίου. Το ίδιο και το Automatic Radar Plotting Aids που εμφανίζει τη θέση των κοντινών πλοίων και επιλέγει μια πορεία για το πλοίο, αποφεύγοντας κάθε είδους σύγκρουση. (Marine Digital, 2022)



a *b*

Εικόνα 18 – a) Radar b) ARPA (Marine Digital, 2022)

XVI. Σύστημα ήχου λήψης: Αυτό το σύστημα ηχείων είναι απαραίτητο για ένα πλοίο με μια πλήρως κλειστή γέφυρα. Αυτό επιτρέπει στον πλοηγό μέσα στην καμπίνα να ακούει ηχητικά σήματα (όπως ομίχλη ή κόρνα πλοίου) από άλλα πλοία που βρίσκονται στην περιοχή. Τοποθετείται στην κονσόλα του εξοπλισμού του πλοίου στη γέφυρα και βοηθά τον πλοηγό να παρακολουθεί σύμφωνα με τους Διεθνείς Κανόνες για την Πρόληψη Συγκρούσεων στη Θάλασσα. (Marine Digital, 2022)

Εικόνα 19 – Sound Reception System (Marine Digital, 2022)

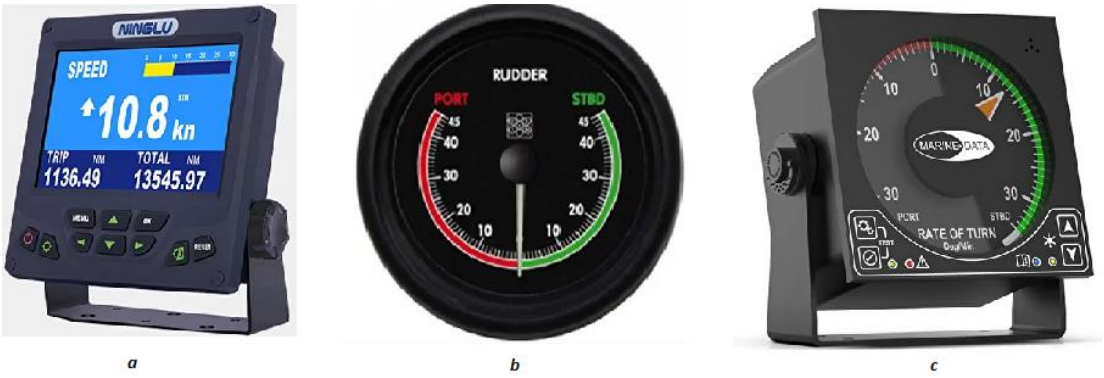
XVII. **Το σύστημα ελέγχου τροχιάς (Track Control System):** ή αλλιώς αυτόματος πιλότος, κατευθύνει το πλοίο προς ένα σημείο διαδρομής ή μια ακολουθία σημείων διαδρομής. Το

σύστημα ελέγχου τροχιάς μπορεί επίσης να έχει λειτουργία ελέγχου κατεύθυνσης. Το πλοίο διευθύνεται από το TCS ή το HCS σε αυτόματη λειτουργία.
Οι λειτουργίες διεύθυνσης χωρίζονται σε τρεις τύπους, και συγκεκριμένα "Auto", "Non-Follow Up (NFU)" και "Follow Up (FU)". Τόσο το NFU όσο και το FU μπορούν να ονομαστούν χειροκίνητες λειτουργίες διεύθυνσης. Ο έλεγχος του πηδάλιου μπορεί να γίνει είτε από το κεντρικό τιμόνι ή από τα πλευρικά τιμόνια (δεξιά και αριστερά – στα φτερά του πλοίου) που μπορεί να γίνει από το πλήρωμα κατά τη διάρκεια της πρόσδεσης. Υπάρχουν ανάλογοι διακόπτες που ορίζουν ποιο τιμόνι θα είναι σε λειτουργία όπως και αν θα είναι αυτόματα ή χειροκίνητα.

XVIII. Συσκευή Κατεύθυνση Εκπομπής (THD): από αυτήν δίνεται η πραγματική κατεύθυνση ενός πλοίου. Το THD παράγει ένα σήμα για την πραγματική κατεύθυνση προς άλλο εξοπλισμό στο πλοίο.

Εικόνα 21 - Transmitting Heading Device (Marine Digital, 2022)

XIX. Διάφορους αισθητήρες (όπως θερμοκρασία νερού, θέσεις πηδαλίου, ρυθμός στροφής, ταχύμετρο, αλμυρότητα, ανεμόμετρο κ.α.) (MDPI, 2022)



a b c

Εικόνα 20 - a) Speed & Distance Log Device b) Rudder Angle Indicator c) Rate of turn indicator (Marine Digital, 2022)

2.2.1 Global Navigation Satellite Systems

Στον τομέα της Ναυτιλίας, το GNSS χρησιμοποιείται για να ικανοποιήσει τη ζήτηση για πλοήγηση (σε ανοιχτή θάλασσα ή σε συγκεκριμένες καταστάσεις, όπως είσοδοι και προσεγγίσεις λιμανιών) και τον εντοπισμό θέσης (συμπεριλαμβανομένης, μεταξύ άλλων, της παρακολούθησης σκαφών, της διαχείρισης της κυκλοφορίας, των φάρων εντοπισμού για καταστάσεις κινδύνου, κ.λπ.) πλοίων και πληρωμάτων από διαφορετικούς ενδιαφερόμενους. Οι ανάγκες των χρηστών και οι απαιτήσεις απόδοσης των λύσεων GNSS εξαρτώνται σε μεγάλο βαθμό από τις εφαρμογές που

έχουν σχεδιαστεί για να ικανοποιούν τις ανάγκες βελτιωμένης ασφάλειας και παραγωγικότητας, σύμφωνα με την απόφαση του IMO A.915(22).

Όσον αφορά την **πλοήγηση**, απευθύνεται σε πλοία που υπόκεινται στον κανονισμό SOLAS αλλά όχι αποκλειστικά. Όλα τα επιβατηγά, τα φορτηγά, τα εμπορικά αλλά και τα ψυχαγωγικά πλοία βασίζονται σε μεγάλο βαθμό στο GNSS για τη ναυσιπλοΐα πόσο μάλλον σε περιοχές με υψηλή κυκλοφορία, με την διαφορά ότι τα πρώτα πρέπει να έχουν τουλάχιστον τρεις συσκευές τοποθετημένες. Επίσης, η πλοήγηση αφορά και τις εσωτερικές πλωτές οδούς (Inland Waterways) καθώς χρησιμοποιείται για την ασφαλή ναυσιπλοΐα σε αυτές (ποτάμια, κανάλια, λίμνες και εκβολές ποταμών).

Για τον **εντοπισμό θέσης** οι συνήθεις εφαρμογές όπου είναι απαραίτητο το GNSS είναι οι ακόλουθες:

a) **Διαχείριση και επιτήρηση κυκλοφορίας:** Αυτές οι δραστηριότητες υποστηρίζονται από συστήματα που βασίζονται σε GNSS, συμπεριλαμβανομένων των AIS και LRIT.
b) **Έρευνα και διάσωση:** είναι η αναζήτηση και η παροχή βοήθειας σε άτομα που βρίσκονται σε κίνδυνο. Διαφορετικοί τύποι συσκευών μπορούν να κάνουν χρήση της τοποθέτησης GNSS όπως φάροι **EPIRB** και **PLB** που μεταδίδουν, μόλις ενεργοποιηθούν, τις απαραίτητες πληροφορίες μέσω δορυφορικής επικοινωνίας. Ακόμη, οι συσκευές **AIS-SART** μεταδίδουν συνεχώς ένα μήνυμα ειδοποίησης που περιλαμβάνει τοποθεσία βάσει GNSS, η οποία σημάνει συναγερμό σε όλα τα πλοία εξοπλισμένα με AIS εντός εμβέλειας VHF[15].
c) **Έλεγχος αλιευτικών σκαφών:** Ο εντοπισμός θέσης GNSS επιτρέπει στα συστήματα παρακολούθησης σκαφών να ελέγχουν τη θέση των αλιευτικών σκαφών, καθώς και τον χρόνο παραμονής σε διεθνή και ξένα ύδατα, αλλά και σε προστατευμένες θαλάσσιες περιοχές κ.λπ.
d) **Λειτουργίες λιμένων:** Η πρόοδος της διέλευσης, οι εργασίες ελλιμενισμού και φόρτωσης-εκφόρτωσης των εμπορευματοκιβωτίων παρακολουθούνται μέσω τεχνολογιών που βασίζονται στο GNSS. Ακόμη, οι γερανογέφυρες, είναι εξοπλισμένες με συσκευές διεύθυνσης που καθορίζουν τη θέση του γερανού και διατηρούν την κίνηση στην επιθυμητή διαδρομή, βελτιώνοντας την ακρίβεια και την παραγωγικότητα, καθώς και την ασφάλεια των χειριστών και των εργαζομένων στο έδαφος.
e) **Ναυτική μηχανική:** Το GNSS χρησιμοποιείται για την υποστήριξη θαλάσσιων κατασκευαστικών δραστηριοτήτων (π.χ. τοποθέτηση καλωδίων και αγωγών) (GNSS Market Report, 2022)

Εκτός από την εφαρμογή του στη βελτίωση της θαλάσσιας ναυσιπλοΐας, το GNSS εφαρμόζεται επίσης σε ένα ευρύ φάσμα θαλάσσιων δραστηριοτήτων, όπως η τοποθέτηση εξόρυξης πετρελαίου, η εγκατάσταση και επιθεώρηση υποβρύχιων καλωδίων και αγωγών, και η βυθοκόρηση λιμένων και πλωτών οδών. Ένα βασικό όφελος είναι η γρήγορη διαχείριση των εμπορευματοκιβωτίων, το οποίο μειώνει την αλλοίωση των τροφίμων και παραδίδονται εγκαίρως. (HEXAGON, 2022) (HEXAGON, 2022)

Τα πλοία και τα λιμάνια βασίζονται στα παγκόσμια δορυφορικά συστήματα πλοήγησης (GNSS) για μια τεράστια γκάμα εφαρμογών που σχετίζονται με τη θέση, την ταχύτητα και την ακριβή παγκόσμια και τοπική ώρα. Ο Διεθνής Ναυτιλιακός Οργανισμός (IMO) επιβλέπει τη SOLAS (Ασφάλεια Πλοήγησης), και έχει την αρμοδιότητα να υιοθετεί επιχειρησιακές απαιτήσεις και μεταφοράς, καθώς και πρότυπα απόδοσης για την παγκόσμια ναυτιλία. Στο κεφάλαιο V για την ασφάλεια της ναυσιπλοΐας, η SOLAS 1960 περιλάμβανε μια απαίτηση για πλοία άνω των 1.600 ολικής χωρητικότητας σε διεθνή ταξίδια να είναι εξοπλισμένα με συσκευή εύρεσης κατεύθυνσης μέσω ραδιοφώνου – μια απαίτηση που χρονολογείται από το 1948.

Τα κράτη μέλη του IMO αναγνώρισαν και ενέκριναν στη Συνέλευση του 1997 (ψήφισμα A.860(20)) την ανάγκη για ένα Μελλοντικό Παγκόσμιο Δορυφορικό Σύστημα Πλοήγησης (GNSS)

[15] LRIT: Long-Range Identification and Tracking, EPIRBs: Emergency Position Indicating Radio Beacons, PLBs: Personal Location Beacons, AIS-SART: Automatic Identification System Search and Rescue Transmitter, VHF: Very High Frequency

το όποιο θα πληροί τις απαιτήσεις για την ακρίβεια πλοήγησης, την ακεραιότητα της υπηρεσίας, τη διαθεσιμότητα, την αξιοπιστία και την κάλυψη. Το 2000, προχώρησε στην υιοθέτηση υποχρεωτικών απαιτήσεων μεταφοράς για το GNSS και αναθεωρήθηκε το κεφάλαιο V της SOLAS, το οποίο τέθηκε σε ισχύ το 2002, που απαιτεί από τα πλοία να φέρουν GNSS ή δέκτη επίγειας ραδιοπλοήγησης, για να καθορίζουν και να ενημερώνουν τη θέση του πλοίου με αυτόματα μέσα, για χρήση ανά πάσα στιγμή καθ' όλη τη διάρκεια του ταξιδιού. Και το 2003 εγκρίθηκε το ψήφισμα A.953(23) το όποιο έκανε τα απαιτούμενα πρότυπα ακρίβειας πιο αυστηρά, κυρίως όσον αφορά σε εισόδους και προσεγγίσεις λιμανιών και παράκτια ύδατα. Το σφάλμα πληροφοριών θέσης δεν πρέπει να είναι μεγαλύτερο από 10 μέτρα με πιθανότητα 95%. Στα ωκεάνια ύδατα, το σύστημα θα πρέπει να παρέχει πληροφορίες θέσης με σφάλμα όχι μεγαλύτερο από 100 μέτρα με το ίδιο ποσοστό πιθανότητας. Μια μελέτη της London Economics έδειξε πως μια αποτυχία του GNSS στον ναυτιλιακό τομέα με διάρκεια πέντε ημερών θα μπορούσε να επιφέρει ζημία περίπου 1,4 δισεκατομμύρια δολάρια ΗΠΑ στην ακαθάριστη προστιθέμενη αξία. (Baumann, 2022) (Baumann, 2022)

Η αρχιτεκτονική του GNSS αποτελείται από τρία τμήματα. Το διαστημικό τμήμα αποτελείται από δορυφόρους που βρίσκονται σε τροχιά περίπου 20,000 km πάνω από τη γη. Κάθε GNSS έχει τον δικό του «αστερισμό» δορυφόρων, διατεταγμένων σε τροχιές για να παρέχουν την επιθυμητή κάλυψη, εκπέμποντας ένα σήμα που αναγνωρίζει και παρέχει τον χρόνο, την τροχιά και την κατάστασή του. Τα θαλάσσια δίκτυα GNSS, που είναι ενσωματωμένα με δορυφορικούς αστερισμούς γεωστατικής τροχιάς (Geostationary Earth Orbit), είναι η σύνθεση δύο υποδικτύων, το παγκόσμιο σύστημα θέσης των ΗΠΑ (GPS) και το ρωσικό παγκόσμιο σύστημα δορυφορικής πλοήγησης (Global'naya Navigazionnaya Sputnikovaya Sistema - GLONASS). Και τα δύο αυτά δίκτυα «de facto πάσχουν από ορισμένες τεχνικές αδυναμίες», και λόγω αυτών, δεν μπορούν να χρησιμοποιηθούν ως το μόνο μέσο ναυσιπλοΐας για τα πλοία. Επιπρόσθετα, πολλές κυβερνήσεις και παγκόσμιοι οργανισμοί δεν θέλουν να εξαρτώνται ή να εμπιστεύονται τις υπηρεσίες GNSS που παρέχονται και ελέγχονται μόνο από δύο χώρες.

Ως εκ τούτου, προβλήθηκαν και αναπτύχθηκαν επαυξημένα δίκτυα των υποδομών όπως περιφερειακά δορυφορικά σύστημα αύξησης (Regional Satellite Augmentation System -RSAS) και μη (Satellite Based Augmentation System - SBAS) για να βελτιώσουν τις ελλείψεις των δύο υφιστάμενων στρατιωτικών λύσεων και να παρέχουν υψηλές επιχειρησιακές τιμές ακεραιότητας, συνέχειας, ακρίβειας και διαθεσιμότητας (Integrity, Continuity, Accuracy, Availability) για τις τρέχουσες μη στρατιωτικές απαιτήσεις στις θαλάσσιες μεταφορές. Αυτά που αναπτύχθηκαν λοιπόν είναι το ευρωπαϊκό σύστημα επικάλυψης γεωστατικής πλοήγησης (European Geostationary Navigation Overlay System - EGNOS), το ιαπωνικό δορυφορικό σύστημα ενίσχυσης MTSAT (MSAS) και το αμερικανικό σύστημα επέκτασης ευρείας περιοχής (WAAS), τα οποία είναι σε θέση να παρέχουν πληροφορίες επικοινωνιών, πλοήγησης και επιτήρησης (Communications, Navigations and Surveillance) από όλα τα πλοία, συμπεριλαμβανομένων άλλων κινητών, στα κέντρα ελέγχου κυκλοφορίας (Traffic Control Centers) ή στον έλεγχο κυκλοφορίας πλοίων (Ship Traffic Control) μέσω του διαστημικού σκάφους GEO. Τα παραπάνω δίκτυα **RSAS** είναι ενσωματωμένα διαλειτουργικά και συμβατά στοιχεία GSAS για την ενίσχυση των δικτύων GPS και GLONASS, περιλαμβάνοντας το EU Galileo και το κινεζικό BeiDou (πυξίδα).

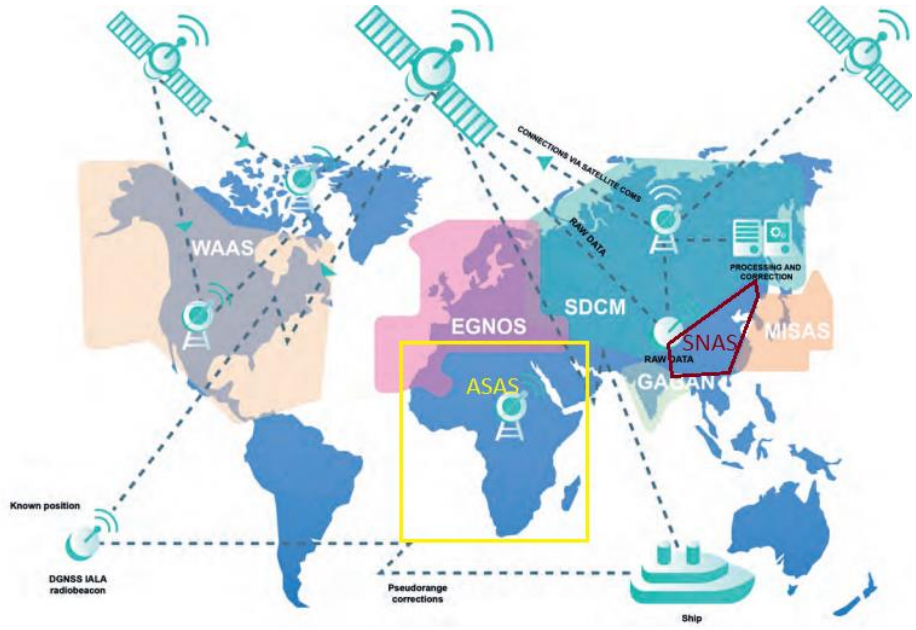
Εικόνα 22 - Τροχιά δορυφόρων GNSS. (HEXAGON, 2022)

Επιπλέον, τα δίκτυα GSAS ενσωματώνουν το δορυφορικό σύστημα πολιτικής πλοήγησης Inmarsat (Civil Navigation Satellite System -CNSO), την επαυξημένη πλοήγηση GNSS και GEOS

(GAGAN), το κινεζικό σύστημα δορυφορικής πλοήγησης (SNAS) και το ρωσικό σύστημα διαφορικής διόρθωσης και παρακολούθησης (System of Differential Correction And Monitoring - SDCM). Στο μεταξύ, προβλέπεται το αφρικανικό δορυφορικό σύστημα επαύξησης (ASAS). Επιπλέον, δύο ακόμη έργα των δικτύων RSAS πρέπει να ολοκληρωθούν και να καλύψουν όλες τις περιοχές της Αυστραλίας και της Νότιας Αμερικής η οποία υποδομή απεικονίζεται στο Σχήμα 1. (Ilcev, 2022)

Εν κατακλείδι, το παγκόσμιο δορυφορικό σύστημα πλοήγησης είναι ο γενικός όρος που αποτελείται από 4 δορυφορικά συστήματα με παγκόσμια κάλυψη και επιπλέον άλλα 2 περιφερειακά συστήματα τα όποια είναι τα εξής:

1. το GPS των ΗΠΑ: το οποίο εκτοξεύτηκε το 1970 και χρησιμοποιείται ένας αστερισμός από 27 δορυφόρους για να παρέχει παγκόσμια κάλυψη
2. το GLONASS της Ρωσίας: το οποίο αποτελείται από 24 δορυφόρους
3. το Galileo της Ευρωπαϊκής Ένωσης: το οποίο και αυτό αποτελείται από 27 δορυφόρους
4. το BeiDou της Κίνας: με 35 δορυφόρους να παρέχουν παγκόσμια κάλυψη
5. το Indian Regional Navigation Satellite System (IRNSS): ή αλλιώς γνωστό και ως NavIC (Navigation with Indian Conseltation) το οποίο παρέχει υπηρεσίες στην Ινδία καθώς και στις γύρω περιοχές και
6. το Quasi-Zenith Satellite System της Ιαπωνίας: το οποίο είναι περιφερειακά δορυφορικά συστήματα πλοήγησης παρέχοντας υπηρεσίες στην Ιαπωνία και στην περιοχή Ασίας – Ωκεανίας.



Εικόνα 23 - Satellite Based Augmentation System, Φωτογραφία από (Intertanko, 2022) και επεξεργασμένη σύμφωνα με το (Ilcev, 2022)

Ο δέκτης του GNSS καθορίζει τη θέση του στην επιφάνεια της γης χρησιμοποιώντας μια διαδικασία εν ονόματι trilateration, όπου η συσκευή μετρά την απόσταση του από την γνωστή θέση τριών δορυφόρων. Επειδή, όμως, οι δορυφόροι ταξιδεύουν με ταχύτητα 2,4 μιλίων ανά δευτερόλεπτο (4 χλμ. ανά δευτερόλεπτο), το trilateration σφάλμα μπορεί να είναι έως και ένα μίλι (1,6 χλμ.). Ο δέκτης πρέπει να επικοινωνήσει με έναν τέταρτο δορυφόρο για να διορθώσει την ώρα και να λάβει τον ακριβή χρόνο από τον οποίο θα καθοριστεί μια ακριβής επιδιόρθωση θέσης. Μια απόκλιση χρονισμού ενός νανοδευτερόλεπτου μπορεί να οδηγήσει σε σφάλμα θέσης ενός ποδιού (30 cm). Το GNSS μπορεί να είναι ακριβές σε περίπου 3 πόδια. Εκτός, όμως από αυτό, υπάρχουν και άλλοι παράγοντες που μπορούν να δημιουργούν μια δυσκολία στους δέκτες για τον υπολογισμό της ακριβής θέσης. Κάποια από αυτά είναι καθυστερήσεις στην Ιονόσφαιρα, λόγω της δραστηριότητας των ιόντων που μπορούν να προκαλέσουν απόκλιση τουλάχιστον 5

μέτρα, στην Τροπόσφαιρα, η οποία μπορεί να προκληθεί από τις αλλαγές που συμβαίνουν στην θερμοκρασία, στην ατμόσφαιρά κλπ.

Επιπλέον, πέρα από τα σφάλματα που μπορούν να προκληθούν στα GNSS σήματα, τα συστήματα αυτά μπορούν να πάσχουν και από διάφορες ευπάθειες. Πιο συγκεκριμένα:

i. παρεμβολές, καθώς τα σήματα ώσπου να φτάσουν στον δέκτη αποκτούν χαμηλό επίπεδο ισχύος και τα καθιστά ευαίσθητα από άλλα που μεταδίδονται στην εμβέλεια συχνοτήτων,
ii. πλαστογραφήσεις, όπου ένας εισβολέας εκπέμπει ένα σήμα με την ίδια δομή και συχνότητα με το σήμα GNSS, με την διαφορά ότι αυτό ελέγχει το επίπεδο ισχύος που εκπέμπεται, έτσι ώστε ο δέκτης θα κλειδώσει στο πλαστογραφημένο σήμα αντί στο πραγματικό. Στο πλαστό σήμα, το μήνυμα αλλάζει έτσι ώστε ο δέκτης να υπολογίσει μια λανθασμένη θέση ή ώρα.
iii. μπλοκαρίσματα σήματος, στην περίπτωση που η οπτική γωνία ενός δορυφόρου μπλοκαριστεί από εμπόδια όπως κτίρια, δέντρα, γέφυρες κ.λπ., ο δέκτης δεν είναι σε θέση να λάβει σήματα ως εκ τούτου να μην μπορεί να υπολογίσει τη θέση ή τον χρόνο του. ή
iv. αστοχίες αστερισμού, πράγμα εξαιρετικά απίθανο να συμβεί δηλαδή να αποτύχει ένας ολόκληρος αστερισμός. (HEXAGON, 2022)

Το δεύτερο τμήμα είναι το τμήμα ελέγχου που περιλαμβάνει ένα επίγειο δίκτυο βασικών σταθμών ελέγχου, σταθμούς αποστολής δεδομένων και σταθμούς παρακολούθησης. Σε κάθε σύστημα GNSS, ο σταθμός παρακολούθησης συνήθως εγκαθίσταται σε μια ευρεία γεωγραφική περιοχή, ελέγχει τα σήματα και την κατάσταση των δορυφόρων και αναμεταδίδει αυτές τις πληροφορίες στον κύριο σταθμό ελέγχου όπου αναλύει τα σήματα και στη συνέχεια μεταδίδει διορθώσεις τροχιάς και χρόνου στους δορυφόρους μέσω του σταθμού εκφόρτωσης δεδομένων όταν είναι απαραίτητο για τη διατήρηση της ακρίβειας. Τέλος, το τμήμα χρηστών αποτελείται από εξοπλισμό που επεξεργάζεται τα λαμβανόμενα σήματα και τα χρησιμοποιεί για την εξαγωγή και την εφαρμογή πληροφοριών τοποθεσίας και χρόνου. (HEXAGON, 2022) (HEXAGON, 2022)

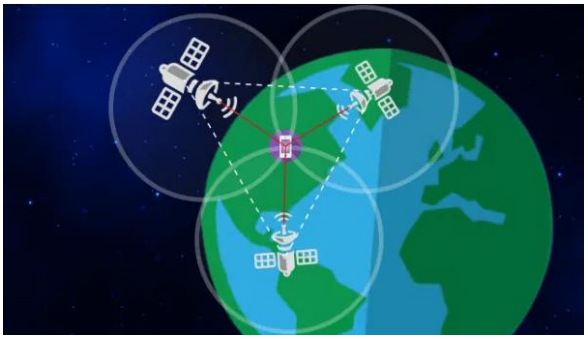
2.2.2 Global Positioning System

Το Παγκόσμιο Σύστημα Εντοπισμού Θέσης (GPS) έχει γίνει αναπόσπαστο κομμάτι του σύγχρονου κόσμου, καθώς η ικανότητα του να εντοπίζει ακριβείς συντεταγμένες τόσο ανθρώπων όσο και αντικειμένων εντάσσεται σε πολλούς τομείς, όπως οι μεταφορές, ο στρατός και η θάλασσα. Στη ναυτιλία διαδραματίζει ολοένα και πιο σημαντικό ρόλο καθώς χρησιμοποιείται σε ένα ευρύ φάσμα δραστηριοτήτων. Οι πληροφορίες του είναι ενσωματωμένες στο σύστημα αυτόματης αναγνώρισης (AIS), το οποίο έχει εγκριθεί από τον Διεθνή Ναυτιλιακό Οργανισμό, παρέχοντας στις κυβερνήσεις μεγαλύτερη επίγνωση της κατάστασης των εμπορικών πλοίων και του φορτίου τους.

Το GPS όπως έχει αναφερθεί αποτελεί ένα κομμάτι του GNSS και για αυτό έχουν πολλά κοινά όσον αφορά στις λειτουργίες τους αλλά και στην αρχιτεκτονική τους. Εν ολίγοις, διασφαλίζει την ασφαλή πλοήγηση (σε ωκεανούς αλλά και σε στενά περάσματα – εσωτερικές πλωτές οδούς). Διευκολύνει την αυτοματοποίηση της διαδικασίας παραλαβής, μεταφοράς και τοποθέτησης εμπορευματοκιβωτίων και έχει μειώσει το σχετικό λειτουργικό κόστος. Ενεργό ρόλο παίζει στις θαλάσσιες επιχειρήσεις έρευνας και διάσωσης, στην τοπογραφία, στην τοποθέτηση σημαδούρων και στην χαρτογράφηση κινδύνου πλοήγησης από τους ναυτικούς και ωκεανογράφους.

Άλλες χρηστικότητές του στον θαλάσσιο τομέα αφορούν την αλιεία. Πιο συγκεκριμένα, τα συστήματα εντοπισμού GPS εγκαθίστανται σε εμπορικά σκάφη για να διασφαλιστεί ότι δεν ψαρεύουν σε απαγορευμένες περιοχές ή περιόδους. Από την αντίθετη μεριά, βοηθά τους ψαράδες να εντοπίσουν τις τοποθεσίες ψαρέματος παρέχοντας τις ακριβείς συντεταγμένες. Τέλος, οι ερευνητές χρησιμοποιούν GPS που είναι τοποθετημένο σε ψάρια για να παρακολουθούν τις κινήσεις τους καθώς δείχνει τον ακριβή τόπο και την ώρα του ψαριού, προσδιορίζοντας έτσι την συμπεριφορά καθώς και το μεταναστευτικό πρότυπο των ψαριών που αποτελεί σημαντική πληροφορία για θαλάσσιες έρευνες. (Grind GIS, 2022)

Το GPS παρέχει την ταχύτερη και πιο ακριβή μέθοδο πλοήγησης για τους ναυτικούς. Τους διευκολύνει να μετρούν την ταχύτητα και να προσδιορίζουν την τοποθεσία. Είναι σημαντικό στη θαλάσσια ναυσιπλοΐα για τον αξιωματικό του πλοίου να γνωρίζει τη θέση του σκάφους. Ενώ βρίσκεται σε ανοιχτή θάλασσα, σε συμφορημένα λιμάνια και πλωτές οδούς, απαιτείται ακριβής θέση, ταχύτητα και κατεύθυνση για να διασφαλιστεί ότι το σκάφος φθάνει στον προορισμό του με τον ασφαλέστερο, οικονομικότερο και έγκαιρο τρόπο που επιτρέπουν οι συνθήκες. Η ανάγκη για ακριβείς πληροφορίες θέσης γίνεται ακόμη πιο κρίσιμη καθώς σχετίζεται με πολλούς από τους κινδύνους θαλάσσιων ατυχημάτων (GPS gov, 2022)



Εικόνα 24 - Διαδικασία τριπλοποίησης (trillateration) (ELECTRICALFUNABOLG, 2022)

Είναι ένα σύστημα εντοπισμού θέσης που βασίζεται σε ένα δίκτυο δορυφόρων που μεταδίδουν συνεχώς κωδικοποιημένες πληροφορίες μέσω ραδιοφωνικών σημάτων. Οι δέκτες ερμηνεύουν τις πληροφορίες που μεταδίδονται από τους δορυφόρους για να προσδιορίσουν με ακρίβεια τις τοποθεσίες στη γη. Αποτελείται από περίπου 29 δορυφόρους που βρίσκονται σχεδόν 20.000 km πάνω από την επιφάνεια της Γης, λειτουργεί σε όλες τις καιρικές συνθήκες και είναι σε μεγάλο βαθμό διαθέσιμο σε όλα τα μέρη του κόσμου, 24 ώρες την ημέρα. Το Υπουργείο Άμυνας των ΗΠΑ έθεσε σε λειτουργία τους δορυφόρους το 1978 για στρατιωτική χρήση, αλλά τους έκανε διαθέσιμους για πολιτική χρήση κατά τη δεκαετία του 1980, χωρίς όμως πλήρη πρόσβαση, με αυτή να αποκτάται περίπου το 2000 (ELECTRICALFUNABOLG, 2022).

Η διαφορά του με το GNSS είναι ότι η τεχνολογία GNSS λειτουργεί σε πολύ ευρύτερη κλίμακα (1559-1610 MHz), χρησιμοποιώντας σήματα από οποιονδήποτε δορυφόρο πλοήγησης, όχι μόνο από το GPS (1559-1591 MHz). Ένας δέκτης GNSS διαθέτει 60 δορυφόρους διαθέσιμους για προβολή, ενώ μια συσκευή χρειάζεται μόνο τρεις δορυφόρους για να προσδιορίσει τη θέση της. Με περισσότερα διαθέσιμα σήματα, η ακρίβεια και η αξιοπιστία των δεδομένων που λαμβάνονται αυξάνεται σημαντικά. Με απλά λόγια, όλοι οι δέκτες GNSS είναι συμβατοί με GPS, αλλά δεν είναι όλοι οι δέκτες GPS συμβατοί με GNSS (GeoTab, 2022).

Το GPS που χρησιμοποιείται στην τοπογραφία είναι πιο περίπλοκο από την τεχνολογία δορυφορικής πλοήγησης. Οι δέκτες GPS διαθέτουν κεραίες υψηλής ποιότητας και χρησιμοποιούν δύο συχνότητες για να δημιουργήσουν μια γραμμή βάσης. Τα δεδομένα συλλέγονται από τους ίδιους δορυφόρους ταυτόχρονα και αργότερα συγκρίνονται για να προσδιοριστεί η διαφορά στο γεωγραφικό πλάτος, μήκος και ύψος μεταξύ των δύο σημείων. Το πλεονέκτημα της τεχνολογίας GNSS στην τοπογραφία είναι η ελευθερία από τη χρήση φυσικών συσκευών. Χρησιμοποιώντας την τεχνολογία GNSS, οι επιθεωρητές δεν περιορίζονται από την οπτική επαφή καθώς μπορούν να τοποθετήσουν σταθμούς έρευνας οπουδήποτε με ανοιχτή θέα στον ουρανό και δεν χρειάζεται να βλέπουν ο ένας τον άλλον. (propeller, 2022)

Όπως και το GNSS έτσι και το υποσύνολο του έχει πιθανότητες αποτυχιών στα αποτελέσματα του. Τα ρολόγια στους δορυφόρους είναι πολύ ακριβή, αλλά δεν παύουν να μετατοπίζονται ελαφρά με αποτέλεσμα μικρά σφάλματα που επηρεάζουν την ακρίβεια. Αυτή η μετατόπιση μπορεί να είναι μικρή, αλλά σε καθημερινή βάση μπορεί να αποδειχθεί ότι είναι μεγαλύτερη. Επίσης, αυτό το σφάλμα είναι δύσκολο να εντοπιστεί επειδή η υπογραφή του μοιάζει με την τυπική σχετική κίνηση μεταξύ ενός δορυφόρου και του δέκτη. Το τμήμα ελέγχου παρακολουθεί συνεχώς τα δορυφορικά ρολόγια και διορθώνει τυχόν μετατοπίσεις που εντοπίζονται.

Ωστόσο, αυτές οι διορθώσεις βασίζονται σε παρατηρήσεις και ενδέχεται να μην υποδεικνύουν την τρέχουσα κατάσταση του ρολογιού, αφήνοντας υπολειπόμενο σφάλμα. Μερικές φορές, τα δορυφορικά ρολόγια συμπεριφέρονται απρόβλεπτα και παράγουν σφάλματα που αυξάνονται σημαντικά πριν οι χειριστές μπορέσουν να το εντοπίσουν και να το επισημάνουν ως ανθυγιεινό. Για παράδειγμα, την 1η Ιανουαρίου 2004, το ρολόι του δορυφόρου GPS SV-23 μετατοπίστηκε για περίπου 3 ώρες, οπότε το σφάλμα ψευδοεμβέλειας είχε αυξηθεί από 0 έως 285 χλμ..

Επίσης, με βάση μιας μελέτης, διαπιστώθηκε ότι η αύξηση του σφάλματος ρολογιού του δορυφόρου GPS προκάλεσε αύξηση του μέσου σφάλματος θέσης λόγω της αύξησης του σφάλματος στα δορυφορικά σήματα GPS, που οδήγησε σε αυξανόμενο σφάλμα στις συντεταγμένες που υπολογίζονται από τον δέκτη GPS. Αυτό οφείλεται στο ότι ο αστερισμός των δορυφόρων GPS είναι δυναμικός, προκαλώντας διαφορετική γεωμετρία του δορυφόρου σε σχέση με την τοποθεσία και τον χρόνο, με αποτέλεσμα η ακρίβεια του GPS να εξαρτάται από τη θέση/χρόνο. (Dinesh Sathyamoorthy, 2022)

Η απώλεια GPS δεν είναι απλώς θεωρητικό πρόβλημα. Μέσα σε λίγα δευτερόλεπτα θα αρχίσουν να ηχούν συναγερμοί καθώς ένα-ένα τα όργανα θα σταματούν να λειτουργούν. Η γυροσκοπική πυξίδα, το ραντάρ, η δυναμική τοποθέτηση παύουν να λαμβάνουν τη θέση του πλοίου. Η οθόνη του ηλεκτρονικού χάρτη δεν θα μπορεί να χρησιμοποιηθεί. Ακόμα και το ρολόι του πλοίου θα σταματήσει να λειτουργεί. Σε μια σειρά δοκιμών, μπορεί να αποδειχθεί ότι σχεδόν κάθε κομμάτι στο σκάφος χρησιμοποιεί GPS - ακόμη και το ενσωματωμένο δορυφορικό σύστημα ψυχαγωγίας.

Το σύστημα λειτουργεί χρησιμοποιώντας ένα στόλο δορυφόρων, αλλά το σήμα που μεταδίδουν είναι αδύναμο και μπορεί εύκολα να παρακαμφθεί. Αν ένας επιτιθέμενος, χρησιμοποιώντας λίγη ισχύ από έναν παρεμβολέα στη συχνότητα που χρησιμοποιεί το GPS κοντά στον δέκτη του πλοίου, μπορεί να τον ξεγελάσει με αποτέλεσμα να μην λαμβάνει τα σωστά σήματα. Για παράδειγμα, η εμπλοκή είναι ένα πραγματικό πρόβλημα στην Κορέα αφού έχουν υπάρξει πολλές περιπτώσεις που οι Βορειοκορεάτες έχουν μεταδώσει παρεμβολές υψηλής ισχύος στη Νότια Κορέα.

Επιπλέον, ο Ήλιος μπορεί επίσης να χτυπήσει δορυφορικά συστήματα εκτός σύνδεσης, και να δημιουργείται θόρυβος στα σήματα κατά τη διάρκεια ηλιακών καταιγίδων, τόσο έντονες που είτε κάνουν τις θέσεις του GPS να ταλαντεύονται ή προκαλούν απώλεια GPS σε ολόκληρη την ηλιόλουστη πλευρά της Γης. Σε περίπτωση αποτυχίας του GPS, ένας εξάντας καθώς και χάρτες είναι ιδανική λύση για αποφυγή τυχόν ατυχημάτων. Όλα τα πλοία που βασίζονται σε ηλεκτρονική πλοήγηση και GPS, ECDIS και AIS είναι επιρρεπή σε παρεμβολές ή επιθέσεις στον κυβερνοχώρο και όλα αυτά τα συστήματα μπορούν να χειραγωγηθούν από χάκερ και εγκληματίες. (Global, 2022)

2.2.3 Automatic Identification System

Το ναυτικό αυτόματο σύστημα αναγνώρισης (AIS) είναι ένα σύστημα ραδιοεπικοινωνιών μέσω του οποίου τα σκάφη μεταδίδουν συνεχώς την ταυτότητα και τη θέση τους σε δημόσια ραδιοκύματα χρησιμοποιώντας μη κρυπτογραφημένα ραδιοσήματα VHS. Λειτουργεί σε ακτίνα 10-20 ναυτικών μιλίων και παρέχει τη δυνατότητα στα σκάφη στη θάλασσα να γνωρίζουν το ένα την παρουσία του άλλου. Τα μηνύματα μεταδίδονται μέσω του αέρα και περιγράφονται στις συστάσεις της διεθνούς ένωσης τηλεπικοινωνιών, του τομέα ραδιοεπικοινωνιών (ITU-R) και βασίζονται στο NMEA 0138. Όταν αναπτύχθηκε πριν από σχεδόν 20 χρόνια, ο πρωταρχικός του σκοπός ήταν να αυξήσει την ασφάλεια στη θάλασσα.

Τα πλοία χρειάζονταν έναν καλύτερο τρόπο για να «βλέπουν» το ένα το άλλο και να αποφεύγουν τις συγκρούσεις. Αλλά οι αρχές χρειάζονταν επίσης έναν καλύτερο τρόπο αναγνώρισης σκαφών και παρακολούθησης της κυκλοφορίας στα ύδατά τους. Αυτό γιατί, στις Ηνωμένες Πολιτείες, στις 24 Μαρτίου 1989, το πετρελαιοφόρο Exxon Valdez προσάραξε στο Prince William Sound της Αλάσκας, και προκάλεσε την μεγαλύτερη καταστροφή πετρελαιοκηλίδας στην ιστορία των ΗΠΑ με έντεκα εκατομμύρια γαλόνια αργού πετρελαίου να ξεχύνονται στο νερό από το κομμένο κύτος Σε απάντηση, το Κογκρέσο των Ηνωμένων Πολιτειών ψήφισε τον Νόμο για τη Ρύπανση από Πετρέλαιο (Oil Pollution Act, OPA-90), μέρος του οποίου

ζητούσε από την Ακτοφυλακή να αναπτύξει ένα σύστημα παρακολούθησης πλοίων για δεξαμενόπλοια που πηγαίνουν στην Αλάσκα. Μέχρι τότε, οι πλοηγοί και οι σταθμοί της ξηράς εξαρτώνταν από την οπτική πλοήγηση, τα αναλογικά ραντάρ και τις φωνητικές επικοινωνίες για να μετριάσουν τις συγκρούσεις. Το νέο σύστημα έπρεπε να είναι αυτόνομο, συνεχές και ψηφιακό—κάτι που θα μπορούσε να επικοινωνεί αυτόματα και να απεικονίζει την τοποθεσία ενός πλοίου σε άλλα πλοία και στις Υπηρεσίες Κυκλοφορίας Πλοίων (Vessel Tracking Services) που εδρεύουν στην ξηρά χωρίς τον κίνδυνο ανθρώπινου λάθους.

Το Λιμενικό Σώμα αποφάσισε ένα σύστημα που χρησιμοποιούσε ραδιοκύματα VHF. Ταυτόχρονα, τα συστήματα παρακολούθησης αναπτύσσονταν και δοκιμάζονταν σε όλο τον κόσμο. «Οι Βρετανοί δοκίμαζαν ένα σύστημα παρακολούθησης βασισμένο σε VHS για πλοία που εισέρχονται και εξέρχονται από το Στενό του Ντόβερ», λέει ο Arroyo. «Η Επιτροπή της Διώρυγας του Παναμά δοκίμαζε ένα σύστημα UHF και οι Σουηδοί ανέπτυξαν ένα άλλο πρωτόκολλο». Στα μέσα της δεκαετίας του '90, η διεθνής κοινότητα συνειδητοποίησε ότι είχε νόημα να συνεργαστούν και ξεκίνησε ένα κίνημα στον Διεθνή Ναυτιλιακό Οργανισμό (IMO) και τη Διεθνή Ένωση Τηλεπικοινωνιών (ITU) για την υιοθέτηση ενός ενιαίου συστήματος που θα μπορούσε να χρησιμοποιηθεί παγκοσμίως. Αποφάσισαν για το σύστημα AIS που βασίζεται σε VHS που χρησιμοποιείται σήμερα. Οι τρεις κύριοι στόχοι του ήταν και είναι:

I. Αποφυγή σύγκρουσης
II. Υπηρεσία κυκλοφορίας σκαφών
III. Παράκτια επιτήρηση (Global Fishing Watch, 2022)

Οι αναμεταδότες συστημάτων αυτόματης αναγνώρισης (AIS) έχουν σχεδιαστεί για να μπορούν να παρέχουν αυτόματα τη θέση, την αναγνώριση και άλλες πληροφορίες σχετικά με το πλοίο σε άλλα πλοία και στις παράκτιες αρχές. Τα συστήματα αυτά αποτελούν μέρος του Παγκόσμιου Συστήματος Θαλάσσιου Κινδύνου και Ασφάλειας (GMDSS) και είναι υποχρεωτικά για όλα τα πλοία άνω των 300 GT[16] και για όλα τα επιβατηγά πλοία, ανεξαρτήτως μεγέθους. Τα πλοία που είναι εξοπλισμένα με AIS πρέπει να το διατηρούν συνεχώς σε λειτουργία ανά πάσα στιγμή, εκτός από τις περιπτώσεις όπου διεθνείς συμφωνίες, κανόνες ή πρότυπα προβλέπουν την προστασία των πληροφοριών ναυσιπλοΐας. Τα πρότυπα απόδοσης για το AIS υιοθετήθηκαν το 1998, και γενικά οι απαιτήσεις είναι η παροχή πληροφοριών από το πλοίο, η λήψη αυτών από παρόμοια εξοπλισμένα πλοία, η παρακολούθηση και ο εντοπισμός τους αλλά και ανταλλαγή των δεδομένων με εγκαταστάσεις της ξηράς. (IMO, 2022)

Τα δεδομένα AIS είναι διαθέσιμα σε όλα τα άλλα εξοπλισμένα πλοία, στα συστήματα κυκλοφορίας σκαφών (VTS), στις συμμετέχουσες υπηρεσίες με βάση την ακτή, συμπεριλαμβανομένων των ακτοφυλακών. Οι πληροφορίες μεταδίδονται για να προσδιορίσουν με σαφήνεια κάθε σκάφος εντός εμβέλειας, μαζί με τις ακόλουθες λεπτομέρειες: το όνομα του πλοίου, τον αριθμό που αποδόθηκε από τον Διεθνή Ναυτιλιακό Οργανισμό (IMO Number), το διακριτικό σήμα κλήσης (call sign)[17], το Maritime Mobile Service Identity (MMSI) [18], τη θέση, την ταχύτητα, την πορεία, τον ρυθμό στροφής, το επόμενο λιμάνι, την εκτιμώμενη ώρα άφιξης του σε αυτό και τα άτομα επί του πλοίου. Ορισμένες από τις πληροφορίες προέρχονται από άλλα συστήματα του πλοίου, ενώ άλλες καταχωρούνται χειροκίνητα.

[16] Ολική χωρητικότητα (gross register tonnage): Είναι ο συνολικός εσωτερικός όγκος όλων των μόνιμα σκεπαστών και κλειστών χώρων του πλοίου που βρίσκονται είτε κάτω από το ανώτατο κατάστρωμα είτε πάνω από αυτό, μετρούμενος σε κόρους. Στην ολική χωρητικότητα περιλαμβάνονται όλοι οι μονίμως κλειστοί χώροι που διατίθενται για φορτίο, εφόδια πλοίου και ενδιαίτηση πληρώματος - επιβατών. (Wikipedia, 2020)

[17] Τα ναυτικά σήματα κλήσης είναι σήματα κλήσης που εκχωρούνται ως μοναδικά αναγνωριστικά σε πλοία και σκάφη. Όλες οι ραδιοφωνικές μεταδόσεις πρέπει να αναγνωρίζονται ξεχωριστά από το σήμα κλήσης. (Wikipedia, 2020)

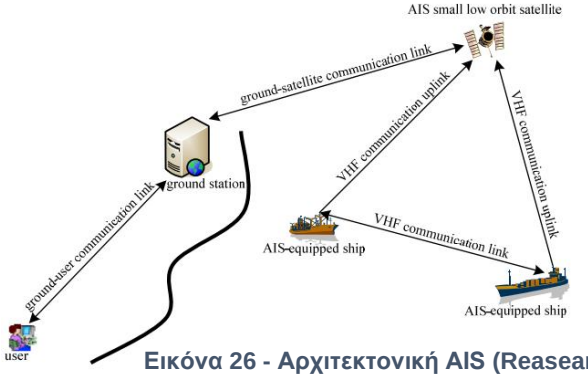
[18] Το Maritime Mobile Service Identity (MMSI) είναι μια σειρά εννέα ψηφίων τα οποία αποστέλλονται σε ψηφιακή μορφή μέσω ενός καναλιού ραδιοσυχνοτήτων, προκειμένου να εντοπίζονται με μοναδικό τρόπο σταθμοί πλοίων, σταθμοί επίγειων πλοίων, ακτοσταθμοί, σταθμοί ακτής εδάφους και ομαδικές κλήσεις. Αυτές οι ταυτότητες σχηματίζονται με τέτοιο τρόπο ώστε η ταυτότητα ή μέρος αυτής να μπορεί να χρησιμοποιηθεί από συνδρομητές τηλεφώνου και τέλεξ που είναι συνδεδεμένοι στο γενικό δίκτυο τηλεπικοινωνιών για να καλούν αυτόματα πλοία. (Wikipedia, 2020)

Εικόνα 25 - a) AIS950 Class A b) AIS350 Class B c) AIS350 Class C (RayMarine, 2022)

Υπάρχουν τριών ειδών – κλάσης τέτοια συστήματα. Είναι η κλάση Α, η οποία είναι για τα πλοία που υποχρεωτικά το έχουν, μεταδίδουν περισσότερες πληροφορίες και πιο συχνά. Η κλάση Β, η οποία είναι για τα πλοία που εθελοντικά εγκαθιστούν το σύστημα, δεν χρειάζεται κάποια χειροκίνητη ενημέρωση πληροφοριών καθώς εισάγονται με την εγκατάσταση και μεταδίδει τις πληροφορίες που παρέχονται από τα λοιπά συστήματα. Τόσο η Α όσο και Β μεταδίδουν και λαμβάνουν δεδομένα, ενώ η κλάση Γ μόνο λαμβάνει. (RayMarine, 2022) Τα δεδομένα που λαμβάνονται από αυτά τα συστήματα χρησιμοποιούνται για την εικονογράφηση – τοποθέτηση τους σε ειδικές οθόνες AIS, οθόνες ραντάρ και στο **Ηλεκτρονικό Σύστημα Οθόνης και Πληροφοριών Χάρτη (Electronic Chart Display and Information System)**. Η μετάδοση αυτής της στατικής και δυναμικής πληροφορίας συγχρονίζεται με το GPS με μεταδόσεις που πραγματοποιούνται σε συχνότητες VHF (161.975 MHz και 162.025 MHz, μέγιστη ισχύ TX 12.5w (Sea News, 2020).

Το AIS χρησιμοποιεί την τεχνολογία Self-Organizing Time Division Multiple Access (SOTDMA) για να επιτύχει υψηλό ρυθμό μετάδοσης και να εξασφαλίσει αξιόπιστη λειτουργία από πλοίο σε πλοίο. Αξίζει να σημειωθεί πως το σήμα που εκπέμπει το AIS για τα δυναμικά δεδομένα στέλνεται κάθε 2 με 10 δευτερόλεπτα όταν το πλοίο είναι εν κινήσει, και κάθε 3 λεπτά όταν αυτό βρίσκεται αγκυροβολημένο, ενώ για τα σταθερά δεδομένα κάθε 6 λεπτά ανεξαρτήτως κατάστασης. (Navipedia, 2022). Το σύστημα AIS που βασίζεται σε δορυφόρους αποτελείται από πέντε στοιχεία, δηλαδή από μικρούς δορυφόρους χαμηλής τροχιάς, από τον εξοπλισμό των πλοίων, από τους επίγειους σταθμούς, από τους χρήστες και τους συνδέσμους επικοινωνίας.

Ενώ οι πληροφορίες του πλοίου ανταλλάσσονται αυτόματα μεταξύ πλοίων μέσω VHF επικοινωνίας, ο δορυφόρος στον οποίο είναι εγκατεστημένος ο αναμεταδότης AIS μπορεί να λάβει το σήμα που μεταδίδεται από το ραδιοκύμα VHF. Ο δορυφόρος μεταφέρει το λαμβανόμενο σήμα στον επίγειο σταθμό που είναι υπεύθυνος για τον έλεγχο ολόκληρου του συστήματος, και στη συνέχεια, ο σταθμός μπορεί να διανείμει τις πληροφορίες του πλοίου στον εξουσιοδοτημένο χρήστη. Οι ζεύξεις επικοινωνίας μεταξύ του δορυφόρου και του σταθμού καθώς και μεταξύ του σταθμού και του χρήστη είναι αμφίδρομες, ενώ η σύνδεση επικοινωνίας από το πλοίο στον δορυφόρο είναι μονής κατεύθυνσης. Κατά συνέπεια, το AIS που βασίζεται σε δορυφόρους είναι σε θέση να παρακολουθεί σφαιρικά την κίνηση του πλοίου σε πραγματικό χρόνο, εάν ο αριθμός των δορυφόρων και των επίγειων σταθμών είναι ικανοποιητικός. (Reasearch Gate, 2022).



Εικόνα 26 - Αρχιτεκτονική AIS (Reasearch Gate, 2022)

Παρακάτω αναφέρονται οι απειλές που έχει αυτό το σύστημα από πλευράς τόσο λογισμικού όσο και υλικού (δηλαδή, ραδιοσυχνότητας [RF]). Πιο αναλυτικά:

Macrocategory	Threat	Software Based	RF Based
Spoofing	Ship spoofing	Yes	Yes
	AtoN spoofing	Yes	Yes
	SAR spoofing	Yes	Yes
	Closest point of approach (CPA) spoofing	No	Yes
	Distress beacon spoofing	No	Yes
	Faking weather forecasts	No	Yes
Hijacking	Hijacking	Yes	Yes
Availability disruption	Slot starvation	No	Yes
	Frequency hopping	No	Yes
	Timing attacks	No	Yes

Εικόνα 27 - Απειλές που σχετίζονται με το AIS (Wilhoit, 2022)

1. **CPA (Closest Point of Approach) Spoofing:** Το CPA λειτουργεί υπολογίζοντας την ελάχιστη απόσταση μεταξύ δύο πλοίων με τουλάχιστον ένα από αυτά να βρίσκεται εν κινήσει. Ρυθμίζεται ώστε να ενεργοποιεί μια ειδοποίηση όταν ανιχνεύεται μια πιθανή σύγκρουση, προκειμένου το πλοίο να αλλάξει πορεία. Η πλαστογράφηση CPA περιλαμβάνει την προσποίηση μιας πιθανής σύγκρουσης με ένα πλοίο-στόχο. Αυτό θα ενεργοποιήσει την ειδοποίηση, η οποία θα οδηγήσει το πλοίο εκτός πορείας για να αποφύγει την πρόσκρουση αλλά ταυτοχρόνως θα κατευθυνθεί σε βράχο ή θα προσαράξει κατά τη διάρκεια της άμπωτης.
2. **AIS-SART Spoofing:** Τα AIS-SART ενεργοποιούνται αυτόματα όταν έρχονται σε επαφή με το νερό και στέλνουν ραδιοφάρους κινδύνου, ακολουθούμενα από συντεταγμένες GPS, που βοηθούν τους διασώστες να εντοπίσουν τους επιζώντες. Η πλαστογράφηση του περιλαμβάνει τη δημιουργία ψευδών φάρων κινδύνου για ανθρώπους που έχουν πέσει στη θάλασσα σε ειδικά επιλεγμένες συντεταγμένες από τους επιτιθέμενους. Οι επιτιθέμενοι (π.χ. πειρατές) μπορούν να ενεργοποιήσουν ειδοποιήσεις SART για να παρασύρουν τα θύματα να κατευθυνθούν σε εχθρικούς θαλάσσιους χώρους. Αξίζει να σημειωθεί ότι βάσει νόμου, τα σκάφη υποχρεούνται να συμμετέχουν σε επιχειρήσεις διάσωσης όταν λαμβάνουν μηνύματα SAR. Η πλαστογράφηση των φάρων κινδύνου μπορεί να είναι ένα πρόσθετο εργαλείο πειρατείας.
3. **Faking Weather Forecasts:** Το AIS μεταδίδει επίσης δυναμικά δεδομένα για να αντικατοπτρίζει τις μεταβαλλόμενες συνθήκες περιβάλλοντος, όπως τα ρεύματα και τον καιρό. Χρησιμοποιεί μια ειδική μορφή μηνύματος—δυαδικό—για να μεταφέρει αυτού του είδους τις πληροφορίες. Η παραποίηση μετεωρολογικών προγνώσεων περιλαμβάνει την ανακοίνωση ψευδών ενημερώσεων. Για παράδειγμα, ενημερώνει για μια ηλιόλουστη μέρα, όταν στην πραγματικότητα αναμένεται καταιγίδα.
4. **Availability Disruption:** μπορεί να χωριστεί σε 3 κατηγόρίες. Η πρώτη είναι η **«πείνα στη θύρα» (slot starvation)** η οποία περιλαμβάνει την πλαστοπροσωπία των ναυτιλιακών αρχών για κράτηση ολόκληρου του «χώρου διευθύνσεων» μετάδοσης AIS, προκειμένου να αποτραπεί η επικοινωνία μεταξύ όλων των σταθμών εντός της κάλυψης. Δεύτερη είναι η **«αναπήδηση συχνότητας»** στην οποία οι επιτιθέμενοι υποδύονται τις ναυτικές αρχές για να δώσουν εντολή να αλλάξουν τις συχνότητες στις οποίες

λειτουργούν. Να σημειωθεί ότι οι αναμεταδότες κλάσης Β δεν μπορούν να ρυθμιστούν χειροκίνητα. Οι χρήστες δεν ειδοποιούνται καν για αλλαγές συχνότητας. Και τελευταία είναι η **«χρονική επίθεση»** η οποία μπορεί να επιφέρει δύο αποτελέσματα. Αφενός να εξαφανίσει πλοία, καθώς στέλνεται εντολή στους αναμεταδότες να καθυστερούν τους χρόνους μετάδοσης, και αφετέρου να υπερφορτώσει το σύστημα (πλημμυρίσει τη θαλάσσια κυκλοφορία) ζητώντας από τους σταθμούς να στέλνουν ενημερώσεις AIS πολύ συχνά.

5. **Ship Spoofing:** Η πλαστογράφηση πλοίων αναφέρεται στη διαδικασία κατασκευής ενός έγκυρου αλλά ανύπαρκτου πλοίου. Περιλαμβάνει την εκχώρηση στατικών και δυναμικών πληροφοριών στο πλασματικό πλοίο. Παρέχει στους επιτιθέμενους ένα ευρύ φάσμα κακόβουλων σεναρίων επίθεσης. Μπορούν να κάνουν τα πλοία να φαίνονται σαν να βρίσκονται εντός της δικαιοδοσίας ενός αντιπάλου κράτους ή να μεταφέρουν πυρηνικό φορτίο ενώ πλέουν στα ύδατα ενός έθνους χωρίς πυρηνικά. Επίσης, η επίθεση αυτή μπορεί να δημιουργήσει προβλήματα αναγνώρισης δεδομένων και εξαγωγής συμπερασμάτων. Παραδείγματος χάριν, ενώ θα μπορούσαν να ανιχνεύουν πλοία που χύνουν πετρέλαιο στην ανοιχτή θάλασσα ή να προβλέπουν θαλάσσιες συναλλαγές, η παραποίηση των πληροφοριών AIS μπορεί να ενοχοποιήσει άλλα πλοία.
6. **AtoN Spoofing:** Ένα **aid to navigation** (**ATON**) είναι οποιοδήποτε είδος σήματος, δείκτης ή εξοπλισμός καθοδήγησης που βοηθά τον ταξιδιώτη στην πλοήγηση. Οι συνήθεις τύποι τέτοιων βοηθημάτων περιλαμβάνουν φάρους, σημαδούρες, σήματα ομίχλης και φάρους ημέρας. (Wikipedia, 2022) Χρησιμοποιούνται για να βοηθήσουν στη διαχείριση της κυκλοφορίας των πλοίων κατά μήκος καναλιών ή λιμανιών ή να προειδοποιούν για κινδύνους, άμπωτες παλίρροιες, βραχώδεις εκβολές και προστατευμένες περιοχές στην ανοιχτή θάλασσα. Η πλαστογράφηση AtoN αναφέρεται στη διαδικασία δημιουργίας ψεύτικων πληροφοριών για να παρασυρθούν τα πλοία-στόχοι να κάνουν λάθος ελιγμούς. Οι επιτιθέμενοι μπορούν να τοποθετήσουν μία ή περισσότερες ψεύτικες σημαδούρες στην είσοδο του λιμανιού, για να παραβιάσουν την κυκλοφορία ή να εξαπατήσουν τα πλοία να πλοηγούν σε χαμηλά νερά.
7. **AIS Hijacking:** Η αεροπειρατεία AIS περιλαμβάνει την αλλαγή οποιασδήποτε πληροφορίας σχετικά με υπάρχοντες σταθμούς (π.χ. φορτίο, ταχύτητα, τοποθεσία και χώρα). Όσον αφορά το λογισμικό της αεροπειρατείας, οι εισβολείς μπορούν να κρυφακούν (MitM) σε συνεχείς επικοινωνίες και να αντικαθιστούν αυθαίρετα πληροφορίες. Στην έκδοση RF (radio frequency), οι εισβολείς μπορούν να παρακάμψουν τα αρχικά μηνύματα με ψεύτικα σήματα υψηλότερης ισχύος. Και στις δύο περιπτώσεις, οι παραλήπτες λαμβάνουν τροποποιημένες - από τον εισβολέα - εκδόσεις των αρχικών μηνυμάτων AIS. Οι επιτιθέμενοι μπορούν, για παράδειγμα, να «μετακινήσουν» στρατιωτικά πλοία εντός της δικαιοδοσίας των αντίπαλων εθνών, προκαλώντας πολιτικές εντάσεις.

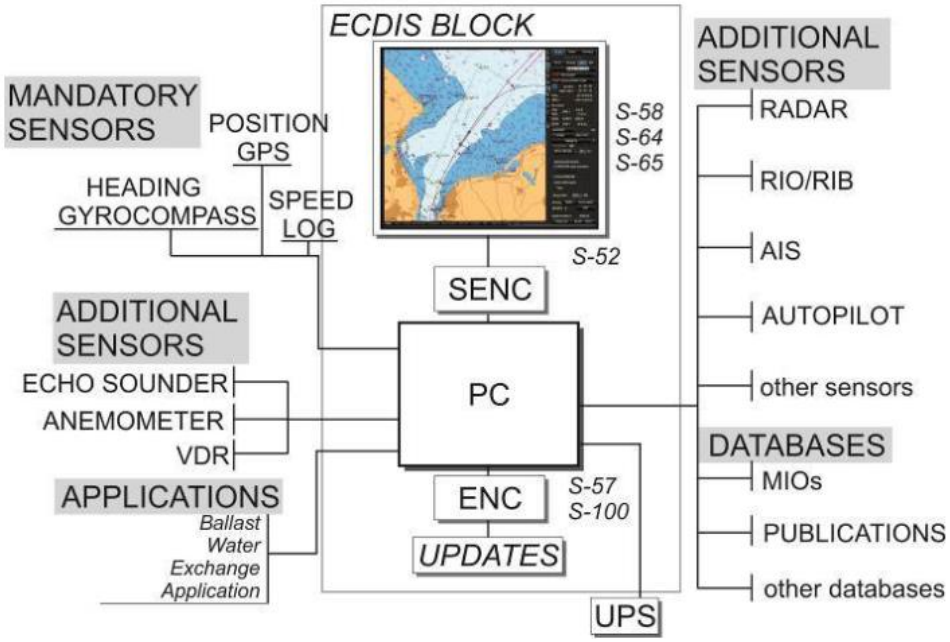
Μέχρι στιγμής επισημάνθηκαν επιθέσεις που γίνονται κατά κύριο λόγο στο υλικό (hardware) των εν λόγω συστημάτων. Όμως οι εγκαταστάσεις AIS χρειάζονται επίσης και λογισμικό για την παροχή δεδομένων σε διαδικτυακούς παρόχους (όπως για παράδειγμα MarineTraffic.com, AIS Hub, Vessel Finder). Οι υπηρεσίες αυτές αν και είναι πολύ χρήσιμες για την παρακολούθηση και την πλοήγηση, φέρουν και ζητήματα ασφάλειας. Λόγω της χαλαρής εφαρμογής των δεκτών AIS, οι διαδικτυακοί πάροχοι συχνά υποχρεούνται να αποδέχονται τα δεδομένα που λαμβάνουν, καθώς αντιπροσωπεύουν μια κοινοπραξία χρηστών που μοιράζεται πληροφορίες. Ως εκ τούτου δεν ελέγχουν εάν τα μηνύματα των πλοίων προέρχονται από τους πραγματικούς αποστολείς και δεν έχουν κανένα μέσο για τον έλεγχο ταυτότητας των αποστολέων προτάσεων AIVDM[19]. Τα παραπάνω θα μπορούσαν να επιτρέψουν στους εισβολείς να πραγματοποιήσουν πλαστογραφήσεις ή/ και επιθέσεις τύπου MitM. (Wilhoit, 2022)

[19] Το AIVDM/ AIVDO είναι ένα πρωτόκολλο δύο επιπέδων. Το εξωτερικό στρώμα είναι μια παραλλαγή του NMEA 0183, του προτύπου για την ανταλλαγή δεδομένων σε συστήματα θαλάσσιας πλοήγησης, και το AIS καθιστά αυτά τα δεδομένα διαθέσιμα για πλοήγηση, συστήματα κατά της σύγκρουσης και άλλες χρήσεις. (gpsd, 2022)

2.2.4 Electronic Chart Display and Information System – ECDIS

Το Ηλεκτρονικό Σύστημα Εμφάνισης και Πληροφοριών Χαρτών (ECDIS) είναι μια εξέλιξη στο σύστημα χαρτών πλοήγησης παρέχοντας πληροφορίες και γραφήματα που χρησιμοποιούνται σε ναυτικά σκάφη και πλοία. Με τη χρήση του συστήματος ηλεκτρονικών χαρτών, έχει γίνει ευκολότερο για το πλήρωμα να εντοπίζει τοποθεσίες και να επιτυγχάνει κατευθύνσεις. Το ECDIS χρησιμοποιεί τη δυνατότητα του Παγκόσμιου Συστήματος Εντοπισμού Θέσης (GPS). Έτσι, εντοπίζει με επιτυχία τα σημεία πλοήγησης και απεικονίζει την ακριβή τοποθεσία του πλοίου, αλλά και εμποδίων, φάρων σε πραγματικό χρόνο, βελτιώνοντας έτσι την ασφαλή πλοήγηση. Διευκολύνει σημαντικά τον φόρτο εργασίας του πλοηγού με τις αυτόματες δυνατότητές του, όπως ο σχεδιασμός και η παρακολούθηση διαδρομής, ο αυτόματος υπολογισμός ETA και η ενημέρωση των δεδομένων του Ηλεκτρονικού Χάρτη Πλοήγησης (ENC).

Επιπλέον, το ECDIS παρέχει πολλά άλλα εξελιγμένα χαρακτηριστικά πλοήγησης και ασφάλειας, συμπεριλαμβανομένης της συνεχούς καταγραφής δεδομένων για μεταγενέστερη ανάλυση. Είναι ένα σύστημα διασυνδεδεμένο με άλλα συστήματα πλοήγησης όπως το Gyrocompass, το RADAR, το σύστημα αυτόματης σχεδίασης (Automatic Radar Plotting Aid - ARPA), το Echo Sounder κ.λπ. Επίσης, ενσωματώνει και εμφανίζει πληροφορίες που περιέχονται σε άλλες ναυτικές εκδόσεις, όπως Πίνακες Παλίρροιας και Οδηγίες Ιστιοπλοΐας και πρόσθετες θαλάσσιες πληροφορίες όπως καιρικές συνθήκες, συνθήκες πάγου και αυτόματη αναγνώριση σκαφών.



Εικόνα 28 - Αρχιτεκτονική συστήματος ECDIS. (S.Žuškin, 2022)

Πρέπει επίσης να σημειωθεί ότι το ECDIS τηρεί τους όρους που θέτει ο Διεθνής Ναυτιλιακός Οργανισμός, και έτσι ενισχύει την αξιοπιστία του συστήματος ηλεκτρονικών χαρτών. Συμμορφώνεται με τον Κανονισμό V/19 & V/27 του IMO της σύμβασης SOLAS, που το καθιστά υποχρεωτικό για όλα τα επιβατηγά πλοία να το κατέχουν και να το χρησιμοποιούν, εμφανίζοντας επιλεγμένες πληροφορίες από έναν Ηλεκτρονικό Χάρτη Πλοήγησης Συστήματος (SENC). Ο εξοπλισμός ECDIS που συμμορφώνεται με τις απαιτήσεις της SOLAS μπορεί να χρησιμοποιηθεί ως εναλλακτική λύση των έντυπων χαρτών. Εκτός από τις γενικές απαιτήσεις για ραδιοεξοπλισμό στα πλοία, αποτελεί μέρος του GMDSS και για ηλεκτρονικά βοηθήματα πλοήγησης που περιλαμβάνονται στο ψήφισμα A.694 του IMO.

Το ECDIS έχει 2 τύπους διαγραμμάτων. Πρώτα το διάγραμμα Raster (RNC): Το RNC είναι ένα άμεσο αντίγραφο ή μια σάρωση των χάρτινων διαγραμμάτων. Μοιάζει πανομοιότυπο με ένα

χάρτινο διάγραμμα, καθώς όλες οι πληροφορίες που εμφανίζονται εκτυπώνονται απευθείας. Δεύτερον, το Electronic Navigational Chart (ENC), το όποιο είναι γραφήματα που δημιουργούνται από υπολογιστή. Οι πληροφορίες σε ένα ENC μπορούν να ενεργοποιηθούν και να απενεργοποιηθούν ανάλογα με τις απαιτήσεις του χρήστη. Για παράδειγμα, ο χρήστης μπορεί να επιλέξει να φαίνονται τα βάθη για να ληφθούν προειδοποιήσεις. Σχετικά με τις προειδοποιήσεις, το ECDIS σημαίνει συναγερμούς και/ή ενδείξεις, όταν για παράδειγμα υπάρχει υπέρβαση ορίων cross-track, απόκλιση από τη διαδρομή, προσέγγιση κρίσιμου σημείου ή περιοχής με ειδικές συνθήκες κ.α. (Bhattacharjee, What is Electronic Chart Display and Information System (ECDIS)?, 2022). (Ghamdi, 2022)

Το ECDIS εκτελείται συνήθως σε υπολογιστή με Microsoft Windows XP και έχει εγγενείς ευπάθειες που το καθιστούν ευάλωτο σε επιθέσεις στον κυβερνοχώρο. Έχει αναφερθεί τον Γενάρη του 2014 από μια έρευνα ότι ένας εισβολέας μπορεί να έχει πρόσβαση και να τροποποιεί αρχεία και γραφήματα του συστήματος (ECDIS) (COMMITTEE, 2022). Ενώ κάθε προϊόν ECDIS είναι διαφορετικό, η κίνηση που παρατηρείται υποδηλώνει ότι αρκετές πλατφόρμες ECDIS που χρησιμοποιούνται συνήθως είναι ευάλωτες ως αποτέλεσμα της διαρροής πληροφοριών μέσω θαλάσσιων δικτύων VSAT (Very small aperture terminal).

Σε αρκετές περιπτώσεις, ενημερώσεις διαγραμμάτων ECDIS μεταδόθηκαν μέσω μη κρυπτογραφημένου πρωτοκόλλου ηλεκτρονικού ταχυδρομείου POP3. Σε πολλές από αυτές τις περιπτώσεις, τα αρχεία που ονομάστηκαν κατάλληλα και στάλθηκαν στα σωστά εισερχόμενα POP3 και για αυτό έγινε αυτόματη λήψη και χρήση από το στοχευμένο ECDIS. Ειδάλλως, οι ενημερώσεις πρέπει να αντιγράφονται χειροκίνητα από ένα μέλος του πληρώματος σε μια εξωτερική συσκευή αποθήκευσης από τα εισερχόμενα email - συχνά σε τακτικά προγραμματισμένη βάση. Επίσης υπάρχουν και αρκετές περιπτώσεις στις οποίες τα γραφήματα ECDIS ενημερώθηκαν μέσω μη ασφαλών συνδέσεων FTP με ή HTTP API. Αν κάποιος εισβολέας υποβάλει κακόβουλα τροποποιημένα αρχεία μέσω οποιουδήποτε από αυτούς τους μηχανισμούς ενημέρωσης, θα μπορούσε να αλλάξει τους ναυτικούς χάρτες που χρησιμοποιούνται για την πλοήγηση στο σκάφος του θύματος. (Pavur, Moser, Strohmeier, Lenders, & Martinovic, 2022)

Σε μια δοκιμή διείσδυσης, οι εμπειρογνώμονες ηθικής πειρατείας του Naval Dome απέδειξαν πόσο ευάλωτα είναι στην πραγματικότητα τα ραντάρ και άλλα συστήματα γεφυρών. Κατά τη διάρκεια μιας αρχικής έρευνας, το Naval Dome έστειλε ένα email γεμάτο με ιούς μέσω της δορυφορικής σύνδεσης του πλοίου στον υπολογιστή του καπετάνιου, ο οποίος συνδεόταν τακτικά με το ECDIS για ενημερώσεις χάρτη. Στην επόμενη ενημέρωση γραφήματος, ο ιός μεταφέρθηκε στο ECDIS όπου εγκαταστάθηκε αμέσως και άρχισε να λειτουργεί αλλάζοντας τη θέση του σκάφους κατά τη διάρκεια ενός νυχτερινού ταξιδιού, εξαπατώντας τον αξιωματικό φρουράς. Οι κρίσιμες παράμετροι που αφορούν τη θέση, την κατεύθυνση, το βάθος και την ταχύτητα του σκάφους χειραγωγήθηκαν αρκετά διακριτικά ώστε να μην κινήσουν υποψίες. Εάν αδίστακτα άτομα βρίσκονταν πίσω από μια παρόμοια επίθεση, θα μπορούσαν εύκολα να είχαν προσαράξει το σκάφος, να είχαν προκαλέσει σύγκρουση ή να παρακρατούσαν το πλοίο για λύτρα. (Wingrove, ‘Impregnable’ radar breached in simulated cyber attack, 2022)

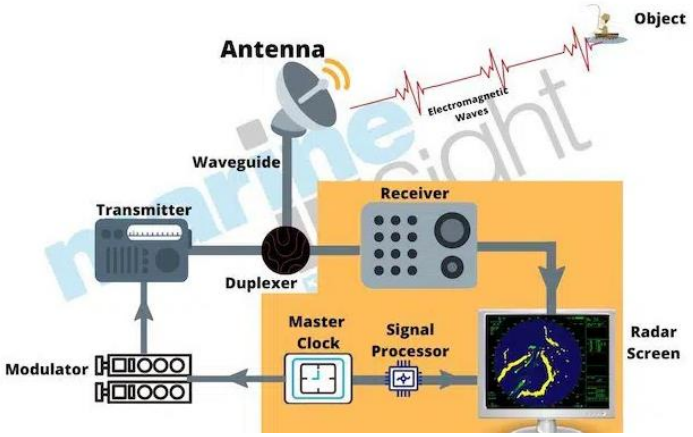
Το σύστημα διαχείρισης επικοινωνίας και πλοήγησης που βασίζεται στο ECDIS θα επέτρεπε σε έναν κυβερνοεγκληματία να έχει πρόσβαση, να διαβάσει, να κατεβάσει, να αντικαταστήσει ή να διαγράψει οποιοδήποτε αρχείο είναι αποθηκευμένο στο μηχάνημα, καθώς και να τροποποιήσει ή να διαγράψει τα περιεχόμενα των αρχείων και των χαρτών στο πλοίο ή στην ξηρά. Μόλις αποκτηθεί μια τέτοια μη εξουσιοδοτημένη πρόσβαση, οι επιτιθέμενοι θα μπορούσαν να αλληλοεπιδράσουν με το σταθμό εργασίας ή τους διακομιστές των δικτύων του πλοίου και της ξηράς. Αυτό θα μπορούσε να έχει ως αποτέλεσμα σοβαρά οικονομικά και περιβαλλοντολογικά ζητήματα. Εάν το ECDIS βρίσκεται σε λειτουργία «ελέγχου τροχιάς» όπου κατευθύνει τον αυτόματο πιλότο, τότε ο χάκερ μπορεί να το ξεγελάσει και να κάνει το πλοίο να αλλάξει κατεύθυνση. Η επίθεση θα μπορούσε να γίνει μέσω θυρών USB/CD, λήψης αρχείων από το Διαδίκτυο και από email (Mednikarov, Tsonev, & Lazarov, 2022).

2.2.5 Radar

Το ραντάρ θαλάσσης είναι εξοπλισμός που χρησιμοποιείται στη γέφυρα του πλοίου από τον αξιωματικό βάρδιας για τη διεξαγωγή ασφαλούς παρακολούθησης πλοήγησης. Είναι ένα υποχρεωτικό βοήθημα στη ναυσιπλοΐα, που χρησιμοποιείται για την παρακολούθηση (με ενσωματωμένο Automatic Radar Plotting Aids - ARPA) και τον εντοπισμό σκαφών (συμπεριλαμβανομένου του δικού του σκάφους). Το radar έχει διάφορες εγγενείς λειτουργίες, όπως είναι τα CPA και TCPA[20], EBL και VRM[21] κ.λπ., με τη χρήση των οποίων τα ατυχήματα μπορούν να αποφευχθούν. Το ραντάρ του πλοίου έχει μια οθόνη (αναφέρεται ως δείκτης θέσης σχεδίου) που εμφανίζει όλους τους στόχους που υπάρχουν εντός της εμβέλειάς του. Δεδομένου ότι όλα τα αντικείμενα είναι ορατά στην οθόνη, η πλοήγηση και η παρακολούθηση της θέσης του πλοίου γίνεται πραγματικά εφικτή. Η ακτοφυλακή, η VTS και οι άλλες αρχές μπορούν να χρησιμοποιήσουν τα δεδομένα ακόμη και από τα ελλιμενισμένα πλοία για να παρακολουθούν την κυκλοφορία στη μικρή εμβέλεια ραντάρ.

Οι συσκευές παρακολούθησης πλοίων είναι υποχρεωτικές σύμφωνα με το COLREGS (Διεθνείς Κανονισμοί για την Πρόληψη Συγκρούσεων στη Θάλασσα). Το Κεφάλαιο V του Κανονισμού 19 της SOLAS ορίζει ότι «Όλα τα πλοία ολικής χωρητικότητας 3000 τόνων και άνω διαθέτουν ραντάρ 3 GHz ή, όπου κρίνεται σκόπιμο από την Αρχή, δεύτερο ραντάρ 9 GHz ή άλλα μέσα για τον προσδιορισμό και την εμφάνιση της εμβέλειας και της διόπτευσης άλλων επιφανειακών σκαφών, εμποδίων, σημαδούρων, ακτογραμμών και σημάτων ναυσιπλοΐας που βοηθούν στην πλοήγηση και στην αποφυγή σύγκρουσης.»

Το θαλάσσιο ραντάρ ταξινομείται στις συχνότητες της ζώνης X (10 GHz), που χρησιμοποιείται για πιο ευκρινή εικόνα και καλύτερη ανάλυση, ή της ζώνης S (3 GHz) που χρησιμοποιείται ειδικά σε βροχή ή ομίχλη. Ένα από τα κύρια χαρακτηριστικά του είναι η παραβολική κεραία που εκπέμπει και λαμβάνει ηλεκτρομαγνητικά κύματα. Το θαλάσσιο ραντάρ λειτουργεί με βάση τη βασική αρχή των ηλεκτρομαγνητικών κυμάτων. Η κεραία του ραντάρ στέλνει τα ηλεκτρομαγνητικά κύματα υψηλής ταχύτητας για να εντοπίσει τη θέση, που καθορίζεται από την απόσταση, την ταχύτητα και την κατεύθυνση που ταξίδεψε το κύμα μαζί με το ύψος του αντικειμένου, κινούμενο ή ακίνητο.



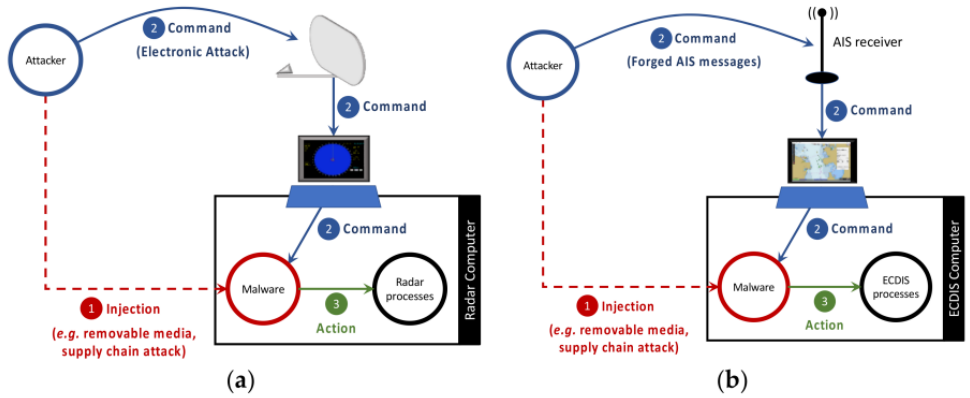
Εικόνα 29 - Τα βασικά στοιχεία του RADAR. (Bhattacharjee, Marine Radars and Their Use in the Shipping Industry, 2022)

[20] Πλησιέστερο σημείο προσέγγισης (Closest Point of Approach) και Χρόνος στο πλησιέστερο σημείο προσέγγισης (Time to Closest Point of Approach) είναι δύο μεταβλητές που ρυθμίζονται από τον χρήστη του συστήματος για το πότε θα ενεργοποιηθεί ο συναγερμός για το ποια είναι η πιο κοντινή επιτρεπτή προσέγγιση από άλλα πλοία / αντικείμενα και ποιος είναι ο χρόνος απόκρισης για να ληφθούν μέτρα αποφυγής. (Digital Yacht, 2022)

[21] Ο μεταβλητός μετρητής αποστάσεων (Variable Range Marker-VRM) και η ηλεκτρονική γραμμή διόπτευσης (Electronic Bearing Line-EBL) μετρούν την απόσταση και τη διόπτευση από το σκάφος σας μέχρι το αντικείμενο στόχου. Στην οθόνη ραντάρ, το VRM εμφανίζεται ως κύκλος με επίκεντρο την παρούσα θέση του σκάφους σας και το EBL εμφανίζεται ως γραμμή που ξεκινά στην παρούσα θέση του σκάφους σας και τέμνει το VRM. Το σημείο τομής είναι ο στόχος του VRM και του EBL. (Garmin, 2022)

Η θέση του αντικειμένου προσδιορίζεται καθώς η κεραία περιστρέφεται συνεχώς πάνω από το πλοίο στέλνοντας και λαμβάνοντας σήματα γύρω από το πλοίο. Η απόσταση από το πλοίο καθορίζεται από το λαμβανόμενο σήμα που αποστέλλεται πίσω στη μονάδα υπολογιστή όπου γίνονται οι υπολογισμοί σύμφωνα με τον χρόνο ανάκλασης. Μόλις ο υπολογιστής μάθει την ώρα, θα υπολογίσει την απόσταση χρησιμοποιώντας τον τύπο ταχύτητας και χρόνου. Εάν δεν υπάρχουν αντικείμενα προς την κατεύθυνση του κύματος, η οθόνη του ραντάρ θα μείνει κενή. Η συχνότητα και ο χρόνος που χρειάζονται τα κύματα για να επιστρέψουν (αντανακλάσεις) στον δέκτη ραντάρ του πλοίου, ορίζουν εάν η διαδρομή του σκάφους μπορεί να συνεχιστεί ή όχι. (Bhattacharjee, Marine Radars and Their Use in the Shipping Industry, 2022)

Ένα είδος επίθεσης στο ραντάρ είναι η χρήση bots, δηλαδή ένα πρόγραμμα που λειτουργεί αυτόματα περιμένοντας τους χάκερ να στείλουν εντολές για να εκτελέσουν χωρίς να το γνωρίζει ο χρήστης. Ο εισβολέας εγχέει το κακόβουλο λογισμικό στο σύστημα στόχο εκμεταλλευόμενος ευπάθειες με αφαιρούμενα μέσα ή ακόμη και μέσω της εφοδιαστικής αλυσίδας. Το bot αναμένει μέχρι να ληφθεί μια αναγνωριστική εντολή και τότε ενεργοποιείται το στάδιο δράσης όπου το κακόβουλο λογισμικό χειρίζεται τις υπολογιστικές διαδικασίες ραντάρ ή ECDIS. Παραδείγματα πιθανών επιβλαβών ενεργειών που εκτελούνται στο στοχευμένο σύστημα είναι η επαναφορά του συστήματος, η εγγραφή και η επανάληψη σεναρίων, το πάγωμα της οθόνης του συστήματος κ.λπ.. (Junior, Moraes, Albuquerque, Machado, & Sá, 2022)



Εικόνα 30 - Μοντέλο επίθεσης σε σύστημα a) Radar, b) AIS/ECDIS (Junior, Moraes, Albuquerque, Machado, & Sá, 2022)

Επιπρόσθετα, οι εμπειρογνώμονες ηθικής πειρατείας του Naval Dome πραγματοποίησαν μια επίθεση στο σύστημα radar του σκάφους. Χρησιμοποίησαν την τοπική διεπαφή μεταγωγέα Ethernet που συνδέει το ραντάρ με το ECDIS, με το σύστημα καταγραφής δεδομένων ταξιδιού και με το σύστημα ειδοποίησης γέφυρας για να εισέλθουν με επιτυχία στο σταθμό εργασίας του ραντάρ. Μετά από αυτό, κατάφεραν να διαγράψουν στόχους ραντάρ από την οθόνη της γέφυρας του σκάφους, κλείνοντας ουσιαστικά τα μάτια του πλοίου. Εκτός της αφαίρεσης στόχων, θα μπορούσαν επίσης να δημιουργήσουν πολλαπλούς ψευδείς στόχους, με διαφορετικά εύρη, εντός του εύρους ανίχνευσης, με σκοπό να παράγουν πολλαπλούς κατασκευασμένους στόχους, ώστε να μην είναι εφικτός ο διαχωρισμός μεταξύ πραγματικών και ψευδών στόχων.

Και αυτή η επίθεση ολοκληρώθηκε χωρίς να δημιουργήσει υποψία στον αξιωματικό. Η οθόνη του συστήματος έδειξε ότι το ραντάρ λειτουργεί σωστά, συμπεριλαμβανομένων των ορίων ανίχνευσης, τα οποία παρουσιάστηκαν ως απολύτως φυσιολογικά καθ' όλη τη διάρκεια της επίθεσης. Η πιθανή απώλεια ζωών και η περιβαλλοντική ζημιά που θα μπορούσε να επέλθει εάν επρόκειτο για κακοπροαίρετους χάκερ που είχαν τον έλεγχο αντί για ηθικούς θα ήταν ανυπολόγιστες. (Wingrove, ‘Impregnable’ radar breached in simulated cyber attack, 2022)

2.3 Συστήματα επικοινωνίας

Τα συστήματα επικοινωνιών στα πλοία χρησιμοποιούνται για γενικούς επιχειρηματικούς σκοπούς αλλά και για την ασφάλεια της ζωής στη θάλασσα (SOLAS[22]) καθώς και για τον αποτελεσματικό συντονισμό **αναζήτησης και διάσωσης (SAR)**. Αξίζει να σημειωθεί ότι για περίπου 90 χρόνια, η έμφαση στα πλοία που βρίσκονται σε κίνδυνο ήταν να επικοινωνήσουν με τα κοντινά πλοία για βοήθεια. Παλαιότερα η επικοινωνία μεταξύ πλοίων αλλά και πλοίων με την ξηρά γινόταν με τα σήματα Morse που στέλνονται από τον ασυρματιστή, ο οποίος έπρεπε να βρίσκεται 24 ώρες το 24ώρο πάνω από το σύστημα. Ο κώδικας Morse είναι ένα αξιόπιστο σύστημα που χρησιμοποιήθηκε στη θάλασσα για σχεδόν 100 χρόνια (η χρήση του Morse διακόπηκε το 1999). Στη δεκαετία του εβδομήντα, ο IMO εισήγαγε ένα σύστημα όπου η επικοινωνία γινόταν πιο αυτοματοποιημένα.

Μεταξύ 1992 και 1999, εισήχθη ένα νέο σύστημα επικοινωνιών, το λεγόμενο **Παγκόσμιο Σύστημα Κινδύνου και Ασφάλειας στη Θάλασσα (GMDSS)**. Σύμφωνα με αυτό, τα πλοία που βρίσκονται σε κίνδυνο έρχονται σε επαφή με τις εγκαταστάσεις έρευνας και διάσωσης της ξηράς για τον συντονισμό. Το GMDSS, ως υβριδικό σύστημα, **χρησιμοποιεί δορυφορικές και επίγειες επικοινωνίες**. Έχει χωρίσει την γη σε τέσσερις επιμέρους περιοχές (A1, A2, A3, A4). Οι εξοπλισμοί που χρησιμοποιούνται είναι οι VHF, Ψηφιακή Επιλεκτική Κλήση (DSC) η οποία μέσω ψηφιακών εντολών μεταδίδει ή λαμβάνει σήματα κινδύνου, επείγοντα, ασφαλείας, μηνύματα ρουτίνας ή προτεραιότητας, NAVTEX, ραδιοεπικοινωνίες (MF, HF εμβέλεια, υψηλών συχνοτήτων ή INMARSAT που παρέχει αμφίδρομη επικοινωνία) και MSI (Πληροφορίες Ναυτιλιακής Ασφάλειας) (E-nautilia, 2022).

Ο θαλάσσιος ηλεκτρικός και ηλεκτρονικός εξοπλισμός πρέπει να λειτουργεί ακόμα και στο πιο εχθρικό περιβάλλον λόγω των δονήσεων, των διακυμάνσεων της θερμοκρασίας, της υγρασίας και της ατμόσφαιρας (που είναι στα αλάτια). Πρέπει να ληφθούν υπόψη τα μέσα διασφάλισης διαθεσιμότητας εξοπλισμού. Μια τυπική εγκατάσταση επικοινωνιών σε πλοίο συμβατό με SOLAS, στις μέρες μας, περιέχει τουλάχιστον τα ακόλουθα:

I. Πομποδέκτης Πολύ Υψηλής Συχνότητας (**VHF**) (156-171 Mhz) + Ψηφιακή Επιλεκτική Κλήση (DSC) για την έναρξη ειδοποιήσεων κινδύνου και την παροχή γενικών επικοινωνιών (οπτικό πεδίο / 30-60 μίλια).

II. Πομποδέκτης Medium Wave (**MF**) + **DSC** (2 MHz) για ειδοποιήσεις και γενικές επικοινωνίες με εύρος περίπου 600-800 μίλια.

III. Πομπός υψηλής συχνότητας (**HF**) + **DSC** (4 - 16 MHz) για παγκόσμια ειδοποίηση κινδύνου και για γενικές επικοινωνίες.

IV. **Emergency Position Indicating Radio Beacon (EPIRB)** (406 MHz) Αυτός ο φάρος που χρησιμοποιείται αυτόματα ή χειροκίνητα, όταν χρησιμοποιείται σε συνδυασμό με δορυφόρους χαμηλής γείωσης (LEO), δορυφόρους (**CosPas** / **Sarsat**), πληροφορεί για την θέση κινδύνου και παρέχει ταυτοποίηση σκάφους σε απόσταση 5 χιλιομέτρων παγκοσμίως.

V. **Search and Rescue Radar Transponder (SART)** (ζώνη X, 9,3-9,5 GHz) είναι μια συσκευή φιλοξενίας που επιτρέπει στα πλοία και τα αεροσκάφη SAR να εντοπίζουν με ακρίβεια μια θέση κινδύνου χρησιμοποιώντας ραντάρ ζώνης X[23].

---

[22] Η Σύμβαση SOLAS στις διαδοχικές της μορφές θεωρείται γενικά ως η σημαντικότερη από όλες τις διεθνείς συνθήκες που αφορούν την ασφάλεια των εμπορικών πλοίων. Η πρώτη έκδοση υιοθετήθηκε το 1914, σε απάντηση στην καταστροφή του Τιτανικού. (IMO, 2022) Η σύμβαση για την ασφάλεια της ζωής στη θάλασσα (αγγλικά: Safety of Life at Sea) είναι μία διεθνής ναυτιλιακή σύμβαση που ορίζει τα ελάχιστα πρότυπα ασφαλείας για την κατασκευή, τον εξοπλισμό και τη λειτουργία των εμπορικών πλοίων. Η σύμβαση απαιτεί από όσα κράτη την έχουν υπογράψει, τα πλοία που φέρουν την σημαία τους να τηρούν αυτά τα ελάχιστα πρότυπα. (wikipedia, 2022)

[23] Η ζώνη X το εύρος συχνοτήτων στη μηχανική ραντάρ , καθορίζεται από το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE) στα 8,0-12,0 GHz. Η ζώνη X χρησιμοποιείται για ραντάρ, δορυφορική επικοινωνία και ασύρματα δίκτυα υπολογιστών . Τα μικρότερα μήκη κύματος της ζώνης X επιτρέπουν εικόνες υψηλότερης ανάλυσης από ραντάρ απεικόνισης υψηλής ανάλυσης για αναγνώριση και διάκριση στόχου. (Wikipedia, 2020)

VI. **Navtex** (518 KHz) (εύρος 800 μιλίων) για τη λήψη ειδοποιήσεων, μετεωρολογικών προβλέψεων και πληροφοριών για την ασφάλεια στη θάλασσα σχετικά με τους κινδύνους ναυσιπλοΐας και τα εμπόδια που ενδέχεται να αντιμετωπίσει το πλοίο κατά τη διέλευση.

VII. **Satcom C** (**Inmarsat**) για προειδοποίηση κινδύνου και μετάδοση και λήψη πληροφοριών ασφάλειας στη θάλασσα μέσω ενισχυμένης ομαδικής κλήσης (EGC). Το Sat C μπορεί επίσης να χρησιμοποιηθεί για γενικές επικοινωνίες και αυτόματη δήλωση θέσης.

VIII. Τα **Inmarsat Sat B, M και mini M** είναι μερικά από αυτά τα συστήματα που υποστηρίζουν ειδοποίηση κινδύνου και ανταλλαγή μηνυμάτων χρησιμοποιώντας φωνή ή τέλεξ. Τα συστήματα επιτρέπουν επίσης τη μεταφορά δεδομένων και υποστηρίζουν ακόμη και αργή σάρωση TV (Sea News, 2020).

Επίσης, το **Iridium** είναι ένα άλλο σύστημα δορυφορικής επικοινωνίας και προσφέρει τηλεφωνική κάλυψη και ανταλλαγή δεδομένων σε οποιοδήποτε μέρος του πλανήτη, ακόμα και στον Βόρειο και Νότιο πόλο. Αλλά και το **Ku Band VSAT** είναι μία ιδιαίτερη μορφή δορυφορικής επικοινωνίας που επιτρέπει την αξιόπιστη μετάδοση δεδομένων μέσω δορυφόρου, παρέχοντας «υψηλές» ταχύτητες και απεριόριστο όγκο δεδομένων, αλλά μειονεκτώντας στην γεωγραφική κάλυψη η οποία είναι μικρότερη από τα προηγούμενα.

Αξιοσημείωτο είναι ότι το διαδίκτυο στα πλοία εγκαταστάθηκε πολύ αργότερα καθώς το κόστος ήταν αυξημένο. Τον Φεβρουάριο του 2006 στην Γενεύη της Ελβετίας εγκρίθηκε η Διεθνής Σύμβαση Εργασίας (ΔΣΕ), που διασφαλίζει μια πιο αξιοπρεπή ζωή αλλά και συνθήκες εργασίας στους ναυτικούς. Πιο συγκεκριμένα, στο κανονισμό 4.10, που αφορά στις συνθήκες ενδιαίτησης επί του πλοίου, στη γενική οδηγία B3.1.11 αναφέρεται ότι πρέπει να ληφθεί υπόψη η ύπαρξη σύνδεσης στο διαδίκτυο χωρίς κάποια οικονομική επιβάρυνση για το ναυτικό, όπου αυτό είναι εφικτό (International Labour Conference, 2022). Βέβαια, και η απόσταση από την ξηρά παίζει σημαντικό ρόλο στην αποστολή και λήψη σημάτων για αυτό και είναι αναγκαία η χρήση γεωστατικών δορυφόρων (Η χρήση και η αξιοποίηση του Διαδικτύου και των εφαρμογών του στη σύγχρονη Εμπορική Ναυτιλία, 2017) .

Τα τελευταία 20 χρόνια στα πρότυπα θαλάσσιας επικοινωνίας εντάσσεται το **Controller Area Network (CAN)** που αναπτύχθηκε στις αρχές της δεκαετίας του 1980. Το πρότυπο CAN είναι ένας δίαυλος εκπομπής όπου οποιαδήποτε συσκευή μπορεί να εκπέμψει όταν είναι έτοιμη και δεν χρειάζεται να περιμένει για να τραβηχτεί από κάποιον κύριο σταθμό. Τα Ναυτιλιακά σκάφη το χρησιμοποιούν **για διασύνδεση εξοπλισμού** όπως αισθητήρες ταχύτητας ανέμου/κατεύθυνσης ανέμου/θερμοκρασίας αέρα, Αυτόματη Σύστημα Αναγνώρισης (AIS), Παγκόσμιο Δορυφορικό Σύστημα Πλοήγησης (GNSS), γυροσκόπιο, πυξίδα, οθόνη πλοήγησης, μεγάλη ποικιλία αισθητήρων κατάστασης πλοίου, συσκευή εγγραφής δεδομένων ταξιδιού (VDR) και οθόνη ταμπλό κατάστασης πλοίου.

Η προδιαγραφή CAN χρησιμοποιεί έναν δίαυλο εκπομπής έτσι ώστε όλες οι συσκευές να ακούν όλες τις εκπομπές. Είναι ουσιαστικά ένα ίσο προς ίσιο δίκτυο. Όταν περισσότεροι από ένας σταθμοί είναι έτοιμοι για μετάδοση, επιλύουν τη σύγκρουση μέσω μιας διαδικασίας γνωστής ως **διαιτησίας**, η οποία είναι κάπως παρόμοια με το Carrier Sense, Multiple Access with Collision Detection (CSMA/CD)[24]. Το πρότυπο διαύλου CAN ορίζει ένα φυσικό επίπεδο και μια μορφή πλαισίου για την ανταλλαγή δεδομένων. Η πραγματική μορφή των δεδομένων καθορίζεται σε πρωτόκολλα υψηλότερου επιπέδου για συγκεκριμένες εφαρμογές και συσκευές. Η μορφή για τα μηνύματα υψηλότερου επιπέδου περιγράφεται στις προδιαγραφές αριθμού ομάδας παραμέτρων

[24] Η πολλαπλή πρόσβαση με αίσθηση φέροντος με ανίχνευση σύγκρουσης (CSMA/CD) είναι μια μέθοδος ελέγχου πρόσβασης μέσου (MAC) που χρησιμοποιείται κυρίως στην πρώιμη τεχνολογία Ethernet για τοπική δικτύωση . Χρησιμοποιεί ανίχνευση φορέα για να αναβάλλει τις μεταδόσεις έως ότου δεν εκπέμπουν άλλοι σταθμοί. Αυτό χρησιμοποιείται σε συνδυασμό με την ανίχνευση σύγκρουσης στην οποία ένας σταθμός εκπομπής ανιχνεύει συγκρούσεις ανιχνεύοντας εκπομπές από άλλους σταθμούς ενώ εκπέμπει ένα πλαίσιο . Όταν εντοπιστεί αυτή η συνθήκη σύγκρουσης, ο σταθμός σταματά να μεταδίδει αυτό το πλαίσιο, μεταδίδει ένα σήμα εμπλοκής και στη συνέχεια περιμένει για ένα τυχαίο χρονικό διάστημα πριν προσπαθήσει να στείλει ξανά το πλαίσιο. (Carrier sense multiple access with collision detection, 2022)

(Parameter Group Number). Ένα PGN ορίζει τη λειτουργία ενός μηνύματος, τη μορφή του πεδίου διαιτησίας διαύλου CAN και τη μορφή των περιεχομένων.

Το πρότυπο **NMEA 2000**[25] **(National Marine Electronics Association - N2K)** έχει σχεδιαστεί για επικοινωνία μεταξύ ηλεκτρονικών θαλάσσιων ειδών σε ένα σκάφος και χρησιμοποιεί τον δίαυλο CAN ως φυσικό επίπεδο. Τα προηγούμενα πρότυπα θαλάσσιας επικοινωνίας χρησιμοποιούσαν συνδέσεις σημείου προς σημείο μεταξύ κάθε συσκευής και ενός κεντρικού ελεγκτή, ενώ ο δίαυλος CAN χρησιμοποιεί έναν ενιαίο δίαυλο επικοινωνίας με τον οποίο διασυνδέονται πολλές συσκευές. Η χρήση του διαύλου CAN αποδίδει ένα πολύ απλούστερο σχήμα καλωδίωσης που απαιτεί λιγότερο συνολικό καλώδιο με αποτέλεσμα αισθητή μείωση στο κόστος εγκατάστασης και συντήρησης, καθώς και χαμηλότερο συνολικό βάρος του συστήματος. Τα μηνύματα N2K υποδηλώνονται με το όνομά τους και το PGN.

Τα τελευταία 15 χρόνια έχουν δημοσιευτεί έγγραφα, που παράλληλα με συνέδρια hacking έχουν καταδείξει επιθέσεις σχετικά με την ασφάλεια στον κυβερνοχώρο για το CAN bus. Καλό είναι να σημειωθεί ότι ορισμένα από τα σενάρια που περιγράφονται παρακάτω είναι αδύνατα με έναν διαύλου CAN που λειτουργεί σωστά ή μια πιστοποιημένη συσκευή NMEA 2000, αλλά μπορεί να είναι αρκετά πιθανά εάν κατασκευαστεί μια αδίστακτη συσκευή ειδικά για να παραβιάζει αυτά τα πρότυπα.

Τόσο ο δίαυλος CAN όσο και το πρότυπο NMEA 2000 παρέχουν έναν μηχανισμό για την αποστολή μηνύματος που απευθύνεται σε συγκεκριμένο δέκτη. Βελτιστοποιούν το εύρος ζώνης του δικτύου στέλνοντας ένα μήνυμα διεύθυνσης επειδή δεν χρειάζονται απάντηση από όλες τις συσκευές. Μια σωστά διαμορφωμένη συσκευή CAN δεν θα «ακούει» ένα μήνυμα διεύθυνσης εάν δεν είναι ο επιδιωκόμενος δέκτης, ενώ θα μπορούσε να σχεδιαστεί για να λειτουργεί σε ακατάλληλη λειτουργία και να ακούει κάθε μετάδοση. Ομοίως, και η πλειονότητα των NMEA 2000.

Ένας κακόβουλος χρήστης θα μπορούσε να έχει εγκαταστήσει έναν κόμβο ώστε να διαβάσει όλα τα PGN. Σε φυσικό επίπεδο, είναι δυνατή η προσθήκη μιας τέτοιας συσκευής, καθώς είναι απλό να προστεθεί κρυφά, αφού ένα πλοίο μπορεί να έχει αρκετές εκατοντάδες συσκευές. Μια αδίστακτη συσκευή σε ένα δίαυλο CAN, μπορεί να γίνει με την χρήση ενός μικρού μήκους καλωδίου, ένα βύσμα Τ για την σύνδεση του με την συσκευή και ενός πάνελ πρόσβασης στο πλοίο. Έτσι, μπορεί να έχει πρόσβαση και, πιθανώς, να διεισδύσει σε πληροφορίες από το δίκτυο ενός σκάφους, για παράδειγμα, μπορεί να παρακολουθήσει όλες ή ένα επιλεγμένο υποσύνολο μεταδόσεων στο δίαυλο επικοινωνιών ή μπορεί να αποθηκεύσει τις πληροφορίες για μεταγενέστερη ανάκτηση ή να μεταδώσει τις πληροφορίες σε άλλο σύστημα εντός ή εκτός του σκάφους σε πραγματικό χρόνο. Με τα παραπάνω θίγεται η **εμπιστευτικότητα** καθώς δεν υπάρχει το απόρρητο των πληροφοριών μεταξύ αποστολέα και παραλήπτη.

Επιπλέον, ένα άλλο σενάριο με την προσθήκη μια τέτοιας συσκευής είναι η έγχυση πλαισίου δηλαδή να στέλνεις ψεύτικα μηνύματα. Για παράδειγμα, μια συσκευή στο δίκτυο θα μπορούσε να στείλει ψεύτικα μηνύματα NMEA 2000 που μεταμφιέζονται ως δέκτης GPS, πυξίδα ή μετρητής βάθους, προκαλώντας την τροφοδοσία ψευδών πληροφοριών στην κονσόλα πλοήγησης. Τα πρότυπα NMEA 2000 και ο δίαυλος CAN δεν παρέχουν χρονική σήμανση στο σώμα του μηνύματος, επομένως δεν παρέχουν ακεραιότητα χρονισμού, και δεν μπορεί να εξασφαλιστεί ότι τα μεταδιδόμενα δεδομένα είναι σωστά. Σε μια επίθεση επανάληψης ένα νόμιμο μήνυμα αποθηκεύεται και αναμεταδίδεται αργότερα από μια αδίστακτη συσκευή. Για παράδειγμα, κατά τη διάρκεια μιας ακραίας άμπωτης σε ένα στενό κανάλι, ένας εισβολέας θα μπορούσε να αναπαράγει πληροφορίες για το μετρητή βάθους από μια προηγούμενη ακραία παλίρροια, γεγονός που πιθανόν να προκαλέσει την προσάραξη ενός πλοίου.

Μια άλλη επίθεση μπορεί να προκύψει από την αποστολή πλαστών bits, αναγκάζοντας σφάλματα μετάδοσης. Επειδή η ακεραιότητα bit που παρέχεται στον δίαυλο CAN γίνεται με την χρήση υπολογισμού CRC[26], ένας επαρκής αριθμός τέτοιων σφαλμάτων bit θα μπορούσε να κάνει

[25] Ένα άρθρο που περιγράφει την αρχιτεκτονική του NMEA μπορείτε να το βρείτε στον ακόλουθο σύνδεσμο: (NMEA Communication Standard for Shipboard Data Architecture, 2022)

[26] Ο κυκλικός έλεγχος πλεονασμού (CRC) είναι ένας κωδικός ανίχνευσης σφαλμάτων που χρησιμοποιείται συνήθως σε ψηφιακά δίκτυα και συσκευές αποθήκευσης για τον εντοπισμό τυχαίων αλλαγών στα ψηφιακά δεδομένα. Τα μπλοκ

άλλες συσκευές να πιστεύουν ότι ο δίαυλος επικοινωνίας είναι αναξιόπιστος. Ένα PGN πολλαπλών πλαισίων NMEA 2000 αποστέλλεται σε πολλαπλά πλαίσια διαύλου CAN, αλλά δεν υπάρχει μηχανισμός που να διασφαλίζει την ακεραιότητα bit ολόκληρου του μηνύματος PGN. Μια ακόμη επίθεση θα μπορούσε να συμβεί εάν μια τέτοια συσκευή χρησιμοποιεί την ίδια διεύθυνση με έναν άλλο κόμβο, οπότε θα ήταν αδύνατο για τους δέκτες να διακρίνουν τους διαφορετικούς πομπούς. Τα παραπάνω θίγουν την **ακεραιότητα** του συστήματος, καθώς δεν είναι σίγουρο εάν το ληφθέν μήνυμα είναι το ίδιο με αυτό που μεταδόθηκε από τον αποστολέα.

Λόγω της ίδιας διεύθυνσης που χρησιμοποιεί αυτή η κακόβουλη συσκευή και της ταυτόχρονης εκπομπής προκύπτει το θέμα της διαιτησίας. Η μετάδοση μετά την απώλεια της διαιτησίας αποτελεί άμεση παραβίαση του πρωτοκόλλου διαύλου CAN. Αυτό μπορεί να προκαλέσει το σφάλμα μετάδοσης καθώς θα έχει ερμηνευτεί έτσι από έναν δέκτη που ανιχνεύει μια κατάσταση διαφορετική από τη μετάδοσή του. Αυτό τελικά θα αναγκάσει τη συσκευή να εισέλθει σε κατάσταση «Απενεργοποίησης» και να απομακρυνθεί από το δίκτυο.

Η κατάσταση «Απενεργοποίησης» επιλύεται με επανεκκίνηση της συσκευής, του ελεγκτή διαύλου της συσκευής ή, σε ακραίες περιπτώσεις, ολόκληρου του δικτύου διαύλου CAN. Ένας άλλος τρόπος για να μπει μία συσκευή σε αυτήν την κατάσταση είναι εάν μία ή περισσότερες συσκευές λειτουργούν με διαφορετικούς ρυθμούς μετάδοσης. Το NMEA 2000 απαιτεί οι συσκευές να λειτουργούν στα 250 kbps. Εάν μια αδίστακτη συσκευή τοποθετηθεί στο δίκτυο και λειτουργεί επίμονα με διαφορετική ταχύτητα, ορισμένες ή όλες οι άλλες συσκευές εκπομπής θα εισέρχονταν τελικά σε κατάσταση «Απενεργοποίησης».

Αυτό μπορεί να οδηγήσει σε περιττές επαναφορές δικτύου ή συσκευών, προκαλώντας μια σειρά από διακοπές δικτύου. Ένας κακόβουλος κόμβος μπορεί επίσης να στείλει ψευδή μηνύματα RTS (Request To Send) και να υπερχειλίσει το buffer εισόδου του δέκτη ή να στείλει ψευδή μηνύματα CTS (Clear To Send) για να κρατήσει μια σύνδεση ανοιχτή και να σφετεριστεί ολόκληρο το εύρος ζώνης του δικτύου. Όλα αυτά καθιστούν μια συσκευή ή ολόκληρο το δίκτυο απρόσιτα χρησιμοποιώντας όλη τη διαθέσιμη μνήμη της συσκευής ή το εύρος ζώνης του δικτύου από πλαστά αιτήματα για εξυπηρέτηση, με την **διαθεσιμότητα** των πληροφοριών να πλήττεται. (Kessler G. , The CAN Bus in the Maritime Environment – Technical Overview and Cybersecurity Vulnerabilities, 2022)

2.4 Άλλα συστήματα – ελέγχου, μηχανής, έρευνας

2.4.1 Συστήματα ελέγχου μηχανής

Το τμήμα μηχανών ενός πλοίου αποτελείται γενικά από δύο βασικούς τομείς: το μηχανοστάσιο (**Engine Room - ER**) και το δωμάτιο ελέγχου κινητήρα (**Engine Control Room - ECR**). Το τμήμα μηχανών στο σύνολό του είναι ένα περιβάλλον με δυσμενείς εργασιακές συνθήκες. Για παράδειγμα στο ER που είναι μια κλειστή περιοχή εντός του κύτους ενός πλοίου, αυτές είναι οι: θερμοκρασία, υγρασία, θόρυβος, δονήσεις και επικίνδυνες ουσίες. Το πλήρωμα του κινητήρα είναι υπεύθυνο για τη λειτουργία, την παρακολούθηση, την αντιμετώπιση προβλημάτων και τη συντήρηση διαφόρων συστημάτων, ενώ το μεγαλύτερο μέρος του χρόνου εργασίας τους κατανέμεται μεταξύ του ER και του ECR (Mallam & Lundh, 2022).

Το μηχανοστάσιο περιέχει διάφορους αναγκαίους αλλά και σύνθετους εξοπλισμούς και συστήματα για την πρόωση πλοίων, την παραγωγή ενέργειας και άλλες απαραίτητες λειτουργίες.

δεδομένων που εισάγονται σε αυτά τα συστήματα λαμβάνουν μια σύντομη τιμή ελέγχου, με βάση το υπόλοιπο μιας πολυωνυμικής διαίρεσης του περιεχομένου τους. Κατά την ανάκτηση, ο υπολογισμός επαναλαμβάνεται και, σε περίπτωση που οι τιμές ελέγχου δεν ταιριάζουν, μπορούν να ληφθούν διορθωτικά μέτρα κατά της καταστροφής δεδομένων. Τα CRC μπορούν να χρησιμοποιηθούν για διόρθωση σφαλμάτων. Τα CRC είναι δημοφιλή επειδή είναι απλά στην εφαρμογή τους σε δυαδικό υλικό, είναι εύκολο να αναλυθούν μαθηματικά και ιδιαίτερα καλά στην ανίχνευση κοινών σφαλμάτων που προκαλούνται από το θόρυβο στα κανάλια μετάδοσης. Επειδή η τιμή ελέγχου έχει σταθερό μήκος, η συνάρτηση που τη δημιουργεί χρησιμοποιείται περιστασιακά ως συνάρτηση κατακερματισμού. (Cyclic redundancy check, 2022)

Επίσης διαθέτει κύριες και βοηθητικές μηχανές, σύστημα ψύξης νερού, λιπαντικού, καυσίμου, αποχέτευσης, υδροσυλλεκτών, έρματος, συστήματα πεπιεσμένου αέρα, πόσιμου νερού, λέβητα και πυρόσβεσης. (Man, Lundh, & MacKinnon, 2022). Το ECR είναι σημαντικό για το τμήμα κινητήρα ως κέντρο πληροφοριών. Συλλέγει δεδομένα σχετικά με το πηδάλιο και την προπέλα και ρυθμίζει την ταχύτητα του σκάφους. Επίσης, ελέγχει την κατανάλωση των καυσίμων, τις στάθμες του νερού καθώς και την κατάσταση της μηχανής. Ένα μεγάλο μέρος των καθηκόντων αφιερώνεται πλέον στην εξ αποστάσεως διαχείριση του προαναφερθέντος εξοπλισμού.

Το ECR επί του σκάφους κατά τη διάρκεια των τελευταίων δεκαετιών εξελίσσεται συνεχώς προς την κατεύθυνση της μηχανογράφησης και του αυτοματισμού. Ο ανάλογος εξοπλισμός αντικαθίσταται, σε πολλές περιπτώσεις, από ψηφιακές διεπαφές σε υπολογιστές, γεγονός που δημιουργεί διαφορετικό χώρο εργασίας. Αυτό, που έχει μηχανογραφηθεί από την άποψη των οργάνων, είναι το σύστημα συναγερμού, πυρανίχνευσης, διαχωρισμού και παρακολούθησης της στάθμης της δεξαμενής. Ωστόσο, οι αντλίες, οι εναλλαγές δεξαμενών, οι ανεμιστήρες κ.λπ. παραμένουν αποκλειστικές λειτουργίες ενσύρματου ελέγχου . (Wagner, Lundh, & Grundevik, 2022).

Ψηφιακά συστήματα εποπτείας με περισσότερη τεχνητή νοημοσύνη και ταχύτερη απόκριση έχουν εισαχθεί για να αντικαταστήσουν ανάλογο εξοπλισμό, προκύπτοντας νέοι τύποι καθηκόντων παρακολούθησης και ελέγχου για τους χειριστές ECR. Όλες αυτές οι αλλαγές συμβάλλουν στη μείωση του αριθμού των μελών του πληρώματος, ενώ παράλληλα επιφέρουν σημαντική αύξηση του φόρτου εργασίας για το υπόλοιπο πλήρωμα χωρίς να επηρεάζουν πολύ την ιεραρχική οργανωτική δομή.

Η εργασία στο τμήμα μηχανών έχει αλλάξει από τις πιο κλασικές εργασίες χειρισμού κινητήρα και μηχανημάτων σε όλο το μηχανοστάσιο σε πιο διοικητικό τύπο εργασίας. Με νέους περιβαλλοντικούς κανονισμούς και βελτιστοποιήσεις μεγέθους πληρώματος, εκτός από τα καθήκοντα παρακολούθησης και ελέγχου κινητήρα, προστέθηκε σημαντικός όγκος διοικητικής – γραφειοκρατικής εργασίας με την καταγραφή των μεταφορών λαδιών, συμβάντων βιοαπόρριψης, εργασίες έρματος κ.λπ. προγραμματισμός συντήρησης, τεκμηρίωση ανεφοδιασμού καυσίμων και άλλα. (ANDERSSON & LINSE, 2022)

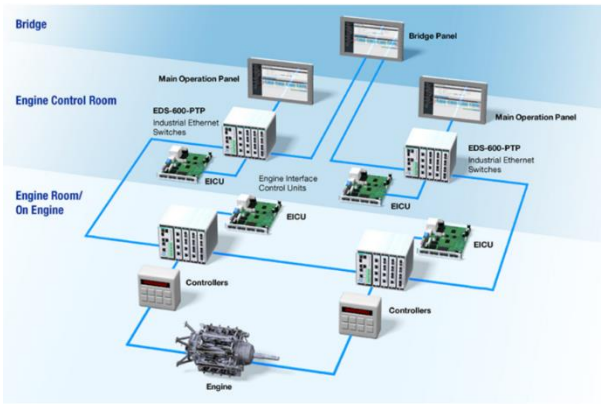
Εικόνα 31 - Ένα ECR σε ένα μεγάλο σύγχρονο κρουαζιερόπλοιο. (Man, Lundh, & MacKinnon, 2022)

Η πραγματική κατάσταση εργασίας στα ECR είναι απαιτητική. Όταν ενεργοποιείται ένας κρίσιμος συναγερμός, οι μηχανικοί πρέπει να παρουσιαστούν στο ECR και να αναπτύξουν γρήγορα επίγνωση της κατάστασης. Οι υψηλοί βαθμοί κόπωσης και άγχους μειώνουν την παραγωγικότητα και οδηγούν σε υψηλότερο κίνδυνο για να γίνουν λάθη. Αυτό που το κάνει ακόμη πιο επιρρεπές σε σφάλματα είναι ότι υπάρχουν γεμάτες οθόνες και χειριστήρια, μια πληθώρα ψηφιακών συστημάτων. Η διαφοροποίηση μεταξύ των παλαιών σχεδίων και της νέας τεχνολογίας

θέτει σε κίνδυνο την απόδοση του πληρώματος και την ασφάλεια του πλοίου. (Mallam & Lundh, 2022)

Από διάφορες άλλες έρευνες έχουν ειπωθεί πως η κατακερματισμένη δομή ψηφιακών πληροφοριών μπορεί να αυξήσει την ευπάθεια και τους λειτουργικούς κινδύνους σε κρίσιμες στιγμές στο ECR. Οι χειριστές μπορούν να αισθάνονται ότι πνίγονται στις διάσπαρτες πληροφορίες. Η γνωστική υπερφόρτωση συμβάλει στον να εμποδίσουν τον ανθρώπινο παράγοντα να παρατηρήσει το περιβάλλον που αλλάζει και να φιλτράρει τις απαραίτητες πληροφορίες. Αυτό μπορεί να οδηγήσει σε παρερμηνείες και να προκύψουν ανθρώπινα λάθη που μπορεί να αποβούν καταστροφικά (Man, Lundh, & MacKinnon, 2022).

Στη σειρά EDS-600 της Moxa είναι ενσωματωμένα τα συστήματα ελέγχου κινητήρα (Engine Control System – ECS), παρέχοντας συνδεσιμότητα με υψηλό εύρος ζώνης για την ενσωμάτωση διαφόρων υποσυστημάτων και εφαρμογών όπως χειριστήρια για την εκκίνηση των βαλβίδων αέρα, τις ακολουθίες εκκίνησης, τις λειτουργίες ρύθμισης, χειριστήρια κινητήρα, κυλίνδρων, βοηθητικά χειριστήρια και εφαρμογές μέτρησης και παρακολούθησης κατάστασης. Προκειμένου να παρέχεται μεγαλύτερη ορατότητα ολόκληρου του συστήματος, δημιουργείται ένα ενιαίο σύγκλινο δίκτυο για τη σύνδεση προπέλας και κινητήρα στο μηχανοστάσιο μέχρι το δωμάτιο ελέγχου και τη γέφυρα. Με αυτό το σύγκλινο δίκτυο, οι χειριστές πλοίων μπορούν να επιτύχουν υψηλότερη ενοποίηση των υποσυστημάτων και μπορούν να προσαρμόσουν γρήγορα τους ελέγχους πλεύσης, πρόωσης και κατανάλωσης καυσίμου, ακόμη και σε ένα ταχέως μεταβαλλόμενο θαλάσσιο περιβάλλον (Digitizing Engine Control Systems for Operational Efficiency, 2022).



Εικόνα 32 – MOXA – case study - Ψηφιοποίηση συστημάτων ελέγχου κινητήρα για λειτουργική απόδοση

Ένα επίτευγμα που επήλθε με την μηχανογράφηση είναι το **Human Machine Interface - HMI**. Είναι μια διεπαφή χρήστη ή πίνακας εργαλείων που συνδέει ένα άτομο με μια μηχανή, σύστημα ή συσκευή. Ο όρος μπορεί τεχνικά να εφαρμοστεί σε οποιαδήποτε οθόνη που επιτρέπει σε έναν χρήστη να αλληλοεπιδρά με μια συσκευή, στην πράξη όμως χρησιμοποιείται πιο συχνά στο πλαίσιο μιας βιομηχανικής διαδικασίας (Inductive Automation, 2022). Πρόκειται για λογισμικό και υλικό που επιτρέπει στους ανθρώπινους χειριστές να παρακολουθούν την κατάσταση μιας διαδικασίας και να παρακάμπτουν χειροκίνητα τις λειτουργίες αυτόματου ελέγχου σε περίπτωση έκτακτης ανάγκης. Επιτρέπει επίσης σε έναν μηχανικό ή χειριστή ελέγχου να διαμορφώσει σημεία ρύθμισης ή αλγόριθμους ελέγχου και παραμέτρους στον ελεγκτή. Το HMI εμφανίζει επίσης πληροφορίες κατάστασης διεργασίας, ιστορικές πληροφορίες και αναφορές. (NIST, 2022)

Από τη γέφυρα του καπετάνιου μέχρι το σύστημα διανομής ισχύος στο μηχανοστάσιο, περιλαμβάνονται όλα τα στοιχεία που θα αγγίξει, δει, ακούσει ή χρησιμοποιήσει ο χειριστής για να εκτελέσει λειτουργίες ελέγχου και να λάβει ανατροφοδότηση για αυτές τις ενέργειες. Το καθήκον ενός συστήματος HMI είναι να κάνει τη λειτουργία μιας τεχνολογίας αυτονόητη στον χρήστη μέσω «μίμησης» της πραγματικής λειτουργίας. Το σύστημα HMI κρίνεται από τη χρηστικότητά του, η οποία περιλαμβάνει το πόσο εύκολο είναι στην εκμάθησή του καθώς και πόσο παραγωγικός μπορεί να είναι ο χρήστης.

Ένα σύστημα HMI για ένα σκάφος θα μπορούσε να περιλαμβάνει σήματα συναγερμού και κατάστασης από διάφορα υποσυστήματα του πλοίου, όπως ισχύ, πρόωση, σταθεροποιητές, επιτήρηση, HVAC και άλλα. Σε θαλάσσιες εφαρμογές, ο χρήστης μπορεί να περιλαμβάνει λειτουργίες επικοινωνίας και πλοήγησης, εξωτερικά και εσωτερικά πιλοτήρια, χειριστήρια μηχανοστασίου, συστήματα διανομής ισχύος, φωτισμό και συναγερμό, πρόσβαση και έξοδο επιβατών, καθώς και περιφερειακά συστήματα όπως βαρούλκα.

Τα συστήματα HMI πρέπει να μπορούν να διασυνδέονται με το υπό έλεγχο σύστημα καθώς και με άλλα σχετικά συστήματα. Για θαλάσσιες εφαρμογές, η διασύνδεση μπορεί να γίνει μέσω σκληρής καλωδίωσης ή ενός συστήματος διαύλου όπως το CAN bus ή το ProfiBus. Η χρήση συστημάτων σειριακού διαύλου αναπτύσσεται αργά λόγω της αυξημένης πολυπλοκότητας και της περιορισμένης δυνατότητας συντήρησης μακριά από την τοποθεσία του πρότυπου κατασκευαστή. Η επικοινωνία μπορεί να επιτευχθεί μέσω πολλών προσεγγίσεων, δηλαδή, ενσύρματη, ασύρματη σύνδεση, μέσω σειριακού διαύλου ή ακόμα και συνδυασμός όλων αυτών, ανάλογα το πώς το HMI πρέπει να ταιριάζει στις εφαρμογές. (Human Machine Interface Systems for Marine Applications, 2022)

Βέβαια, η ψηφιοποίηση καθιστά τα παραπάνω συστήματα ευάλωτα σε κυβερνοεπιθέσεις. Τα αποτελέσματα της ανάλυσης από μία έρευνα χρησιμοποιώντας το MITRE ATT&CK για τα συστήματα πρόωσης, μηχανημάτων και ελέγχου ισχύος είναι τα εξής:

1) Αρχική πρόσβαση: Ο επιτιθέμενος αποθηκεύει κακόβουλο λογισμικό σε αφαιρούμενα μέσα, τα όποια εισάγονται στα συστήματα
2) Συλλογή: Ο κακόβουλος χρήστης με πρόσβαση στο δίκτυο του πλοίου μπορεί να χρησιμοποιήσει την επίθεση MiTM για να διαμορφώσει την κυκλοφορία του δικτύου σε πραγματικό χρόνο.
3) Επιπτώσεις: Το πλοίο μπορεί να προσαράξει ή να συγκρουστεί με άλλο.

Ένα πλοίο αποτελείται από διάφορα λειτουργικά συστήματα. Πιθανά σενάρια επίθεσης στο περιβάλλον του πλοίου μπορούν να εξηγηθούν μέσω του CVE[27] του συστήματος ελέγχου κινητήρα. Μια πιθανή ροή αυτού του σεναρίου μπορεί να ξεκινήσει από τα τηλεχειριστήρια Auto-Maskin (RPs) και τις μονάδες ελέγχου DCU που χρησιμοποιήθηκαν για τον έλεγχο και την παρακολούθηση κινητήρων πλοίων. Ο επιτιθέμενος μπορεί να επιχειρήσει να χρησιμοποιήσει τον προεπιλεγμένο εργοστασιακό κωδικό πρόσβασης (DCU / 1234) από το εγχειρίδιο του προϊόντος RP 210E που είναι εγκατεστημένο στη γέφυρα ή να χρησιμοποιήσει τα CVE-2018-5401 και CVE-2018-5402 για να αποκτήσει πρόσβαση χωρίς άδεια. Τα DCU 210E και CVE 2018-5400 μπορεί να χρησιμοποιηθούν για πλαστογράφηση ή επιθέσεις αναμετάδοσης με το Modbus-TCP. Τα αυθαίρετα μηνύματα μπορούν να σταλούν σε συσκευές DCU ή RP εξ αποστάσεως χωρίς να μπουν στο μηχανοστάσιο. (Jo, Choi, You, Cha, & Lee, 2022)

2.4.2 Συστήματα ελέγχου έρματος

Από την εισαγωγή των σκαφών με χαλύβδινο κύτος, το νερό έχει χρησιμοποιηθεί ως έρμα για τη σταθεροποίηση σκαφών στη θάλασσα. Το νερό έρματος αντλείται για να διατηρούνται ασφαλείς συνθήκες λειτουργίας καθ' όλη τη διάρκεια του ταξιδιού. Αυτή η πρακτική μειώνει την πίεση στο κύτος, παρέχει εγκάρσια σταθερότητα, βελτιώνει την πρόωση και την ευελιξία και αντισταθμίζει τις αλλαγές βάρους σε διάφορα επίπεδα φορτίου και γίνεται καλύτερη εξοικονόμηση καυσίμου και νερού. Ενώ το νερό έρματος είναι απαραίτητο για ασφαλείς και αποτελεσματικές σύγχρονες ναυτιλιακές δραστηριότητες, το πλοίο δεν μπορεί απλώς να το απορρίψει οπουδήποτε λόγω των ευαίσθητων οικοσυστημάτων στους διαφορετικούς ωκεανούς. Μπορεί να δημιουργήσει σοβαρά οικολογικά, οικονομικά και υγειονομικά προβλήματα λόγω της πληθώρας θαλάσσιων ειδών που μεταφέρονται στο νερό έρματος των πλοίων.

Αυτά περιλαμβάνουν βακτήρια, μικρόβια, και διάφορους άλλους μικρούς οργανισμούς όπως φυτοπλαγκτόν. Το μεταφερόμενο είδος μπορεί να επιβιώσει και να δημιουργήσει έναν αναπαραγωγικό πληθυσμό στο περιβάλλον του ξενιστή, να γίνει χωροκατακτητικά ανταγωνιστικό

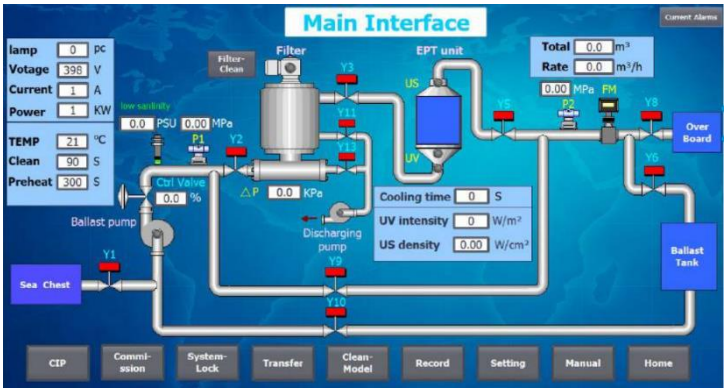
[27] Common Vulnerabilities and Exposures

και να πολλαπλασιαστεί σε αναλογίες παρασίτων. Οι επιστήμονες το αντιλήφθηκαν για πρώτη φορά το 1903 μετά από μια μαζική εμφάνιση της ασιατικής άλγης φυτοπλαγκτού Odontella (Biddulphia sinensis) στη Βόρεια Θάλασσα. Ώστοσο, τη δεκαετία του 1970 η επιστημονική κοινότητα άρχισε να εξετάζει το πρόβλημα λεπτομερώς. Στα τέλη της δεκαετίας του 1980, ο Καναδάς και η Αυστραλία ήταν μεταξύ των χωρών που αντιμετώπιζαν ιδιαίτερα προβλήματα με χωροκατακτητικά είδη και έφεραν τις ανησυχίες τους στην προσοχή της Επιτροπής Προστασίας Θαλάσσιου Περιβάλλοντος (Marine Environment Protection Committee - MEPC) του IMO.

Η εξάπλωση αυτών των ειδών αναγνωρίζεται πλέον ως μία από τις μεγαλύτερες απειλές για την οικολογική και οικονομική ευημερία του πλανήτη. Το παραπάνω δημιούργησε την ανάγκη συνεργασίας των κυβερνήσεων, των οικονομικών τομέων, των μη κυβερνητικών και των διεθνών οργανισμών, και έτσι δημιουργήθηκε η Σύμβαση του ΟΗΕ για το Δίκαιο της Θάλασσας (άρθρο 196). Αυτή παρέχει το παγκόσμιο πλαίσιο απαιτώντας από τα κράτη να συνεργαστούν για την πρόληψη, τη μείωση και τον έλεγχο της ρύπανσης του θαλάσσιου περιβάλλοντος, συμπεριλαμβανομένης της σκόπιμης ή τυχαίας εισαγωγής ειδών, ξένων ή νέων, σε ένα συγκεκριμένο μέρος. Ο Οργανισμός ενέκρινε, τον Νοέμβριο του 1997, το ψήφισμα A.868(20) - Κατευθυντήριες γραμμές για τον έλεγχο και τη διαχείριση του νερού έρματος των πλοίων.

Στις 13 Φεβρουαρίου 2004 εγκρίθηκε με συναίνεση μεταξύ των κρατών μελών του IMO, η Διεθνής Σύμβαση για τον Έλεγχο και τη Διαχείριση του Νερού και Ιζημάτων του Έρματος Πλοίων (Σύμβαση BWM). Η Σύμβαση απαιτεί από όλα τα πλοία να εφαρμόζουν ένα σχέδιο διαχείρισης υδάτων έρματος σύμφωνα με ένα δεδομένο πρότυπο και να φέρουν αντίστοιχο βιβλίο καταγραφής. Το πρόγραμμα επεκτάθηκε περαιτέρω στην πεντηκοστή τρίτη σύνοδο του MEPC τον Ιούλιο του 2005 για να αναπτύξει και να εγκρίνει 14 σετ Κατευθυντήριων γραμμών, που εγκρίθηκε με το ψήφισμα MEPC.173(58) τον Οκτώβριο του 2008. Η σύμβαση BWM τέθηκε σε ισχύ στις 8 Σεπτεμβρίου 2017.

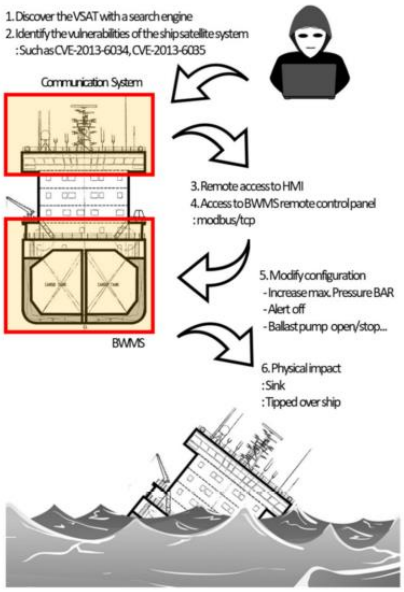
Τα πλοία που εκτελούν ανταλλαγή νερού έρματος θα πρέπει να το κάνουν με απόδοση 95 τοις εκατό και τα πλοία που χρησιμοποιούν σύστημα διαχείρισης υδάτων έρματος (BWMS) θα πληρούν ένα πρότυπο απόδοσης που βασίζεται σε συμφωνηθέντες αριθμούς οργανισμών ανά μονάδα όγκου. (Ballast Water Management - IMO, 2022) Η σύμβαση ορίζει δύο πρότυπα για το νερό που απορρίπτεται. Το πρότυπο D-1 καλύπτει την ανταλλαγή νερού έρματος ενώ το πρότυπο D-2 καλύπτει την επεξεργασία του. Μετά την έρευνα ανανέωσης του IOPP, τα σκάφη θα πρέπει να πληρούν το πρότυπο εκφόρτωσης D-2. Το τελευταίο επιτυγχάνεται συνήθως με την εγκατάσταση ενός εγκεκριμένου συστήματος διαχείρισης υδάτων έρματος (BWMS). Τα πλοία που ναυπηγούνται μετά την έναρξη ισχύος θα πρέπει να έχουν εγκατεστημένο σύστημα επεξεργασίας κατά την παράδοση. (Ballast Water Management - DNV, 2022)



Εικόνα 33 - Ενδεικτική εικόνα ενός Human Machine Interface ελέγχου συστήματος έρματος. (Manuals Lib, 2022)

Το σύστημα Ballast Water Management System (BWMS) αποτελείται από μια δεξαμενή εγκατεστημένη στο κάτω μέρος του πλοίου καθώς και στην αριστερή και δεξιά πλευρά του κύτους για να διατηρεί το κέντρο βάρους του πλοίου. Μια αντλία χρησιμοποιείται για να γεμίσει ή να αδειάσει τη δεξαμενή με θαλασσινό νερό. Οι αντλίες του πλοίου ελέγχονται από το Human Machine Interface (HMI) και μπορούν να παρακολουθούνται από την ξηρά μέσω ενός

δορυφορικού συστήματος επικοινωνίας. Για να αποφευχθεί η ανατροπή του πλοίου όταν έχει κλίση, η αντλία BWMS πρέπει να λειτουργεί με ακρίβεια και η αστοχία αυτού του συστήματος μπορεί να προκαλέσει βύθιση του πλοίου.



Εικόνα 34 - Σενάριο επίθεσης στο σύστημα ελέγχου έρματος (Jo, Choi, You, Cha, & Lee, 2022)

Οι πληροφορίες που δημοσιεύθηκαν τον Ιούλιο του 2021 ήταν το έναυσμα για την μελέτη μεθόδων εισβολής στο εν λόγω σύστημα. Πιο συγκεκριμένα, τον Δεκέμβριο του 2020, μια ιρανική ομάδα χάκερ παραβίασε το σύστημα βιομηχανικού ελέγχου των εγκαταστάσεων νερού του Ισραήλ (ICS) αποκτώντας πρόσβαση στο σύστημα HMI. Σε αυτό το σύστημα, η θύρα Modbus / TCP 502 ήταν ανοιχτή στο Διαδίκτυο και ήταν ευάλωτη σε μη εξουσιοδοτημένη πρόσβαση. Ο αντίπαλος ήταν σε θέση να χειριστεί την πίεση και τη θερμοκρασία του νερού. Αυτό το παράδειγμα υποστηρίζει την πρόβλεψη επιθέσεων στο BWMS ενός πλοίου : (Iran’s secret cyber files on how cargo ships and petrol stations could be attacked, 2022).

Η επίθεση ξεκινά με την αποστολή εντολών εξ αποστάσεως από την ξηρά στο πλοίο μέσω θαλάσσιου εξοπλισμού δορυφορικών επικοινωνιών. Αυτή η επίθεση θα χρησιμοποιούσε ένα Seagull 5000i και Sealink CIR, που είναι συσκευές θαλάσσιας δορυφορικής επικοινωνίας τοποθετημένες σε πλοία. Το Σώμα των Φρουρών της Επανάστασης του Ιράν (IRGC) σχεδίασε την επίθεση σε τρεις φάσεις, που η κάθε φάση έχει τα δικά της στάδια

1) **Σχεδιασμός**
   Αναγνώριση: Το πρώτο βήμα είναι να προσδιοριστεί το μοντέλο του θαλάσσιου δορυφορικού εξοπλισμού επικοινωνίας που ήταν οι Thuraya και Wideye. Κατά την ανάλυση αυτής της μελέτης, γνωστοποιήθηκε μια νέα απειλή που προέκυψε από το γεγονός ότι ο κωδικό πρόσβασης στο BWMS του πλοίου ήταν εμφανής. Αυτό ανακαλύφθηκε από ένα μέλος του πληρώματος σε μια υπηρεσία κοινωνικού δικτύου, κοινοποιώντας και άλλες πληροφορίες όπως το όνομα του πλοίου και τον εξοπλισμό του.
2) **Προετοιμασία**
   a) **Ανάπτυξη πόρων**: Οι συσκευές Thuraya που αναφέρονται έχουν ευπάθειες διαπιστευτηρίων με σκληρό κώδικα που έχουν εντοπιστεί στα CVE-2013-6034 και CVE-2013-6035. Πολλά πλοία που βρίσκονται ακόμη σε υπηρεσία ενδέχεται να έχουν αυτήν την ευπάθεια. Κάποιες δορυφορικές συσκευές επικοινωνίας μπορεί να είναι προσβάσιμες χρησιμοποιώντας θύρα TCP 1827, χωρίς πιστοποίηση.
   b) **Αρχική πρόσβαση**: Ο αντίπαλος μπορεί να αποκτήσει πρόσβαση στο δίκτυο του πλοίου μέσω ενός γνωστού έγκυρου λογαριασμού, ο οποίος έχει προσδιοριστεί στο

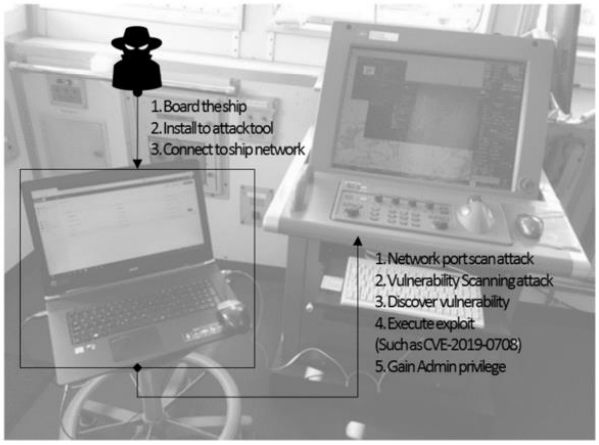
προηγούμενο στάδιο και θα μπορούσε να είναι ο προεπιλεγμένος λογαριασμός ("admin").

c) **Πλευρική κίνηση**: Το επόμενο βήμα περιλαμβάνει την είσοδο του στο σύστημα BWMS του σκάφους. Το BWMS του εσωτερικού δικτύου θα πρέπει να είναι προσβάσιμο από το τερματικό θαλάσσιων δορυφορικών επικοινωνιών και ως εκ τούτου το τερματικό και το BWMS συνδέονται από το ίδιο δίκτυο.

3) Εισχώρηση

a) **Εντολή και έλεγχος**: Ο κακόβουλος χρήστης επιτίθεται στο σύστημα, διαμορφώνει τα δεδομένα που συλλέγονται και επεξεργάζονται από αυτό, όπως για παράδειγμα της αντλίας. Επίσης μπορεί να απενεργοποιήσει και τον συναγερμό της. Όσον αφορά το υλικό, η επίθεση παρεμβαίνει στην ακριβή λειτουργία της αντλίας και του μετρητή πίεσης προκαλώντας δυσλειτουργία του αισθητήρα ή μπλοκάροντας/διαμορφώνοντας τις πληροφορίες κατάστασης του. Όσον αφορά το λογισμικό, η επίθεση καταστρέφει το σύστημα αρχείων διακομιστή διαχείρισης ή προκαλεί σφάλματα διακομιστή.

b) **Επίπτωση**: Το χειρότερο ενδεχόμενο είναι η βύθιση ή η ανατροπή του πλοίου και στην καλύτερη των περιπτώσεων η αυξημένη κλίση του πλοίου με ότι αυτό συνεπάγεται (Jo, Choi, You, Cha, & Lee, 2022).



Εικόνα 35 – Σενάριο επίθεσης στο BWMS (Jo, Choi, You, Cha, & Lee, 2022)

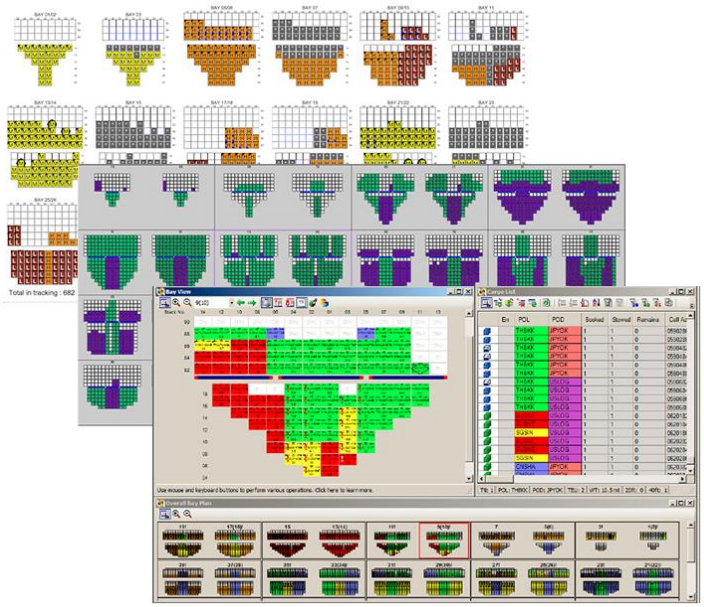
Σε μια ελεγχόμενη επίθεση που έκαναν οι εμπειρογνώμονες του Naval Dome επέλεξαν να διεισδύσουν στο σύστημα χρησιμοποιώντας ένα μολυσμένο USB. Μόλις συνέδεσαν το μολυσμένο αυτό μέσο αποθήκευσης στο Σύστημα Ελέγχου Μηχανών του σκάφους, το αρχείο με τον ιό έτρεξε μόνο του και άρχισε να αλλάζει τη λειτουργικότητα των βοηθητικών συστημάτων. Ο πρώτος στόχος ήταν **το σύστημα έρματος**, όπου στην οθόνη όλα φαινόντουσαν φυσιολογικά, ενώ οι βαλβίδες και οι αντλίες είχαν διακοπεί. Ανέφεραν επίσης ότι είχαν την δυνατότητα να επηρεάσουν όλα τα βοηθητικά συστήματα που ελέγχονται από το ΣΕΜ, συμπεριλαμβανομένου του κλιματισμού, των γεννητριών, των συστημάτων καυσίμων και άλλων. Ο Itai Sela, διευθύνων σύμβουλος της εταιρείας, σημείωσε επίσης ότι οι ιοί στα συστήματα των πλοίων μπορούν να μεταφερθούν άθελά τους από τον κατασκευαστή του συστήματος. Ακόμα και οι αναβαθμίσεις λογισμικού μπορούν να ανοίξουν ακούσια την πύλη σε μια επίθεση στον κυβερνοχώρο (Naval Dome exposes vessel vulnerabilities to cyber attack, 2022) (Tests Show Ease of Hacking ECDIS, Radar and Machinery, 2022).

2.4.3 Συστήματα φόρτωσης και ισορροπίας φορτίου

Το σύστημα φόρτωσης των φορτίων που μεταφέρουν τα πλοία είναι αλληλένδετο με το σύστημα διαχείρισης έρματος, καθώς και τα δύο σχετίζονται με την ισορροπία του σκάφους. Σε ένα πλοίο μεταφοράς εμπορευματοκιβωτίων, προετοιμάζεται ένα **σχέδιο φόρτωσης ή αλλιώς στοιβασίας (Bay or Stowage plan)** σύμφωνα με την ποσότητα, το βάρος των εμπορευματοκιβωτίων που πρόκειται να φορτώσει και εκφορτώσει σε ένα συγκεκριμένο λιμάνι. Εκτός των άλλων,

υπολογίζεται η κατάσταση των δεξαμενών, δηλαδή η μάζα που μεταφέρεται από το πλοίο εκτός από το φορτίο. Αυτό γίνεται για να διατηρείται η σταθερότητα του ανά πάσα στιγμή.

Το σχέδιο αυτό είναι απλώς μια λίστα CSV[28] ή κάτι παρόμοιο, και σύμφωνα με τους ερευνητές του Pen Test Partners μπορεί να παραβιαστεί και να τροποποιηθεί. Για την διαδικασία της φορτο-εκφόρτωσης μπορεί να χρειαστούν από λίγες ώρες έως και 2 μέρες. Στην περίπτωση όμως που γίνει τροποποίηση των δεδομένων και δεν υπάρχει πλήρης γνώση για το που βρίσκεται κάθε container, ο χρόνος μπορεί να μεταβληθεί σε βδομάδες προκειμένου να γίνει χειροκίνητα η απογραφή του πλοίου. Το μπλοκάρισμα ενός λιμανιού για μια περίοδο ισοδυναμεί με τεράστιο κόστος και θα μπορούσε ακόμη να θέσει σε κίνδυνο τον εφοδιασμό μιας ολόκληρης χώρας.



Εικόνα 36 - Πρόγραμμά διαχείρισης φορτίου σε εμπορευματοκιβώτια. (Munro, Sinking container ships by hacking load plan software, 2022)

Για το σχέδιο αυτό και την ασφαλή στοιβασία του φορτιού στα πλοία υπεύθυνος είναι ο Διευθυντής του πλοίου (Chief Officer) (cargo plan stowage plan, 2022). Υπάρχουν διάφοροι λόγοι που προσδιορίζουν την σημαντικότητα του εν λόγω σχεδιασμού. Αυτοί είναι η προστασία του πλοίου, του φορτίου, η χρήση της μέγιστης διαθέσιμης χωρητικότητάς του, η ταχύτερη φορτοεκφόρτωση και φυσικά η ασφάλεια του πληρώματος και των ανδρών της ξηράς ανά πάσα στιγμή. Ορισμένα πράγματα που πρέπει να υπολογίζονται κατά τη φόρτωση εμπορευματοκιβωτίων φορτίου είναι:

- Ο προγραμματισμός φορτίου να γίνεται σύμφωνα με το πιο πρόσφατο φορτίο, δηλαδή το φορτίο για μεταγενέστερο λιμάνι δεν πρέπει να τοποθετείται πάνω από αυτό ενός προγενέστερου λιμένα
- Οι συνθήκες φόρτισης πρέπει να υπολογίζονται για την ευστάθεια, δύναμη διάτμησης, ροπή κάμψης, στρέψης και βύθισμα κ.λπ.
- Η γραμμή ορατότητας του IMO

[28] Ένα αρχείο τιμών διαχωρισμένων με κόμματα (Comma Separated Values) είναι ένα οριοθετημένο αρχείο κειμένου που χρησιμοποιεί κόμμα για να διαχωρίσει τιμές. Κάθε γραμμή του αρχείου είναι μια εγγραφή δεδομένων . Κάθε εγγραφή αποτελείται από ένα ή περισσότερα πεδία , διαχωρισμένα με κόμμα. Η χρήση του κόμματος ως διαχωριστικού πεδίου είναι η πηγή του ονόματος για αυτήν τη μορφή αρχείου . Ένα αρχείο CSV συνήθως αποθηκεύει δεδομένα πίνακα (αριθμούς και κείμενο) σε απλό κείμενο , οπότε κάθε γραμμή θα έχει τον ίδιο αριθμό πεδίων. (Comma-separated values, 2022)

- Η στοιβασία των επικίνδυνων φορτιών (International Maritime Dangerous Goods – IMDG) να γίνεται σύμφωνα με τους κανονισμούς που έχουν οριστεί και το Έγγραφο συμμόρφωσης με τις ειδικές απαιτήσεις
- Η τιμή GM ή αλλιώς Μετακεντρικό ύψος, που είναι η απόσταση μεταξύ του κέντρου βάρους (Center of Gravity - CoG) του πλοίου και του μετακέντρου του, γιατί είναι υπεύθυνη για τον καθορισμό του παράγοντα ευστάθειας του πλοίου (how to plan cargo containers stowage on container ship, 2022)

Ο παραπάνω σχεδιασμός υπόκειται στους κανόνες των Ηνωμένων Εθνών για την Ηλεκτρονική Ανταλλαγή Δεδομένων για τη Διοίκηση, το Εμπόριο και τις Μεταφορές (UN/EDIFACT) που περιλαμβάνει ένα σύνολο διεθνώς συμφωνημένων προτύπων, καταλόγων και κατευθυντήριων γραμμών για την ηλεκτρονική ανταλλαγή δεδομένων μέσω μηνυμάτων (UNEDIFACT, 2022). Ένα τέτοιο μήνυμα είναι το BAPLIE που χρησιμοποιείται μεταξύ ναυτιλιακών γραμμών, λιμενικών αρχών, τερματικών σταθμών και πλοίων για την παροχή συμβουλών στη ναυτιλιακή βιομηχανία. Καθορίζονται επίσης γενικές πληροφορίες σχετικά με αυτό, όπως η ακριβής θέση, το βάρος και η κατηγορία επικίνδυνου φορτίου (BAPLIE, 2022). Σύμφωνα με μια νέα οδηγία SOLAS για το πιστοποιημένο μεικτό βάρος εμπορευματοκιβωτίων εξαγωγής απαιτείται το μήνυμα Verified Gross Mass (VERMAS), που επιτρέπει την υποβολή της επαληθευμένης ακαθάριστης μάζας του συσκευασμένου εμπορευματοκιβωτίου και των υποστηρικτικών πληροφοριών. (VERMAS, 2022)

Τα μηνύματα EDI μπορούν να κοινοποιηθούν απευθείας μεταξύ ορισμένων λιμανιών, επομένως το σχέδιο φόρτωσης είναι λιγότερο εκτεθειμένο. Ωστόσο, εξακολουθεί να υπάρχει σημαντική έλλειψη ασφάλειας στην επικύρωση της ακεραιότητας του μηνύματος. Το ενδεχόμενο τροποποίησης των δεδομένων αυτών μπορεί να επιφέρει ορισμένες συνέπειες. Ένα παράδειγμα είναι να μεταβληθούν τα δεδομένα σε ελλιπές ή υπερβολικό βάρος, δημιουργώντας την ανάγκη για έκτακτη φόρτωση ή εκφόρτωση του νερού έρματος αντίστοιχα. Αυτό μπορεί να προκαλέσει σημαντικά περιβαλλοντικά προβλήματα και πρόστιμα. Επίσης, επηρεάζει την απόφαση για την λήψη καυσίμων, αλλά και την ταχύτητα και απόδοση του πλοίου λόγω βέλτιστου συνολικού φορτίου.

Ένας πιθανός χάκερ θα αναζητούσε την τελευταία τιμή από ένα μήνυμα VGM (Verified Gross Mass), η οποία δείχνει το βάρος του φορτίου. Η αλλαγή αυτής της τιμής θα σήμαινε ότι το λογισμικό προγραμματισμού φόρτωσης του σκάφους θα τοποθετούσε το εμπορευματοκιβώτιο σε λάθος θέση. Οι ερευνητές εξήγησαν ότι είναι δυνατό χρησιμοποιώντας παρόμοια κόλπα να τοποθετηθεί ένα βαρύ εμπορευματοκιβώτιο με λάθος ετικέτα στην κορυφή της στοίβας, μετακινώντας το κέντρο βάρους πολύ ψηλά.

Ενώ ορισμένες ενέργειες εξισορρόπησης είναι αυτόματες, οι αντλίες μεταφοράς ενδέχεται να μην είναι σε θέση να αντιμετωπίσουν μια ταχέως εξελισσόμενη, απρόβλεπτη κατάσταση εκτός ισορροπίας. Πέρα από το κίνδυνο του που ελλοχεύει για το πλοίο, το φορτίο και το πλήρωμα, μπορεί να πληγεί και το κύρος της διαχειρίστριας εταιρίας. Τέλος, ένα εξίσου πιθανό γεγονός είναι η ανατροπή του και το μπλοκάρισμα μιας σημαντικής διώρυγας (π.χ. Σουέζ το 2021) που μπορεί να επιφέρει κρίσιμα αποτελέσματα στην παγκόσμια οικονομία – αύξηση τιμών, εναλλακτική διαδρομή, κατανάλωση καυσίμων κ.λπ.

Επίσης, ο επιτιθέμενος έχει την δυνατότητα να επεξεργαστεί και τα δεδομένα των φορτίων, κυρίως αυτών που χρειάζονται ειδικό χειρισμό. Για παράδειγμα, τα containers – ψυγεία πρέπει να βρίσκονται σε συγκεκριμένες θέσεις που διαθέτουν τροφοδοτικά. Οι κακοποιοί θα μπορούσαν να αλλάξουν την ονομασία μιας παρτίδας αγαθών που χρειάζονται ψύξη έτσι ώστε τα αγαθά να τοποθετηθούν οπουδήποτε. Ορισμένα φορτία είναι ευαίσθητα σε έντονες μυρωδιές, ιδιαίτερα ο καφές, και πρέπει να τοποθετούνται μακριά από δυσοσμία.

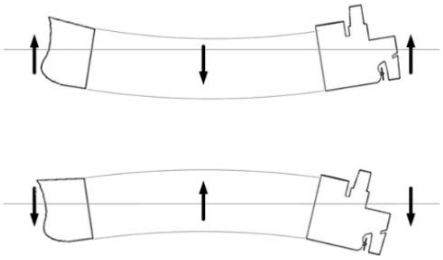
Οι εγκληματίες ενδιαφέρονται λιγότερο να αποσταθεροποιήσουν τα πλοία και περισσότερο να κλέψουν αγαθά αλλάζοντας τη διαδρομή των εμπορευματοκιβωτίων. Για τον σκοπό αυτό θα χρησιμοποιούσαν τα μηνύματα «COPRAR / COPARN / CODECO / COARRI»[29]. Αυτό έχει

[29] Έχει αναπτυχθεί ένα έγγραφο ως μέρος ενός συνόλου οδηγιών αναφοράς για τα μηνύματα θαλάσσιων εμπορευματοκιβωτίων από την ομάδα International Transport Implementation Guidelines Group (ITIGG) και καλύπτει την

αποδειχθεί αφού κατά καιρούς έχει γίνει κατάχρηση στα συστήματα ανταλλαγής μηνυμάτων πλοίων και τερματικών προκειμένου είτε να αποκρύψουν ή να δρομολογήσουν ναρκωτικά ή να τα κλέψουν. (Leyden, 2022) (Munro, Making prawn espressos, or hacking ships by deciphering BAPLIE EDIFACT messaging, 2022) (Munro, Sinking container ships by hacking load plan software, 2022)

Τα πλοία μεταφοράς χύδην φορτίου είναι τελείως διαφορετικά από αυτά των εμπορευματοκιβωτίων. Την δεκαετία 80 με 90 υπήρχαν πολλά πλοία μεταφοράς χύδην φορτίου που βυθίστηκαν, όπως για παράδειγμα το MV Derbyshire που εξαφανίστηκε και εντοπίστηκε 20 χρόνια αργότερα. Οι έρευνες έδειξαν ότι η αιτία ήταν η υπερβολική πίεση η οποία προκάλεσε τη διάσπασή του. Για να αντιμετωπιστούν τέτοιου είδους απώλειες και να διασφαλιστεί ότι οι τάσεις δεν υπερβαίνουν τις προδιαγραφές σχεδιασμού, εφαρμόστηκαν **συστήματα παρακολούθησης καταπόνησης κύτους (Hull Stress Monitoring Systems - HSMS)**. Ο σκοπός τους είναι να ασχολούνται με τη φόρτωση στο λιμάνι και να διαχειρίζονται το φορτίο στη θάλασσα.

Η φόρτωση πρέπει να γίνεται προσεκτικά καθώς υπάρχουν δυο οριακές περιπτώσεις καταπόνησης στα εν λόγω πλοία. «Θεωρώντας το πλοίο ως κινούμενο επί της κορυφής ή της κοιλάδας ενός πρυμναίου κύματος, ίδιου περίπου μήκους και ταχύτητας, παρουσιάζεται περίσσεια άντωσης περί το μέσον του σκάφους, εφόσον η κορυφή του φορτίζοντος κύματος είναι κοντά στην μέση τομή -**hogging**- είτε η περίσσεια άντωσης βρίσκεται στα άκρα του σκάφους, πράγμα που συμβαίνει όταν η κοιλάδα του κύματος είναι στο κέντρο του πλοίου -**sagging**.» (Παπανικολάου, 2009). Όταν φορτώνεται ένα πυκνό φορτίο όπως σιδηρομετάλλευμα, είναι εκπληκτικά εύκολο να συμβεί το παρακάτω:



Εικόνα 37 - Sagging και Hogging (Munro, Sinking bulk carrier ships by hacking HSMS, 2022)

Η φόρτωση παραδοσιακά θα γινόταν από τον Chief Officer κάνοντας χειροκίνητους υπολογισμούς για την εκτίμηση των δυνάμεων κάμψης στο κύτος. Σήμερα γίνεται με τη χρήση ηλεκτρονικών μετρητών καταπόνησης και επιταχυνσιομέτρων που τροφοδοτούν δεδομένα σε συστήματα παρακολούθησης επί του σκάφους. Εάν εντοπιστεί υπερβολική καταπόνηση ηχούν συναγερμοί στη γέφυρα, ειδοποιώντας το πλήρωμα να αναλάβει δράση. Τα δεδομένα τροφοδοτούνται επίσης σε Voyage Data Recorder, συνήθως μέσω δικτύου IP.

Το σύστημα HSMS, σύμφωνα με τον Munro μπορεί να παραβιαστεί εφόσον πρώτα έχει αποκτηθεί πρόσβαση στο δίκτυο είτε μέσω της μονάδας satcom είτε μέσω ενός phish. Από κει

ηλεκτρονική ανταλλαγή δεδομένων (Electronic Data Interchange – EDI) που σχετίζεται με τη ναυτιλία. Συγκεκριμένα, παρέχει καθοδήγηση ως προς τη συνιστώμενη χρήση κωδικών, χαρακτηριστικών, στοιχείων δεδομένων, σύνθετων στοιχείων και τμημάτων, για να διασφαλιστεί η συνεπής χρήση σε όλη την παγκόσμια κοινότητα εμπορίου και μεταφορών. Τα μηνύματα EDI αυτά είναι εναλλάξιμα και αναγνώσιμα από άλλες παρόμοιες υπηρεσίες σε όλο τον κόσμο. Τα παραπάνω μηνύματα σύμφωνα με το εν λόγω έγγραφο σημαίνουν τα εξής:

COPRAR: Container Discharge/Loading Order, περιέχει την εντολή ότι τα καθορισμένα εμπορευματοκιβώτια πρέπει να εκφορτωθούν από το πλοίο

COPARN: Container Announcement, προορίζεται για την εκτέλεση μιας ποικιλίας εντολών που σχετίζονται με τις κινήσεις του φορτίου

CODECO: Container Gate-in/Gate-out Report, επιβεβαιώνει ότι έχει πραγματοποιηθεί η μετακίνηση του φορτίου από ή στον μεταφορέα της ενδοχώρας

COARRI: Container Discharge/Loading Report, ο τερματικός σταθμός αναφέρει ότι το φορτίο έχει εκφορτωθεί/φορτωθεί από το / στο πλοίο

(International Reference Guideline For The Implementation Of Transport EDI Messages, 2022)

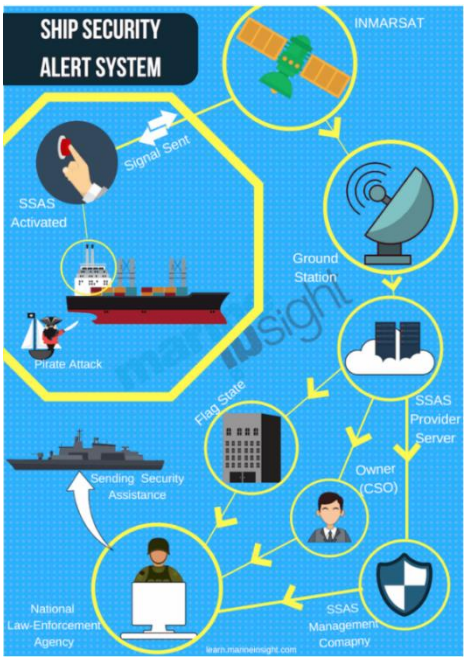
και έπειτα μπορεί ο επιτιθέμενος είτε να διακόψει είτε να χειριστεί τα δεδομένα φόρτωσης που τροφοδοτούνται από και προς το σύστημα παρακολούθησης. Αυτό θα έχει ως αποτέλεσμα να μην ηχήσει κάποια προειδοποίηση, η φόρτωση να συνεχιστεί κανονικά, το πλήρωμα που βασίζεται στα αυτοματοποιημένα συστήματα παρακολούθησης να μην ανησυχήσει και το σκάφος στην τελική να κόβεται στην μέση. (Munro, Sinking bulk carrier ships by hacking HSMS, 2022)

2.4.4 Συστήματα ασφαλείας

Στη θάλασσα υπάρχουν πολλοί κίνδυνοι τόσο φυσικοί όσο και ανθρωπογενείς. Μια από τις μεγαλύτερες ανησυχίες, τόσο για το πλήρωμά όσο και για τους πλοιοκτήτες, είναι οι αυξημένες δραστηριότητες πειρατείας. Η αντιμετώπιση της ένοπλης ανθρώπινης επίθεσης είναι μια μεγάλη πρόκληση που αντιμετωπίζει σήμερα η ναυτιλιακή βιομηχανία. Ένα παλαιότερο σύστημα που υπήρχε για την αντιμετώπιση τέτοιων επιθέσεων, είναι το **Σύστημα Προειδοποίησης Ασφάλειας Πλοίου (Ship Security Alerting System - SSAS)**, το οποίο επέτρεπε σε ένα πλοίο να στέλνει σήματα κινδύνου στο κέντρο ελέγχου. Σύμφωνα με τις διεθνείς απαιτήσεις, σχεδόν όλα τα πλοία, και κυρίως αυτά που εκτελούν υπερατλαντικά ταξίδια, πρέπει να είναι εφοδιασμένα με αυτό.

Το σύστημα αυτό είναι ένα μέτρο για την ενίσχυση της ασφάλειας του πλοίου και την καταστολή πειρατείας ή/και τρομοκρατίας κατά της ναυτιλίας. Αναγνωρισμένο ευρέως ως μέρος του Διεθνούς Κώδικα Ασφαλείας Πλοίων και Λιμενικών Εγκαταστάσεων (Κωδικός ISPS), το SSAS συμπληρώνει τις προσπάθειες του Διεθνούς Ναυτιλιακού Οργανισμού (IMO) να αυξήσει την ασφάλεια των θαλάσσιων σκαφών και είναι η κατάληξη από την συνεργασία του τελευταίου με το Cospas-Sarsat. Η βασική ιδέα είναι ότι σε περίπτωση περιστατικού που μπορεί να οριστεί ως απειλή για το πλοίο, ενεργοποιείται ο φάρος SSAS του πλοίου.

Είναι ένας τύπος αθόρυβου συναγερμού ασφαλείας, το οποίο, όταν ενεργοποιηθεί, δεν εκπέμπει κανένα οπτικοακουστικό σήμα στο πλοίο ή σε κοντινά σκάφη ή δυνάμεις ασφαλείας. Η ειδοποίηση στις περισσότερες περιπτώσεις λαμβάνεται πρώτα από τον ιδιοκτήτη του πλοίου ή τις διορισμένες επαγγελματικές υπηρεσίες διαχείρισης και παρακολούθησης, με σημαντικές λεπτομέρειες όπως η τοποθεσία του πλοίου, ημερομηνία και ώρα ειδοποίησης κλπ.. Ο συναγερμός μεταφέρεται συνεχόμενα στα εν λόγω μέρη εκτός αν απενεργοποιηθεί ή επαναρρυθμιστεί. Στη συνέχεια μεταβιβάζεται στο κράτος σημαίας του πλοίου και αυτοί οι παραλήπτες είναι υποχρεωμένοι να ενημερώσουν τις πλησιέστερες εθνικές αρχές της περιοχής.



Εικόνα 38 - Λειτουργία Σύστηματος Προειδοποίησης Ασφάλειας Πλοίου (Anish, 2022)

Αυτές με την σειρά τους θα αποστείλουν κατάλληλες στρατιωτικές δυνάμεις ή δυνάμεις επιβολής του νόμου για την αντιμετώπιση της τρομοκρατικής ή πειρατικής απειλής (Anish, 2022).

Το παραπάνω είναι φαινομενικά αποτελεσματικό σύστημα, έχει όμως πολλά μειονεκτήματα. Αυτό το σύστημα θαλάσσιας ασφάλειας είναι αργό και ελαφρώς ανεπαρκές για τον χειρισμό τεράστιων καταστάσεων παραβίασης της ασφάλειας που προκύπτουν από πειρατικές επιθέσεις. Ως αναβάθμιση αυτού του συστήματος, το **σύστημα αναφοράς ασφάλειας πλοίου (Ship Security Reporting System - SSRS)** είναι ένα πιο ακριβές σύστημα που επιτρέπει ταχύτερη δημιουργία αντιγράφων ασφαλείας για ένα πλοίο που βρίσκεται σε κίνδυνο.

Σύμφωνα με το SSRS, ένα σήμα κινδύνου από το πλοίο αποστέλλεται απευθείας στο Maritime Security Center- Horn of Africa (MSCHOA) και στο UK Maritime Trade Operations (UKMTO). Αυτό το σύστημα έχει εισαχθεί ειδικά για τον περιορισμό στις περιοχές του Κόλπου Άντεν και στα ανοιχτά της Σομαλίας. Επιτρέπει τη συνεχή παρακολούθηση των σκαφών εντός του καθορισμένου εύρους, δηλαδή υπάρχει συνεχής λήψη σημάτων. Όταν το MSHAO ή το UKMTO λαμβάνει ένα σήμα κινδύνου, αρχικά επαληθεύει την γνησιότητά του. Στη συνέχεια, οι πληροφορίες του σκάφους ανακτώνται και μεταφέρονται στις σχετικές ναυτικές δυνάμεις που είναι αρμόδιες για τη θαλάσσια ασφάλεια σε αυτές τις περιοχές και δραστηριοποιούνται αμέσως (KaranC, 2022).

Εκτός όμως από τα παραπάνω συστήματα, έχουν εγκατασταθεί και **Συστήματα Βιντεοεπιτήρησης (Video Surveillance Systems - VSS)** και διαδραματίζουν αξιόλογο ρόλο σε όλους τους τύπους σύγχρονων πλοίων για την ασφάλεια τους, του φορτίου και του πληρώματος. Αυτά τα συστήματα χρησιμοποιούνται κυρίως για την παρακολούθηση και τον εντοπισμό των κρίσιμων λειτουργιών του πλοίου και για την προστασία από επιθέσεις τρομοκρατών και πειρατών. Ωστόσο, τα VSS βρέθηκαν πρόσφατα ευάλωτα σε αρκετές κυβερνοεπιθέσεις και έχουν προκύψει ορισμένα ζητήματα ασφαλείας.

Για παράδειγμα, ερευνητές από το Bitdefender διαπίστωσαν ότι δύο μοντέλα καμερών CCTV (Closed Circuit Television), που χρησιμοποιούνται στα σύγχρονα πλοία, είναι ευάλωτα σε ελαττώματα υπερχείλισης buffer. Με την εκμετάλλευση αυτής της ευπάθειας, οι ερευνητές μπόρεσαν να παρακολουθήσουν τις δραστηριότητες της χακαρισμένης κάμερας και να αντικαταστήσουν τους κωδικούς πρόσβασης. Επιπλέον, αυτή η ευπάθεια μπορεί να προκαλέσει κατάρρευση του συστήματος VSS ή, χειρότερα, να δημιουργήσει σημείο εισόδου για άλλες κυβερνοεπιθέσεις (Akpan, Bendiab, Shiaeles, Karamperidis, & Michaloliakos, 2022). Να

σημειωθεί, επίσης, ότι οι κάμερες ενέχουν υψηλότερα επίπεδα κινδύνου επειδή είναι συχνά πρόσθετες.

Σε ένα φυλλάδιο δημοσιοποιήθηκε ένα άρθρο το όποιο αναφέρει ένα σενάριο πολυτροπικής επίθεσης σε λιμάνι, δηλαδή συνδυασμός κυβερνοεπίθεσης αλλά και φυσικής. Ως απλό παράδειγμα, η εισβολή σε κάμερες ασφαλείας σε ένα λιμάνι αυξάνει την ευπάθεια σε μια φυσική εισβολή. Έτσι, μια κυβερνοεπίθεση θα μπορούσε να είναι προάγγελος μιας φυσικής επίθεσης ή και το αντίστροφο. Ένα σενάριο με αυξημένη την πιθανότητα επιτυχίας είναι το παρακάτω:

- Κλείσιμο των πυλών και παραπλάνηση καρτών ή άλλων ταυτοποιήσεων για έλεγχο πρόσβασης εισόδου εξόδου.
- Απενεργοποίηση των συναγερμών και των καμερών για αποφυγή εντοπισμού.
- Διακοπή παροχής ρεύματος για απόσπαση προσοχής και διευκόλυνση των επιτιθέμενων.
- Απενεργοποίηση των φωτεινών σηματοδοτών για δημιουργία μποτιλιαρίσματος, έτσι ώστε τα οχήματα έκτακτης ανάγκης να μην μπορούν να ανταποκριθούν.
- Παραβίαση συστήματος επικοινωνίας έκτακτης ανάγκης και παραπληροφόρηση μελών.

Όταν εξετάζουμε πιθανά σενάρια για συνδυασμένες επιθέσεις, θα πρέπει να ληφθεί υπόψη η απειλή, η ευπάθεια και οι συνέπειες για τον προσδιορισμό του κινδύνου. Το παραπάνω σενάριο, εκτός από λιμάνι, μπορεί να λάβει χώρα και σε πλοίο, με εξίσου καταστροφικά αποτελέσματα (Roberts, et al., 2022).

2.4.5 Καταγραφείς δεδομένων ταξιδιού

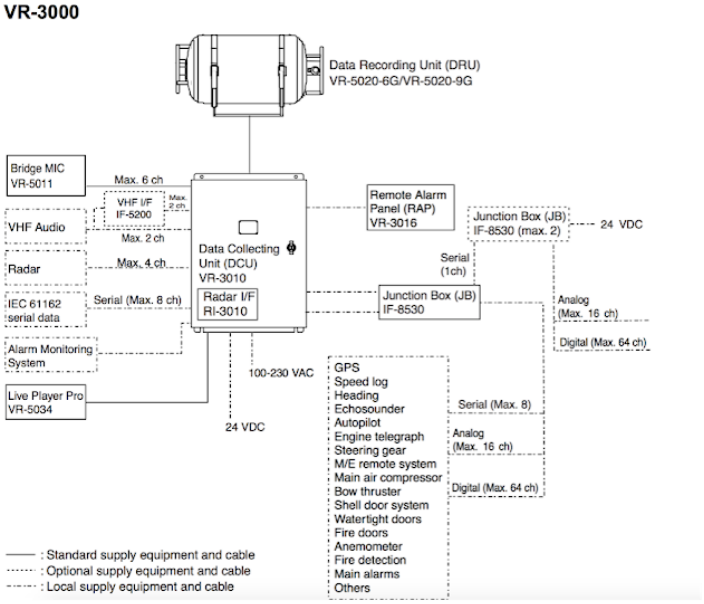
Η τεχνολογία πληροφοριών όχι μόνο επιτρέπει την αποτελεσματική επικοινωνία σε πραγματικό χρόνο και την παρακολούθηση των πλοίων, αλλά χρησιμοποιεί επίσης ορισμένες προληπτικές λύσεις και τεχνολογίες μετά το ατύχημα, για να βελτιώσει την ασφάλεια και να διασφαλίσει τη συμμόρφωση. Το κύριο σύστημα που χρησιμοποιείται είναι το «μαύρο κουτί» του ναυτιλιακού κόσμου, γνωστό και ως σύστημα **καταγραφής δεδομένων ταξιδιού (Voyage Data Recorder - VDR)**, το οποίο έγινε υποχρεωτικό τον Ιούλιο του 2002, σύμφωνα με τους κανονισμούς του IMO για όλα τα επιβατηγά πλοία και άλλα πλοία άνω των 3.000 ολικής χωρητικότητας.

Ενώ ο πρωταρχικός σκοπός αυτού του συστήματος είναι να βοηθήσει τη διαδικασία διερεύνησης μετά το ατύχημα, οι εταιρείες μπορούν επίσης να το χρησιμοποιήσουν για προληπτική συντήρηση, ανάλυση, πρόληψη ατυχημάτων, παρακολούθηση απόδοσης και μείωση του συνολικού λειτουργικού κόστους του σκάφους (Sea Rates, 2022). Τα συστήματα περιλαμβάνουν μια προστατευτική κάψουλα αποθήκευσης. Είναι τοποθετημένα εξωτερικά του πλοίου, και μπορούν να ανακτηθούν από δύτες σε περίπτωση βύθισης του.

Εικόνα 39 - Voyage Data Recorder (Marine Digital, 2022)

Η κάψουλα περιέχει 24 ώρες καταγεγραμμένων δεδομένων πλοίου, συμπεριλαμβανομένων αυτών που προέρχονται από διαφορετικούς αισθητήρες και εξοπλισμού του σκάφους. Παραδείγματα αυτών θα περιλαμβάνουν πληροφορίες κινητήρα/έλικα και προωθητή, δεδομένα αυτοματισμού, πηδάλια, ανοίγματα κύτους, στεγανές και πυροσβεστικές πόρτες, ραδιοεπικοινωνίες VHF, συνομιλίες από την γέφυρα, ραντάρ, AIS και ECDIS, σημαντικούς συναγερμούς και σήματα από τους αισθητήρες (όπως βάθος, άνεμος, ταχύτητα, θέση, πορεία, κ.λπ.). (Sea News, 2020)

Η κατανόηση των εσωτερικών στοιχείων ενός VDR μπορεί να παρέχει στις αρχές ή σε τρίτους πολύτιμες πληροφορίες κατά τη διεξαγωγή εγκληματολογικών ερευνών. Ωστόσο, η δυνατότητα παραποίησης των δεδομένων μπορεί επίσης να επιτρέψει επιθέσεις. Στις 9 Δεκεμβρίου του 2015 ο Ruben Santamara δημοσίευσε μια έρευνά του σχετικά με την επίθεση σε ένα σύστημα καταγραφής δεδομένων ταξιδιού. Εκεί αναφέρει ότι δεν είχε πρόσβαση στο υλικό κομμάτι του συστήματος αλλά κατάφερε να βρει τόσο υλικολογισμικό (firmware) όσο και λογισμικό για το στόχο του.



Εικόνα 40 - Τυπική αρχιτεκτονική ενός συστήματος VR-3000 (Santamarta, 2022)

Οι λεπτομέρειες που παρουσιάζονται παρακάτω βασίζονται αποκλειστικά σε στατική ανάλυση και εξομοίωση QEMU[30] σε λειτουργία χρήστη. Μέσα στη μονάδα συλλογής δεδομένων (Data Collecting Unit - DCU) υπάρχει μια μηχανή Linux με πολλαπλές διεπαφές επικοινωνίας, όπως USB, IEEE1394 και LAN, και ένας σκληρός δίσκος αντιγράφου ασφαλείας που αναπαράγει εν μέρει τα δεδομένα που είναι αποθηκευμένα στη μονάδα εγγραφής δεδομένων (Data Recording Unit -DRU). Το DRU προστατεύεται από επιθέσεις προκειμένου να επιβιώσει σε περίπτωση ατυχήματος. Περιέχει επίσης έναν δίσκο Flash για αποθήκευση δεδομένων για περίοδο 12 ωρών. Αυτή η μονάδα αποθηκεύει όλα τα απαραίτητα δεδομένα πλοήγησης και κατάστασης.

Αφού πέρασαν μερικές ώρες αντιστρέφοντας τα διαφορετικά δυαδικά αρχεία, ήταν σαφές ότι η ασφάλεια δεν είναι ένα από τα δυνατά σημεία αυτού του εξοπλισμού. Πολλές υπηρεσίες είναι επιρρεπείς σε υπερχειλίσεις buffer και τρωτά σημεία εγχύσεις εντολών (command injection). Ο μηχανισμός ενημέρωσης υλικολογισμικού είναι ελαττωματικός. Η κρυπτογράφηση είναι αδύναμη,

[30] Το QEMU είναι ένας εξομοιωτής επεξεργαστή και υποστηρίζει εξομοίωση ARM, PowerPC, SPARC, x86, x86-64 και άλλων. Έχει δύο τρόπους λειτουργίας: a) λειτουργία χρήστη: όπου μπορεί να εκκινήσει διεργασίες Linux που έχουν μεταγλωττιστεί για μια CPU σε μια άλλη CPU, μεταφράζοντας τα syscalls on the fly, b) και πλήρη εξομοίωση συστήματος: όπου προσομοιώνει ένα πλήρες σύστημα (εικονική μηχανή), που περιλαμβάνει έναν επεξεργαστή και διάφορα περιφερειακά όπως δίσκο, ελεγκτή ethernet κ.λπ. (CNBlogs, 2022)

και βασικά, σχεδόν ολόκληρο το σχέδιο θα πρέπει να θεωρείται τρωτό. Ψάχνοντας περαιτέρω στις δυαδικές υπηρεσίες, βρέθηκε μια ευπάθεια που επιτρέπει σε μη επαληθευμένους εισβολείς με απομακρυσμένη πρόσβαση στο VR-3000[31] να εκτελούν αυθαίρετες εντολές με δικαιώματα root. Αυτό μπορεί να χρησιμοποιηθεί για την πλήρη παραβίαση της συσκευής.

Ωστόσο, ο συμβιβασμός του DCU δεν αρκεί για να καλύψει τα ίχνη ενός εισβολέα, καθώς περιέχει μόνο έναν εφεδρικό σκληρό δίσκο, ο οποίος δεν έχει σχεδιαστεί να επιβιώνει σε ακραίες συνθήκες. Η βασική συσκευή σε αυτό το σενάριο κατά της εγκληματολογίας είναι το DRU. Η προνομιακή θέση που αποκτήθηκε με την παραβίαση του DCU θα επέτρεπε στους εισβολείς να τροποποιήσουν/διαγράψουν δεδομένα και στο DRU, καθώς αυτή η μονάδα συνδέεται απευθείας μέσω μιας διεπαφής IEEE1394. Επίσης, κακόβουλοι εισβολείς θα μπορούσαν να το χρησιμοποιήσουν για να κατασκοπεύσουν το πλήρωμα ενός σκάφους, καθώς τα συστήματα αυτά συνδέονται απευθείας με μικρόφωνα που βρίσκονται, τουλάχιστον, στη γέφυρα. (Santamarta, 2022)

[31] Το Furuno VR3000 είναι ένα πλήρες σύστημα Voyage Data Recorder (VDR) και συμμορφώνεται πλήρως με τις προδιαγραφές απόδοσης του IMO και τις απαιτήσεις μεταφοράς

Κεφάλαιο 3: Περιστατικά στο Ναυτιλιακό Τομέα

3.1 Εισαγωγικό Σημείωμα

Η ραγδαία τεχνολογική ανάπτυξη, η είσοδος νέων εφαρμογών διαχείρισης πληροφοριών και μέσων επικοινωνίας, καθώς και η αύξηση των ολοκληρωμένων σκαφών (integrated vessels[32]) στο ναυτιλιακό τομέα, πέρα από την αξιοσημείωτη συμβολή τους στην ανάπτυξη των θαλάσσιων μεταφορών, συνδέονται ταυτόχρονα με την εμφάνιση νέων απειλών, τις λεγόμενες κυβερνοαπειλές. Οι κακόβουλες επιθέσεις σε διάφορα πληροφοριακά συστήματα των ναυτιλιακών εταιρειών, των εμπορικών πλοίων και των λιμενικών εγκαταστάσεων γίνονται ολοένα και πιο συχνές.

Information Technology (IT)	Operation Technology (OT)
Administration, accounts, crew lists, etc.	PLCs, SCADA
Planned maintenance	On-board measurement & control
Spares management & requisitioning	ECDIS, GPS, Dynamic positioning
Electronic manuals and certificates	Remote support for engines
Permits to work	Data loggers
Charter party, notice of readiness, etc.	Engine and cargo control
At Risk:	At Risk:
Mainly finance & reputation	Life, property & environment as well as finance & reputation

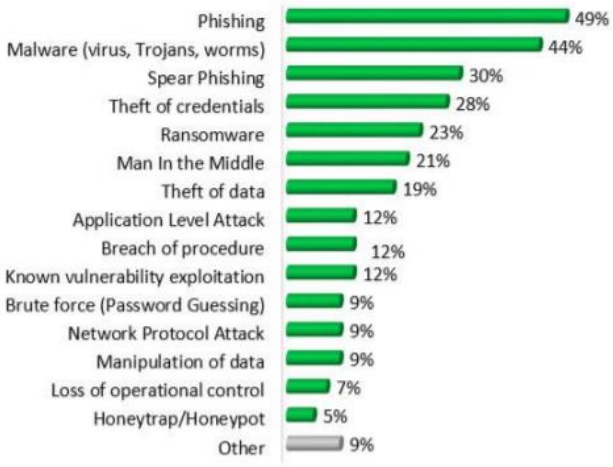
Εικόνα 41 - Τεχνολογία πληροφορικής και λειτουργίας (Advanced Polymer Coatings, 2022)

Κατά συνέπεια η ομαλή και ασφαλής λειτουργία τους αντιμετωπίζει πολύ σοβαρούς κινδύνους, γεγονός που με τη σειρά του μπορεί να επηρεάσει την πιθανότητα ναύλωσης προκαλώντας σοβαρές οικονομικές απώλειες στα «ψηφιακά» θύματα και όχι μόνο (Η χρήση και η αξιοποίηση του Διαδικτύου και των εφαρμογών του στη σύγχρονη Εμπορική Ναυτιλία, 2017). Απειλές μπορεί να προκύψουν από εσφαλμένη ενσωμάτωση και αλληλεπίδραση των κυβερνοσυστημάτων, από ενημερώσεις αυτών ή από επιθέσεις εξωτερικών πηγών που δεν είναι πάντα ανιχνεύσιμες. Υπάρχουν επίσης ενδείξεις πως και οι πειρατές μπορεί να εκμεταλλεύονται ευπάθειες και κενά στην Κυβερνοασφάλεια των πλοίων στοχεύοντας σε συγκεκριμένα φορτία.

Εικόνα 42 - Συμβάντα στον ναυτιλιακό κλάδο (DNV, 2021)

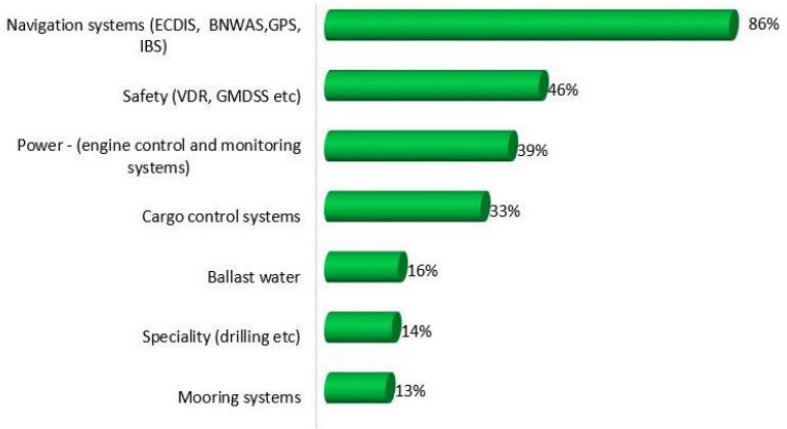
32 Ολοκληρωμένο σκάφος είναι το πλοίο που έχει ένα ολοκληρωμένο σύστημα γέφυρας (Integrated bridge system) που είναι ένα είδος συστήματος διαχείρισης πλοήγησης συνδέοντας διάφορα συστήματα για να παρέχει όλες τις λεπτομέρειες σχετικά με την πλοήγηση του πλοίου σε ένα σημείο. Συνήθως αποτελείτε από: Αυτόματο πιλότο, Διπλό ραντάρ / ARPA, Gyro, Συστήματα στερέωσης θέσης, Διπλή ρύθμιση ECDIS, Οθόνη Conning, Σύστημα διανομής ισχύος, Τιμόνι, GMDSS (marine insight, 2021)

Τον Αύγουστο 2018 η IHS Markit[33] δημοσίευσε μια έρευνα σχετικά με την κατάσταση στην Ναυτιλία με τα αποτελέσματα που έχουν ληφθεί να προκύπτουν από ένα ευρύ φάσμα μελέτης. Διερευνώνται τα πιο ευάλωτα συστήματα, τα πρότυπα - κατευθυντήριες γραμμές που λαμβάνουν υπόψη τους και τα ποσά που έχουν δαπανηθεί στην κυβερνοασφάλεια. Ακόμη, ερωτήθηκαν αν τυχόν έχουν πέσει θύμα, αν το αντιλήφθηκαν και ποιο το κόστος από την εν λόγω επίθεση. Στη συνέχεια απεικονίζονται οι πιο συχνές επιθέσεις με βάση την έρευνα.



Εικόνα 43 - Πληροφορίες για την φύση των περιστατικών από τους ερωτηθέντες της έρευνας. (IHS Markit | 2018 Maritime Cyber Security Results, 2021)

Το ερωτηματολόγιο αυτό απαντήθηκε από 350 άτομα τα οποία εργάζονται στον ναυτιλιακό κλάδο. Κάποια από τα ευρήματα ήταν ότι το 27% δεν είχε λάβει ποτέ εκπαίδευση για τους κινδύνους που εγκυμονούν και για τους τρόπους προστασίας από ένα πιθανό χτύπημα. Παράλληλα, οι μισοί περίπου από τους ερωτηθέντες είχαν σχέδιο αντιμετώπισης ή αποκατάστασης από κυβερνοεπίθεση. Επιπλέον, το 49% των ερωτηθέντων ανέφεραν διακοπή της υπηρεσίας ως αποτέλεσμα της επίθεσης και το 26% υπέστη οικονομικές ζημιές. Το ποσό των απωλειών που προέκυψαν από το συμβάν κυμαίνεται από μερικές χιλιάδες μέχρι και εκατομμύρια δολάρια. Εκτός, από αυτά σημειώθηκαν ότι κάποιοι υπέστησαν πλήξη στο κύρος, κλοπή φορτίου αλλά και απώλεια συμβολαίων. Τέλος, μόνο το 16% είχε ασφάλεια για να καλύψει την παραβίαση ενώ το 84% δεν την είχε καλύψει. (IHS Markit | 2018 Maritime Cyber Security Results, 2021)



Εικόνα 44 - Περιοχές που θεωρούνται πιο ευάλωτες σε επιθέσεις (IHS Markit | 2018 Maritime Cyber Security Results, 2021)

33 Η IHS Markit Ltd είναι ένας αμερικανό-βρετανικός πάροχος πληροφοριών με έδρα το Λονδίνο (wikipedia, 2021)

Σε αυτό το κεφάλαιο θα αναφέρουμε ορισμένα περιστατικά επίθεσης που συνέβησαν στην ναυτιλιακή βιομηχανία όσον αφορά τον κυβερνοχώρο. Πέρα όμως από τα ιστορικά δεδομένα για τα οποία υπάρχουν αποδείξεις ότι έλαβαν χώρα, θα αναφερθούν και σενάρια πιθανής επίθεσης. Στη δεύτερη περίπτωση, τα στοιχεία συλλέγονται από ορισμένα εργαλεία που αναλύουν την τρωτότητα του συστήματος.

System	Threat	Impact	Reference
AIS	AIS malfunction, jamming, spoofing	Not mentioned	Kessler et al. [16]
	Spoofing, replay attack, frequency hopping attack	Not mentioned	Dumbala [28]
	Designed without security, malicious version, malware	Hijacking, smuggling, theft	Jones, K.D. et al. [29]
	False signals, represent nonexistent emergencies	Collisions, pollution, grounding, interruption of port operations	Alcaide and Llave [30]
ECDIS	Physical access Internet connection establishment Authorized access Operating system support and security patches Operating system configuration etc.	Provides physical/logical access Exploitation of well-known vulnerabilities Reduces performance and opens backdoor	Svilicic et al. [7]
	Vulnerable versions of SMB and Remote Desktop Protocol (RDP)	Infection and dysfunctionality of all ECDIS stations in the network	Svilicic et al. [19]
	Outdated Apache web server Vulnerable version of SMB	Gain unauthorized access Remote attacker	Svilicic et al. [20]
	Vulnerable versions of SMB and Remote Desktop Protocol (RDP)	Execute arbitrary code without authentication Disclose sensitive information	Svilicic et al. [21]
	Designed without security, malicious version, malware	Hijacking, smuggling, theft	Jones, K.D. et al. [29]
	GNS spoofing by malware	Sails to different coordinates Crash the operator station	Lund et al. [18]
	Virus, DoS, spoofing	Not mentioned	Dumbala [28]
SATCOM	Backdoors Hardcoded credentials Insecure protocols Undocumented protocols Password reset weaknesses	Install malicious firmware Execute arbitrary code	Santamarta [4]
	Unencrypted protocols	Disclose sensitive information	Pavur et al. [25]
	Default credentials, not updated software, etc.	Not mentioned	Dumbala [28]
	Cyberattack by hostile states	Disclose sensitive information	Haynes [31]
BWMS	Phishing emails, malware	Ransomware, false command	Dumbala [28]
	Cyberattack by hostile states	Sinking of the ship	Haynes [31]
	Designed without security, malicious version, malware	Hijacking, smuggling, theft	Jones, K.D et al. [29]
other	NMEA: unencrypted message DoS attacks	Injection of fake messages System shutdown	Caprolu et al. [24]
	Inaccurate ENC file	Sinking of the ship	Awan and Ghamdi [23]
	Default account and password	Elevation privilege	Tierney et al. [26]
	Default password and the passenger's Wi-Fi	Access system inside the ship Information intercept	Tierney et al. [27]
	Described the risk levels of these attack surfaces using risk assessment methodologies		Hyra et al. [8]
	Proposed a risk assessment method for ship control systems using fuzzy sets and attack trees		Shang et al. [22]

Εικόνα 45 - Πίνακας αποτελεσμάτων ερευνών (Jo, Choi, You, Cha, & Lee, 2022)

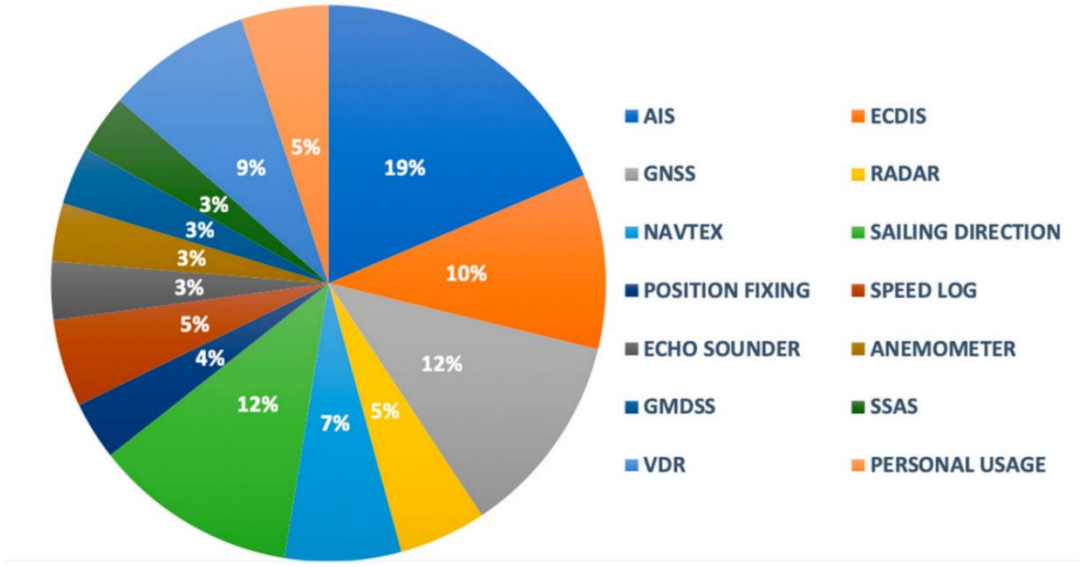
Ένα τέτοιο εργαλείο, όπως έχουμε αναφέρει σε προηγούμενη ενότητα είναι το MITRE ATT&CK, που στην ουσία είναι μια βάση δεδομένων απειλών ασφαλείας που αναλύει τον τρόπο με τον οποίο ένας αντίπαλος εισβάλλει και εξαπλώνεται μέσω συστημάτων υπολογιστών,

εστιάζοντας σε δεδομένα που εντοπίζονται σε πραγματικές παραβιάσεις. Τα δεδομένα περιγράφονται από τα τρία στοιχεία, δηλαδή Τακτικές, Τεχνικές (552 στο σύνολο μαζί με τις υπό τεχνικές) και Διαδικασίες, τα οποία επιτρέπουν την κατασκευή άμυνας σε βάθος (Defense in Depth -DiD).

Η έρευνα που διεξάχθηκε παρουσίασε απειλές ανά σύστημα και συνέπειες όπου υπήρξαν όπως φαίνεται και στην εικόνα 44. Ένα από τα ευρήματα ήταν τα απαρχαιωμένα λογισμικά και οι ανασφαλείς συνδέσεις δικτύου (Jones et al). Αυτό γιατί πολλά πλοία κατασκευάστηκαν πριν υπάρξει η ανησυχία για την κυβερνοασφάλεια. Το παλαιότερο λογισμικό, όμως, είναι πιο επιρρεπές σε ευπάθειες και ορισμένα συστήματα έχουν βρεθεί ότι δεν διαθέτουν ενημερώσεις κώδικα ασφαλείας. (Jo, Choi, You, Cha, & Lee, 2022) Ορισμένες ενσωματωμένες συσκευές, για παράδειγμα, εξακολουθούν να εκτελούν Windows XP και Windows NT και οι μετατροπείς σπάνια αλλάζουν τους κωδικούς πρόσβασης διαχειριστή. Η συνδεσιμότητα που έχουν όλα τα συστήματα μεταξύ τους (NMEA) καθιστά τα κρίσιμα αυτά συστήματα ελέγχου εύκολα να παραβιαστούν. (Threat Post, 2022)

3.2 Περιστατικά στα συστήματα γέφυρας/πλοήγησης

Σχετικά με τα **ολοκληρωμένα συστήματα πλοήγησης (Integrated Navigational System)**, ένα άλλο εργαλείο που αναπτύχθηκε για την ανάλυση επιθέσεων στον κυβερνοχώρο είναι η αλυσίδα θανάτωσης εισβολής (intrusion kill chain). Αυτό παρέχει ένα μοντέλο που περιγράφει τη διαδικασία εργασίας ενός εισβολέα που επιδιώκει να διεισδύσει στο σύστημα υπολογιστή σε επτά φάσεις: αναγνώριση (reconnaissance), οπλισμός (weaponization), παράδοση (delivery), εκμετάλλευση (exploitation), εγκατάσταση (installation), διοίκηση και έλεγχος (command & control) και ενέργειες (actions). Έτσι, ενώ το μοντέλο αναπτύσσεται ως βοήθημα στον αμυνόμενο, χρησιμοποιείται και σαν σημείο διαδρομής του επιτιθέμενου. Τέλος, προσδιορίζει και τους πόρους που απαιτούνται για την ανάπτυξη της επίθεσης (Lund, 2022).



Εικόνα 46 - Σύνθεση συλλεγόμενων στοιχείων τρωτότητας. (Ghamdi, 2022)

Στο παραπάνω διάγραμμα φαίνονται τα πιο πιθανά τρωτά σημεία στη γέφυρα ενός πλοίου. Ο Staphan Gerling στο Area41 Security Conference ανέφερε πως η σύνδεση στο διαδίκτυο γίνεται μέσω WiFi, GSM[34] και μέσω δορυφόρου (SAT). Η επίθεση στο πλοίο μπορεί να γίνει στο Internet

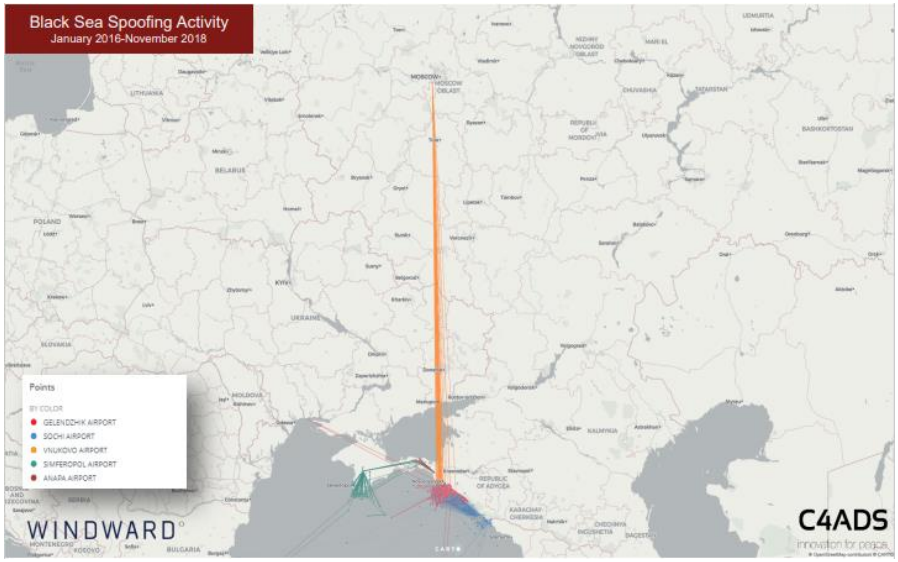
[34] Global System for Mobile communications (Παγκόσμιο Σύστημα Κινητών Επικοινωνιών), είναι ένα κοινό Ευρωπαϊκό ψηφιακό σύστημα κινητής τηλεφωνίας. (Wikipedia, 2020)

Router, στους υπολογιστές του και στις κινητές συσκευές, όπως tablet, τηλέφωνα, στέλνοντας phishing emails και επηρεάζοντας το σύστημα με κακόβουλο λογισμικό και στη συνέχεια αποκτώντας απομακρυσμένη πρόσβαση. Αφού γίνει αυτό τότε είναι δυνατόν να βρεθούν οι πύλες (gateways) που έχουν πρόσβαση στο NMEA network, συνεπώς και σε όλα τα όργανα που αυτό συνδέει όπως είναι ο αυτόματος πιλότος, Sonar, Radar, GPS, AIS και άλλα. (Area41, 2020)

3.2.1 GNSS

Τον Ιούνιο του 2017, ένα συμβάν πλαστογράφησης που αφορούσε σχεδόν 20 πλοία έλαβε χώρα στη Μαύρη Θάλασσα. Σε αυτό το περιστατικό, ο πλοίαρχος του ATRIA, ένα δεξαμενόπλοιο 37.500 τόνων, είχε αποδείξεις για δραστηριότητες πλαστογράφησης GNSS. Ενώ βρισκόταν στα ανοικτά των ακτών του λιμανιού Gelendzhik της Ρωσίας, τα ενσωματωμένα συστήματα πλοήγησης του πλοίου έδειξαν ότι βρισκόταν στη μέση του αεροδρομίου Gelendzhik, περίπου 20 χιλιόμετρα μακριά. Τα συστήματα πλοήγησης από τουλάχιστον 20 κοντινά πλοία έδειξαν ότι βρίσκονταν όλα στην ίδια τοποθεσία.

Κατά συνέπεια, πολλά σκάφη σήμαναν συναγερμούς καθώς έδειχναν επικείμενες συγκρούσεις. Υπήρχαν ευρέως εικασίες εκείνη την εποχή ότι το συμβάν πλαστογράφησης της Μαύρης Θάλασσας οφειλόταν σε ρωσικό ηλεκτρονικό πόλεμο. Μεταγενέστερες αναφορές έδειξαν ότι αυτό το περιστατικό ήταν μέρος ενός ευρύτερου σχεδίου παρεμβολών GNSS που τοποθετούσε πλοία σε πολλά αεροδρόμια, συμπεριλαμβανομένων του Sochi, St. Petersburg, και του Vladivostok.



Εικόνα 47 - Black sea Spoofing Activity (Board, 2022)

Στις 15 Μαΐου 2018, όταν ο Ρώσος Πρόεδρος Βλαντιμίρ Πούτιν διέσχιζε τη γέφυρα του στενού Kerch από τη Ρωσία στην Κριμαία, τα συστήματα δορυφορικής πλοήγησης στα δωμάτια ελέγχου περισσότερων από 24 πλοίων που ήταν αγκυροβολημένα κοντά άρχισαν ξαφνικά να εμφανίζουν ψευδείς πληροφορίες σχετικά με τη θέση τους. Τα συστήματα τους έδειχναν ότι ήταν αγκυροβολημένα σε απόσταση μεγαλύτερη των 65 χιλιομέτρων - στο αεροδρόμιο Anapa. Αυτό δεν ήταν τυχαίο σφάλμα, σύμφωνα με το Κέντρο Προηγμένων Αμυντικών Μελετών, γνωστό και ως C4ADS. Γνωστοποίησε πως ήταν ένα εσκεμμένο σχέδιο για να δυσκολέψει οποιονδήποτε στην παρακολούθηση ή στην πλοήγηση κοντά στον Πούτιν. (Insider, 2022)

Εικόνα 49 - GNSS Spoofing (Insider, 2022)

Παρεμβολές GNSS, απώλεια σήματος και μειωμένη ακρίβεια θέσης στην Ανατολική Μεσόγειο αναφέρθηκαν για πρώτη φορά από το 2018 και συνεχίζουν μέχρι σήμερα να επηρεάζουν περιοχές από την Κύπρο και τις ακτές της Αιγύπτου μέχρι το Ισραήλ και τη Σαουδική Αραβία. Ο IMO, η USCG, η Ναυτιλιακή Διοίκηση των ΗΠΑ (MARAD) και άλλες ναυτιλιακές ομάδες έχουν εκδώσει πολλαπλές συμβουλές σχετικά με αυτά τα επεισόδια, τα οποία φαίνεται να συνεχίζονται αμείωτα.

Location and Date	Spoofing Incidents Description
The Southern Ocean, 2008–2018	To disguise her illegal fishing operations, m/v Andrej Longov/Sea Breez 1/Ayda/STS-50 committed identity fraud by repeatedly falsifying her registry, producing multiple fake signals, and appearing in nearly 100 different locations simultaneously.
Gulf of Oman/Malaysia, September 2013	M/v Ramtin was involved in "spoofing" by falsely transmitting her AIS identity during suspicious activities and deceiving authorities at Karachi port under the name of m/v Hamoda.
Ten global locations connected to one of the superpower states, 2016–2019	9883 suspected spoofing incidents.
The Black Sea, June 2017	Vessel tracking systems placed many vessels near Novorossiysk Commercial Sea Port in the nonsensical location, on the Gelendzhik Airport.
The East China Sea, 28 October 2018	M/v Yuk Tung was involved in "spoofing" by falsely transmitting its AIS identity in a suspicious ship-to-ship transfer and deceiving authorities under the name of m/v Hika, which was anchored in the Gulf of Guinea, more than 7000 m away.
Point Reyes in northern California, August 2018–June 2019	Ships thousands of miles at sea mysteriously reported GPS positions in ring patterns off the coast of San Francisco.
Eastern Mediterranean and the Red Sea, 2018–2019	Signal interference, loss of erratic AIS/GPS signals.
Strait of Hormuz, July 2019	A British oil tanker, the Stena Impero, was seized by Iranian forces after the ship was spoofed into changing course into Iranian waters.
Ningbo (China)-Nampo (Democratic People's Republic of Korea), July–November 2019	The m/v Fu Xing 12 manipulated its identity by employing two AIS on board and using four different ship names to disguise its operations in delivering illegal coal and other resources.
Port of Shanghai, 2018–2019	Fake signals caused ships to appear to be moving in ring patterns at short intervals.
Ponce De Leon Inlet, Florida, 2020	Four visual AtoNs appeared on the map based on fake AIS messages.
Elba Island, 3 December 2019	Deliberate spoofing of the vast number of artificial AIS targets temporarily affected the navigation of ships.
Galapagos, July 2020	One of the world's largest fleets of fishing nations misreported its location (approximately 10,000 km from its observed location) to conceal illegal fishing activities in the exclusive economic zone (EEZ) around the Galápagos Islands.

Εικόνα 48 – Επισκόπηση γεγονότων πλαστογράφησης GNSS που επηρέασαν τη θαλάσσια κυκλοφορία μεταξύ των ετών 2008 και 2020 (Andrej Androjna, 2022)

Τον Ιούλιο του 2019 κατασχέθηκε από τις ιρανικές δυνάμεις το πλοίο (φορτίο και πλήρωμα) STENA IMPERO στο Στενό του Ορμούζ αφού εξαπατήθηκε για να αλλάξει την πορεία του. Το πετρελαιοφόρο υπό σημαία Ηνωμένου Βασιλείου κατασχέθηκε βάσει του ισχυρισμού ότι το πλοίο βρισκόταν σε λάθος κανάλι κατά την έξοδο από το Στενό παραβιάζοντας το Διεθνές Δίκαιο. Μια δορυφορική διαδρομή του σκάφους δείχνει ότι το πλοίο προχωρούσε κανονικά μέσω του Στενού προτού κάνει μια ξαφνική στροφή προς τα χωρικά ύδατα του Ιράν (Andrej Androjna, 2022).

Πιστεύεται επίσης ότι το Ιράν κατέλαβε το δεξαμενόπλοιο ως αντίποινα για την κατάσχεση ενός πετρελαιοφόρου τους από το Ηνωμένο Βασίλειο στο Γιβραλτάρ λίγες εβδομάδες νωρίτερα λόγω των παραβιάσεων των κυρώσεων της Ευρωπαϊκής Ένωσης (ΕΕ), και της γενικότερης κλιμάκωσης που υπήρχε μεταξύ των δύο χωρών. Το ιρανικό πρακτορείο ειδήσεων Fars, από την

άλλη, ανέφερε ότι το Stena Impero συγκρούστηκε με ένα ιρανικό αλιευτικό σκάφος, του οποίου το σήμα κινδύνου αγνοήθηκε. Επίσης, ο Οργανισμός Λιμένων και Ναυτιλίας του Ιράν (PMO) σημείωσε ότι το πλοίο απελευθέρωσε υπολείμματα πετρελαίου από τις δεξαμενές του. (safety4sea, 2022)

3.2.2 GPS

Η επίθεση στο στίγμα παγκόσμιας θέσης (GPS) μπορεί να γίνει με δύο διαφορετικούς τρόπους, αφενός με παρεμβολή στο σήμα ή παρακώλυση επικοινωνίας (jamming[35]) και αφετέρου με πλαστογράφηση (spoofing[36]). Αυτά έχουν ως σκοπό την παραπλάνηση της γεωγραφικής θέσης. Βέβαια μία επίθεση πλαστογράφησης στο GPS ενός πλοίου είναι πιο δύσκολη από την παρεμβολή, εφόσον συνήθως απαιτείται να γίνει κοντά στο πλοίο προκειμένου τα ψεύτικα σήματα να γίνουν αποδεκτά ως αληθινά. (Area41, 2020) Από την άλλην όμως, οι Lund et al. περιέγραψαν ένα σενάριο κυβερνοεπίθεσης όπου το κακόβουλο λογισμικό τροποποιεί τις συντεταγμένες του GPS με μια επίθεση MiTM. Η επίθεση προκαλεί τη συντριβή του συστήματος σε μια «μπλε οθόνη» ή την κατεύθυνση του πλοίου σε διαφορετικές συντεταγμένες. (Jo, Choi, You, Cha, & Lee, 2022)

Ένα παράδειγμα πλαστογράφησης (spoofing) με χαρακτήρα άσκησης είναι αυτό του Πανεπιστήμιου του Τέξας. Τον Ιούλιο του 2013 το πανεπιστήμιο, με εξοπλισμό 3,000$ κατάφερε και πήρε τον έλεγχο της πλοήγησης ενός mega-yacht αξίας $80 εκατ., με εγκατεστημένα σύγχρονα ψηφιακά συστήματα και άρτια εκπαιδευμένο πλήρωμα. Για την εν λόγω άσκηση ήταν ενήμεροι μόνο ο πλοίαρχος και η πλοιοκτήτρια εταιρία. Οι «εισβολείς» έστελναν δικά τους στίγματα στο σύστημα αφού κατάφεραν να παρέμβουν στις κεραίες GPS, με αποτέλεσμα να αλλάξουν την πορεία του yacht με τα συστήματα να μην δείχνουν κάποια παρέκκλιση από την πορεία που είχαν ορίσει. (Isalos,net, 2020)

Πιο συγκεκριμένα τον Ιούνιο, το γιοτ, που ονομάζεται White Rose of Drachs, ήταν να ταξιδέψει από το Μονακό στη Ρόδο. Όταν λοιπόν το γιοτ έπλεε στα διεθνή ύδατα, περίπου 30 μίλια από τις ακτές της Ιταλίας, οι φοιτητές Jahshan Bhatti και Ken Pesyna (με επικεφαλής τον επίκουρο καθηγητή Todd Humphreys) μετέδωσαν ένα αχνό σήμα GPS από τη συσκευή πλαστογράφησης προς τις δύο κεραίες GPS του πλοίου. Τα πλαστά σήματα της ομάδας υπερίσχυσαν των αυθεντικών σημάτων μέχρι που αποκτήσαν τον έλεγχο του συστήματος πλοήγησης του πλοίου. Σε αντίθεση με το μπλοκάρισμα (jamming) του σήματος GPS, η πλαστογράφηση δεν ενεργοποιεί συναγερμούς στον εξοπλισμό.

Μόλις αποκτήθηκε ο έλεγχος, η στρατηγική ήταν να εξαναγκάσουν το πλοίο σε μια νέα διαδρομή χρησιμοποιώντας λεπτούς ελιγμούς που ανακατεύθυναν το γιοτ μερικές μοίρες από την αρχική του πορεία. Μόλις αναφέρθηκε μια ασυμφωνία τοποθεσίας από το σύστημα πλοήγησης του πλοίου, το πλήρωμα ξεκίνησε μια διόρθωση πορείας. Στην πραγματικότητα, κάθε διόρθωση πορείας έβγαζε το πλοίο εκτός από τη γραμμή πορείας του. Μετά από αρκετούς τέτοιους ελιγμούς, το γιοτ είχε εξαπατηθεί σε μια παράλληλη τροχιά εκατοντάδες μέτρα από την προβλεπόμενη, η ομάδα είχε πλαστογραφήσει με επιτυχία το πλοίο. (The University of Texas, 2020)

Το 2019 μια νέα έρευνα έδειξε ότι χιλιάδες πλοία στη Σαγκάη, πέφτουν θύματα πλαστογράφησης των συστημάτων GPS. Κανείς δεν ξέρει ποιος κρύβεται πίσω από αυτή την πλαστογράφηση, ή ποιος μπορεί να είναι ο τελικός σκοπός της. Μία πιθανότητα είναι η χρήση από λαθρέμπορες, και μια άλλη ότι το ίδιο το κινεζικό κράτος που δοκιμάζει ένα νέο ηλεκτρονικό όπλο ίσως για ενδεχόμενη χρήση σε αμφισβητούμενες περιοχές της Θάλασσας της Νότιας Κίνας.

---

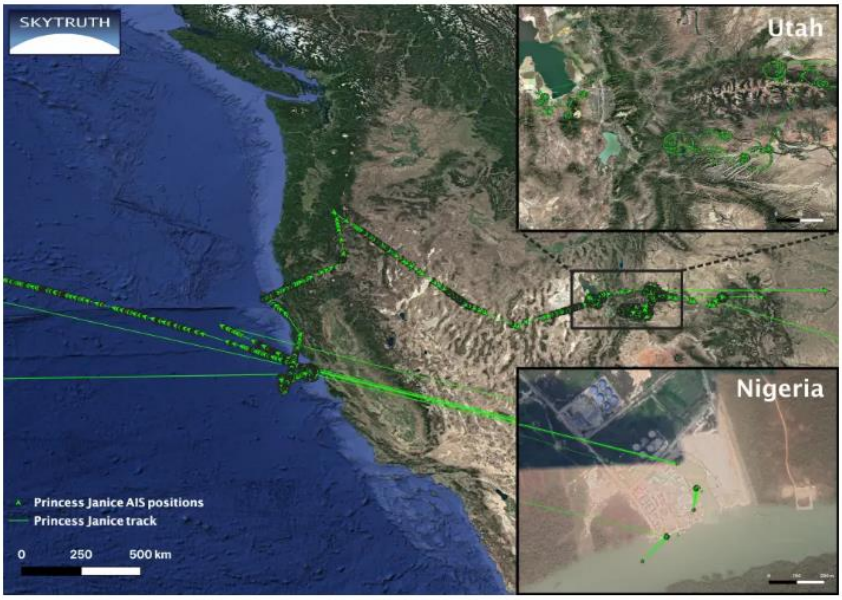
[35] Είναι επίθεση που σκόπιμα ή μη προκαλείται στο σήμα του πομπού, του δέκτη ή του σημείου ασύρματης πρόσβασης από παρεμβολές ή θορύβους. (Wikipedia, 2020)

[36] Είναι μια τεχνική προκειμένου να αποκτηθεί παράνομη πρόσβαση στους υπολογιστές με τη δημιουργία πακέτων TCP/IP, χρησιμοποιώντας τη διεύθυνση και τα στοιχεία κάποιου άλλου αξιόπιστου. Οι δρομολογητές (routers) χρησιμοποιούν την διεύθυνση της IP προορισμού (destination IP) ώστε να διαδώσουν τα πακέτα μέσω διαδικτύου αγνοώντας - αλλάζοντας εικονικά την διεύθυνση της IP πηγής (source IP). (Wikipedia, 2020)

Τον Ιούλιο του 2019, το πλοίο μεταφοράς εμπορευματοκιβωτίων MV Manukai έφτανε στο λιμάνι της Σαγκάης, στο πολυσύχναστο παραπόταμο του Yangtze τον Huangpu. Καθώς ο καπετάνιος του παρακολουθούσε τις οθόνες πλοήγησής του παρατήρησε ένα άλλο πλοίο στο ίδιο κανάλι να κινείται με περίπου επτά κόμβους. Ξαφνικά, το άλλο πλοίο εξαφανίστηκε από την οθόνη και λίγα λεπτά αργότερα, φαινόταν να ήταν πίσω στην αποβάθρα. Αυτό συνέβη κάμποσες φορές, και συγκλονισμένος ο καπετάνιος έλεγξε οπτικά την θέση του άλλου πλοίου που ήταν ακίνητο στην αποβάθρα όλη την ώρα.

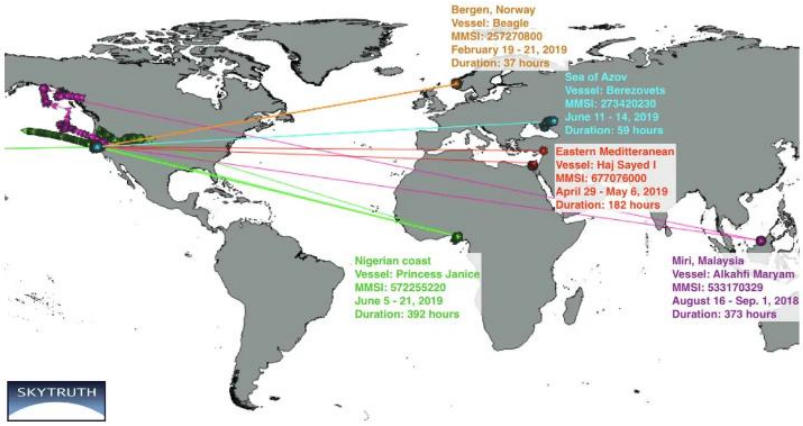
Όταν ήρθε η ώρα για το Manukai να κατευθυνθεί προς το δικό του αγκυροβόλιο, η γέφυρα άρχισε να αντηχεί πολλαπλούς συναγερμούς και οι μονάδες GPS του πλοίου είχαν χάσει τα σήματά τους, ο αναμεταδότης AIS του είχε αποτύχει και ένα τελευταίο σύστημα έκτακτης ανάγκης που βασιζόταν επίσης στο GPS δεν μπορούσε να διορθωθεί. Αν και το Manukai τελικά ελλιμενίστηκε με ασφάλεια, ο καπετάνιος υπέβαλε μια αναφορά στο Κέντρο Πλοήγησης της Ακτοφυλακής των ΗΠΑ. Το ίδιο συνέβαινε και στο γειτονικό του πλοίο - η πραγματική τους θέση και ταχύτητα είχαν αντικατασταθεί από ψευδείς συντεταγμένες. Αυτό μπορεί να προκαλέσει λάθη ναυσιπλοΐας και γενικά συγκρούσεις ή προσαράξεις.

Την ίδια μέρα που το Manukai αντιμετώπισε δυσκολίες καταγράφηκε έντονη παρέμβαση όταν σχεδόν 300 πλοία πλαστογραφήθηκαν. Τα δεδομένα της Σαγκάης που εξέτασε το C4ADS διαπίστωσαν ότι ήταν διαφορετική περίπτωση από το hacking που παρατηρήθηκε στα ρωσικά ύδατα, όπου τα πλοία ήταν όλα πλαστογραφημένα σε ένα μόνο σημείο. Πιο συγκεκριμένα, έδειξαν τα πλοία να «πηδούν» κάθε λίγα λεπτά σε διαφορετικές τοποθεσίες σε δακτυλίους στην ανατολική όχθη του Huangpu. Οι επιθέσεις αυτές επηρέαζαν όλες τις συσκευές GPS, όχι των πλοίων. (MIT Technology Review, 2022)



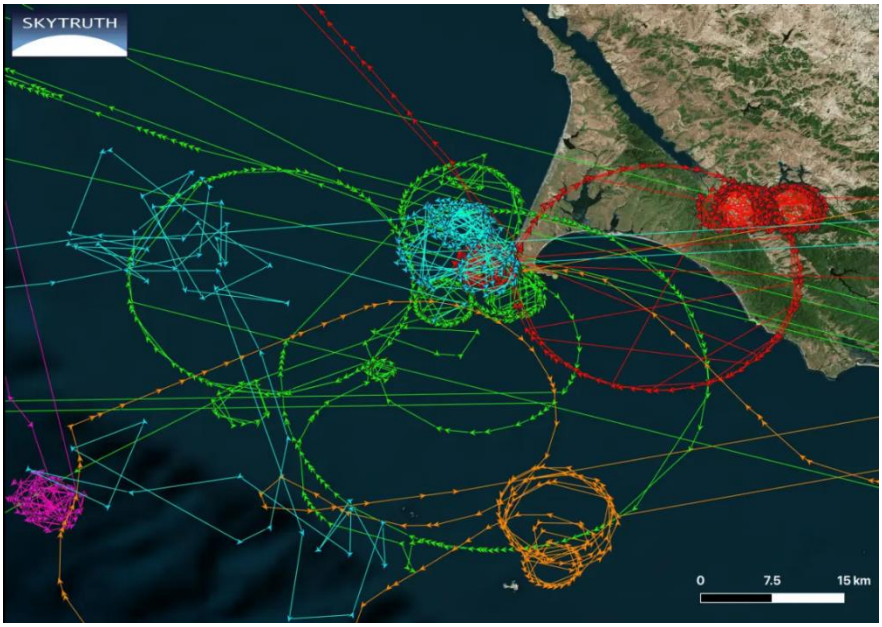
Εικόνα 50 - Princess Janice από το Point Reyes στην ενδοχώρα, κυκλικές κινήσεις στη Γιούτα και πίσω στη Νιγηρία. (BigThink, 2022)

Το ίδιο πράγμα συνέβη στις 5 Ιουνίου 2019, όταν το νιγηριανό σκάφος Princess Janice έκανε ένα «αδύνατο» ταξίδι. Αντί να μεταφέρει πληρώματα από και προς τις εξέδρες άντλησης πετρελαίου στον Κόλπο της Γουινέας, μεταφέρθηκε με κάποιο τρόπο στην ακτή της βόρειας Καλιφόρνια, ακριβώς έξω από το Point Reyes και φαινόταν να πλέει στην ενδοχώρα οργώνοντας βουνά και ερήμους μέχρι τη Γιούτα. Το Princess Janice ήταν μόνο ένα από τα δώδεκα πλοία-φαντάσματα που παρατηρήθηκαν να κάνουν κύκλους στις θάλασσες στα ανοιχτά του Point Reyes Ωστόσο, όλα συνέχισαν να πλέουν ανοιχτά της Ισημερινής Γουινέας, της Μαλαισίας, της Νορβηγίας και άλλων απομακρυσμένων τοποθεσιών.



Εικόνα 51 - Πέντε πλοία που «εκτοπίστηκαν» στο Point Reyes, από μέρη σε όλο τον κόσμο. (BigThink, 2022)

Μερικά πλοία εκτοπίστηκαν στη Μαδρίτη ή στο Χονγκ Κονγκ για λίγες μόνο ώρες, αλλά το εικονικό ταξίδι του Princess Janice στη Βόρεια Αμερική διήρκεσε περίπου δύο εβδομάδες. Το περιστατικό του Point Reyes, που δημοσιοποιήθηκε από τον Bjorn Bergman, ερευνητή των περιβαλλοντικών παρατηρητών SkyTruth και Global Fishing Watch, ήταν το πιο πρόσφατο παράδειγμα ενός φαινομένου γνωστού ως «circle spoofing». Στην «κανονική» πλαστογράφηση GPS, η τοποθεσία (συνήθως ενός πλοίου) «μεταφέρεται» σε ένα στατικό σημείο κάπου αλλού. Στην πλαστογράφηση κύκλου, η θέση μετακινείται σε δυναμική θέση, περιστρέφοντας σε κυκλικό μοτίβο. Αυτό κάνει την πλαστογράφηση κύκλου πιο δύσκολη στην ανάγνωση και δυνητικά πιο επικίνδυνη. (BigThink, 2022)



Εικόνα 52 - Πλοία-φαντάσματα που κάνουν κύκλους ανοιχτά της Καλιφόρνιας (BigThink, 2022)

Τον Ιούνιο του 2021 τα δεδομένα παρακολούθησης δύο πολεμικών πλοίων του ΝΑΤΟ πλαστογραφήθηκαν. Πιο συγκεκριμένα, επρόκειτο για το HMS Defender του Βασιλικού Ναυτικού του Ηνωμένου Βασιλείου και το HNLMS Evertsen του Βασιλικού Ναυτικού της Ολλανδίας τα οποία βρίσκονταν στο λιμάνι της Οδησσού. Σύμφωνα με τα σήματα έδειχναν ότι τα δυο αυτά πλοία έφυγαν λίγο πριν τα μεσάνυχτα της 18ης Ιουνίου πλέοντας προς την Σεβαστούπολη, πλησιάζοντας σε απόσταση δύο ναυτικών μιλίων την είσοδο του λιμανιού, το οποίο είναι το

στρατηγικό λιμάνι του ρωσικού στόλου της Μαύρης Θάλασσας. Ωστόσο, εκείνη την εποχή, μεταδίδονταν βίντεο ζωντανά από το ουκρανικό λιμάνι της Οδησσού, το οποίο έδειχνε ότι δεν έφυγαν ποτέ από το λιμάνι καθ' όλη την διάρκεια της νύχτας. (USNI news, 2022) (The News, 2022)

Σε πιο πρόσφατες ειδήσεις η Αμερικανική Ακτοφυλακή έχει λάβει επίσης αναφορές περιστατικών παρεμβολών GPS από τη Διώρυγα του Σουέζ, την Κύπρο, τη Μάλτα και την Κωνσταντινούπολη, τον Περσικό Κόλπο κοντά στο Νταμάμ, στη Σαουδική Αραβία, και στα ανοικτά των ακτών στη Βραζιλία. Οι παρεμβολές GPS στον θαλάσσιο τομέα παρακολουθούνται και καταπολεμούνται μέσω του Ναυτιλιακού Κέντρου του NATO. (US MARAD: GPS interference incidents reported in the eastern Mediterranean Sea, 2022)

3.2.3 AIS

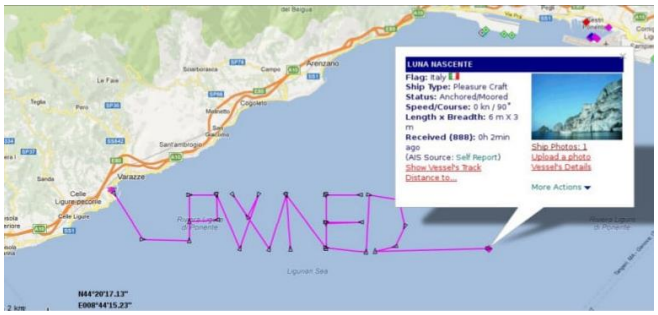
Οι Kessler et al., ταξινόμησαν διάφορες απειλές κυβερνοεπιθέσεων για τα συστήματα AIS. Υποστήριξαν ότι η δυσλειτουργία του AIS, η εμπλοκή του και η πλαστογράφηση ήταν από τους πιο συνηθισμένους τύπους επίθεσης. Οι Alcaide et al. εξήγησαν ότι το σύστημα αυτόματης αναγνώρισης ενός πλοίου είναι ένα από τα πιο ευάλωτα σε πιθανές επιθέσεις στον κυβερνοχώρο. Η αλλαγή της πραγματικής θέσης ενός πλοίου ή η έγχυση ενός ψευδούς σήματος μπορεί να επιφέρει τη σύγκρουση ή την αναστολή λειτουργίας του. (Jo, Choi, You, Cha, & Lee, 2022)

```
!AIVDM,1,1,,A,16SteH0P00Jt63hHaa6SagvJ087r,0*42
   MessageType:        1
   MMSI:               440348000
   NavigationStatus:   0
   Speed Over Ground:  0
   Longitude:          -70.7582
   Latitude:           43.08015
   Course Over Ground: 93.4
   TrueHeading:        511

!AIVDM,1,1,,A,H42O55i18tMET00000000000000,2*6D
!AIVDM,1,1,,A,H42O55lti4hhhilD3nink000?050,0*40
   MessageType:        24
   MMSI:               271041815
   Name:               PROGUY
   ShipAndCargo:       60
   VendorID:           1D00014
   CallSign:           TC6163
   Dimensions:         15x5
```

Εικόνα 53 - Δείγμα προτάσεων AIVDM για αναφορές θέσεις (πάνω) και στατικές (κάτω) (Wilhoit, 2022)

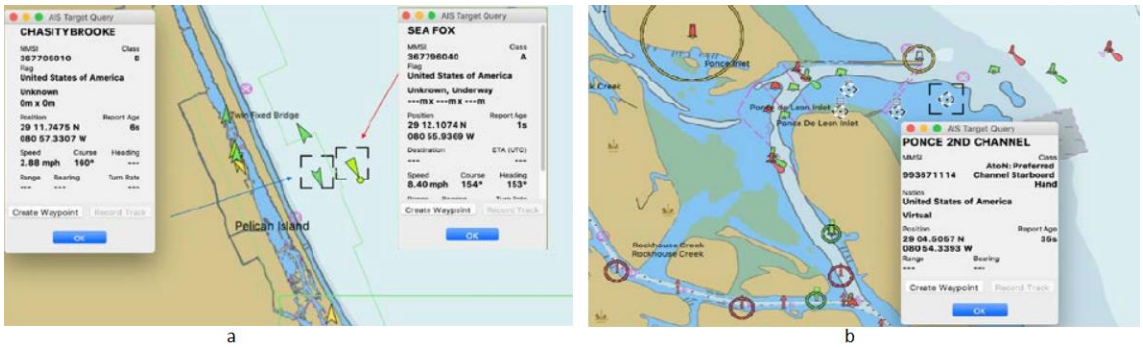
Οι ερευνητές ζητημάτων ασφαλείας M.Balduzzi και K. Wilhoit ξεκίνησαν με ελέγχους στο σύστημα για πλαστογραφήσεις. Πρώτα, δημιούργησαν έγκυρες πληροφορίες AIS κοντά σε ένα υδάτινο σώμα ή έναν πραγματικό σταθμό AIS, χρησιμοποιώντας τον κωδικοποιητή AIVDM. Στη συνέχεια, έστειλαν έγκυρα μηνύματα AIS στους παρόχους χρησιμοποιώντας έναν γενικό πελάτη δικτύωσης. Τέλος, εφάρμοσαν ένα αυτοματοποιημένο σενάριο για να πλαστογραφήσουν έναν σταθμό AIS που ακολουθεί μια διαδρομή για μια συγκεκριμένη χρονική περίοδο. Αναλυτικότερα δημιούργησαν ένα φανταστικό πλοίο που γράφει «PWNED» στη Μεσόγειο Θάλασσα, όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 54 - Πλαστογράφηση AIS (Wilhoit, 2022)

Εξετάζοντας τις επιθέσεις MitM, αρχικά, υπέκλεψαν έγκυρες προτάσεις AIVDM που μεταδόθηκαν μέσω του αέρα από έναν κοντινό σταθμό αναπτύσσοντας μια πύλη AIS την οποία ήλεγχαν. Στη συνέχεια χρησιμοποιήσαν έναν διακομιστή μεσολάβησης για να αναχαιτίσουν, να τροποποιήσουν και να στείλουν μηνύματα AIS στους διαδικτυακούς παρόχους, οι οποίοι τα αποδέχθηκαν. Σε ένα δεύτερο πείραμα, επέλεξαν ένα πλοίο, στο οποίο τροποποίησαν τις πληροφορίες μέσω μιας επίθεσης που βασίζεται σε λογισμικό. Με επιτυχία ανάγκασαν τους παρόχους να το δείξουν σε διαφορετική από την αρχική του τοποθεσία. (Wilhoit, 2022)

Στην έρευνα του MIT Technology του 2019 αναφέρθηκε ότι λαθρέμπορες κλωνοποιούσαν τις ταυτότητες AIS άλλων πλοίων για να γλιστρήσουν μέσα και έξω από το λιμάνι ανενόχλητα από τις αρχές. Πιο συγκεκριμένα, τον Ιούνιο του τρέχοντος έτους στη Σαγκάη, ένα πετρελαιοφόρο κλωνοποίησε το σύστημα AIS προκειμένου να αποφύγει τη σύλληψη του από ένα περιπολικό σκάφος MSA. Άλλα περιστατικά παραβιασμένης τεχνολογίας AIS αφορούν την κλοπή άμμου από τον ποταμό Yangtze. Ένα τέτοιο παράδειγμα αποτελεί το πλοίο New Glory που πλαστογραφήθηκε τουλάχιστον πέντε φορές μέσα στους έξι μήνες του ίδιου έτους. (MIT Technology Review, 2022)



a b

Εικόνα 55 - Επιθέσεις AIS και δημιουργία ψεύτικων a) πλοίων b) AtoN (Kessler G. , Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity, 2022)

Τον Ιούνιο του 2020 δημοσιοποιήθηκε αναφορά για 2 περιστατικά παραποίησης δεδομένων AIS. Το ένα αφορά 9 πλοία στις ακτές της παραλίας Daytona στη Φλόριντα (a). Τα 7 από αυτά βρίσκονταν πράγματι την συγκεκριμένη χρονική στιγμή εκεί όπως το Chastity Brooke, ενώ τα άλλα 2 βρίσκονταν εκεί 6 μήνες νωρίτερα, όπως το Sea Fox. Το δεύτερο περιστατικό συνέβη στην είσοδο του Ponce De Leon (b). Με βάση πλαστά μηνύματα εμφανίστηκαν στον ηλεκτρονικό χάρτη AtoNs ορίζοντας έτσι λανθασμένες εισόδους στο κανάλι. (Kessler G. , Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity, 2022)

3.2.4 ECDIS

Ο Ruben Santamarta, κύριος σύμβουλος ασφαλείας της IOActive. περιέγραψε τα Backdoors, τα κωδικοποιημένα διαπιστευτήρια, τα μη ασφαλή και μη τεκμηριωμένα πρωτόκολλα και τις αδυναμίες επαναφοράς κωδικού πρόσβασης που βρέθηκαν στα τερματικά δορυφορικής επικοινωνίας. Περιέγραψε περαιτέρω τα σενάρια παραποίησης για το ECDIS, τις πληροφορίες κατάστασης πλοίου και τις πληροφορίες φορτίου με βάση τις ευπάθειες ασφαλείας που σχετίζονται με τα τερματικά SAILOR 900 VSAT (Cobham, Δανία) και JUE-250 FB (Japan Radio Co. Ltd., Τόκιο, Ιαπωνία).

Επιπλέον, οι Awan και Ghamdi συνέλεξαν και ανέλυσαν περιπτώσεις ατυχημάτων πλοίων που θα μπορούσαν να επηρεάσουν την ασφάλεια στον κυβερνοχώρο. Για παράδειγμα, στη βύθιση ενός ανθρακοφόρου το 2004, ο ηλεκτρονικός χάρτης πλοήγησης (ENC) δεν ήταν ενημερωμένος και απέτυχε να εμφανίσει το μικρό βάθος νερού. Αυτό υποδηλώνει ότι ένα ανακριβές αρχείο ENC μπορεί να οδηγήσει στη βύθιση ενός πλοίου.

Οι Svilicic et al. πραγματοποίησαν μια ποσοτική αξιολόγηση κινδύνου στον κυβερνοχώρο χρησιμοποιώντας ένα εργαλείο σάρωσης ευπάθειας ασφαλείας στο σύστημα JAN-901B ECDIS. Η διεπαφή αυτού του συστήματος αποτελούνταν από ένα τοπικό δίκτυο Ethernet (LAN, 10/100 Mbps) και το IEC61162-1/2, USB και εκτελούνταν σε σύστημα Windows XP. Πραγματοποιώντας περαιτέρω αξιολογήσεις βρήκαν ότι ένα Transas Navi Sailor 4000 ECDIS είναι εγκατεστημένο σε λειτουργικό σύστημα Windows 7 και ότι σαν κρίσιμη ευπάθεια είναι οι ευάλωτες εκδόσεις του SMB[37] και του πρωτοκόλλου απομακρυσμένης επιφάνειας εργασίας (RDP) που χρησιμοποιούνται στο σύστημα.

Στη συνέχεια το Navi Sailor 4000 ECDIS (Wärtsilä Transas, Φινλανδία), που είναι εγκατεστημένο στο εκπαιδευτικό ερευνητικό πλοίο Kraljica Mora, διαπιστώθηκε ότι είχε έναν ξεπερασμένο διακομιστή ιστού Apache και μια ευάλωτη έκδοση του SMB. Τέλος, αξιολογήθηκαν ευπάθειες ασφαλείας χρησιμοποιώντας ένα εργαλείο σάρωσης στο σύστημα NACOS MULTIPILOT Platinum 2017 ECDIS (Wärtsilä SAM Electronics GmbH, Γερμανία), που είναι εγκατεστημένο σε σκάφος ROPAX. Αυτές οι μελέτες υποδεικνύουν τη χρήση ευάλωτων εκδόσεων του SMB και του RDP ως ευπάθεια. (Jo, Choi, You, Cha, & Lee, 2022)

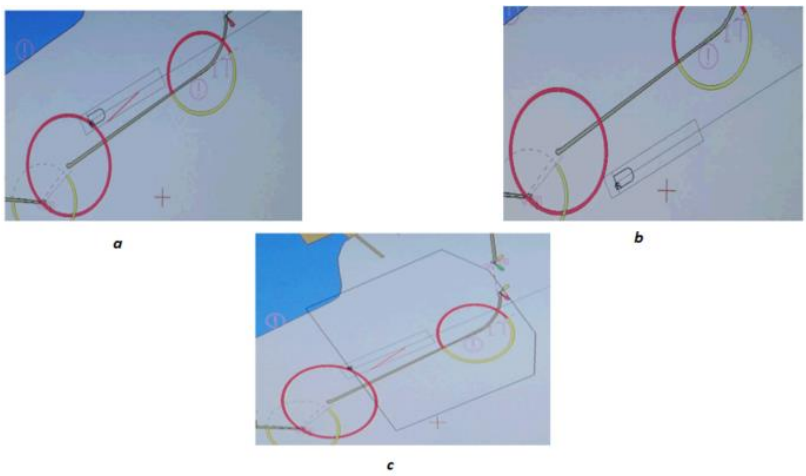
Ο Ken Munro μέσω της εταιρίας Pen Test Partners, τον Ιούνιο του 2018, δημοσίευσε ένα άρθρο σχετικά με την παραβίαση του ECDIS. Αρχικά, για να επέλθει στα χέρια του η πρόσβαση στο δίκτυο του πλοίου, παραβίασε το hardware δορυφορικού τερματικού Cobham, όπου οι διεπαφές διαχειριστή ήταν μέσω telnet και HTTP, και με τον έλεγχο επικύρωσης να ήταν απλώς ένα CRC[38]. Διαπίστωσε και άλλες ευπάθειες όπως ότι οι κωδικοί πρόσβασης ήταν ενσωματωμένοι στις ρυθμίσεις παραμέτρων, κατακερματισμένοι με MD5[39], ότι δεν υπήρχε προστασία επαναφοράς για το υλικολογισμικό (ένας χάκερ θα μπορούσε να εγκαταστήσει μια παλαιότερη πιο ευάλωτη έκδοση υλικολογισμικού) και άλλες τις οποίες δεν αποκάλυψε.

Ο Munro και η εταιρία του δοκίμασαν πάνω από 20 διαφορετικές μονάδες ECDIS και βρήκαν κάθε είδους ελαττώματα ασφαλείας. Τα περισσότερα έτρεχαν παλιά λειτουργικά συστήματα, όπως το Windows NT. Ένα ενδιαφέρον παράδειγμα είχε μια κακώς προστατευμένη διεπαφή διαμόρφωσης. Χρησιμοποιώντας αυτή, μπορέσαν να μετατοπίσουν την θέση του σκάφους πλαστογραφώντας τον δέκτη GPS του πλοίου. Ενημερώνεται το ECDIS ότι ο δέκτης GPS βρίσκεται σε διαφορετική θέση. Ακόμη χειρότερα, θα μπορούσαν να το διαμορφώσουν εκ νέου για να κάνουν το πλοίο να φαίνεται μικρότερο από ό,τι στην πραγματικότητα. Το ECDIS συχνά τροφοδοτεί τον πομποδέκτη AIS. Έτσι, με μία πλαστογράφηση στην αλλαγή μεγέθους και θέσης, το ECDIS μπορεί να σημάνει ειδοποίηση σύγκρουσης σε άλλα πλοία.

[37] Server Message Block (SMB) είναι ένα πρωτόκολλο κοινής χρήσης αρχείων και δεδομένων δικτύου (Microsoft SMB Protocol and CIFS Protocol Overview, 2022)

[38] Cyclic redundancy check ονομάζονται έτσι επειδή η τιμή ελέγχου (επαλήθευση δεδομένων) είναι πλεονασμός (επεκτείνει το μήνυμα χωρίς να προσθέτει πληροφορίες) και ο αλγόριθμος βασίζεται σε κυκλικούς κώδικες. Τα CRC είναι δημοφιλή επειδή είναι απλά στην εφαρμογή τους σε δυαδικό υλικό, είναι εύκολο να αναλυθούν μαθηματικά και ιδιαίτερα καλά στην ανίχνευση κοινών σφαλμάτων που προκαλούνται από το θόρυβο στα κανάλια μετάδοσης (Cyclic redundancy check, 2022)

[39] Ένας κατακερματισμός MD5 δημιουργείται λαμβάνοντας μια συμβολοσειρά οποιουδήποτε μήκους και κωδικοποιώντας την σε ένα δακτυλικό αποτύπωμα 128 bit. Η κωδικοποίηση της ίδιας συμβολοσειράς χρησιμοποιώντας τον αλγόριθμο MD5 θα έχει πάντα ως αποτέλεσμα την ίδια έξοδο κατακερματισμού 128 bit (MD5 Hash Generator, 2022)



Εικόνα 56 - a) Κανονικό b) Αλλαγή θέσης c) Αλλαγή μεγέθους (Munro, Hacking, tracking, stealing and sinking ships, 2022)

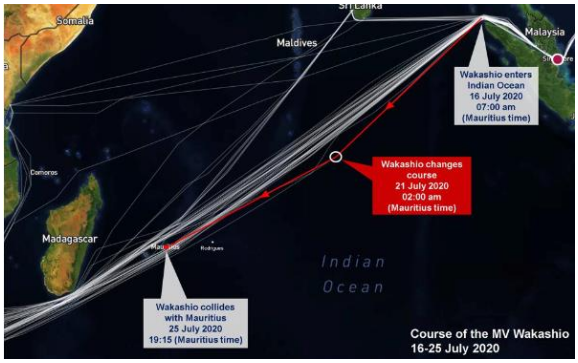
Επιπλέον, μια διαφορετική τεχνική για τον αναγκασμό του πλοίου να εγκαταλείψει την πορεία του, μπορεί να επιτευχθεί με μία επίθεση MitM, εισάγοντας μικρά εσφαλμένα μηνύματα. Πιο συγκεκριμένα, μπορούν να τροποποιηθούν τα μηνύματα NMEA, επηρεάζοντας το αντίστοιχο OT σύστημα. Αξιοσημείωτο είναι το ότι δεν υπάρχει έλεγχος ταυτότητας, κρυπτογράφηση ή επικύρωση αυτών των μηνυμάτων, είναι απλό κείμενο. Έτσι όταν τα πλοία βρίσκονται σε κατάσταση «ελέγχου τροχιάς» (πράγμα που συμβαίνει τις περισσότερες φορές) και ακολουθούν την πορεία του ECDIS, θα μπορούσε να εξαπατηθεί ο αυτόματος πιλότος, οδηγώντας τα στην συντριβή τους, ιδιαίτερα στην ομίχλη. (Munro, Hacking, tracking, stealing and sinking ships, 2022)

Ο Brendan Saunders, τεχνικός επικεφαλής ναυτιλίας στην εταιρεία κυβερνοασφάλειας NCC Group, εξιστορεί ένα ακόμη περιστατικό. Αυτό αφορούσε ένα τάνκερ βάρους 80.000 τόνων σε ασιατικό λιμάνι. Ένα μέλος του πληρώματος εισήγαγε στους υπολογιστές του πλοίου ένα USB stick το οποίο περιείχε κακόβουλο λογισμικό. Βεβαία, τα συστήματα πλοήγησης μολύνθηκαν, όταν μέσω USB ένα δεύτερο μέλος πήγε να ενημερώσει τους χάρτες του πλοίου πριν από τον απόπλου. Κατά συνέπεια, η αναχώρηση καθυστέρησε, μιας και τα συστήματα ECDIS δεν έχουν anti-virus. (Baraniuk, 2022)

Το Πολεμικό Ναυτικό των ΗΠΑ ανέφερε ότι οι εσφαλμένοι ψηφιακοί χάρτες που χρησιμοποιήθηκαν στο ECDIS είχαν ως αποτέλεσμα το USS Guardian να προσαράξει στις Φιλιππίνες το 2013. Οι ψηφιακοί χάρτες που παρείχε η Εθνική Υπηρεσία Γεωχωρικών Πληροφοριών (NGA) απέκλιναν κατά οκτώ (8) ναυτικά μίλια και είχαν ως αποτέλεσμα τη προσάραξη του ναρκαλιευτικού σκάφους καθώς επίσης και την καταστροφή 43.000 τετραγωνικών ποδιών του υφάλου στις Φιλιππίνες. Τον Σεπτέμβρη του ίδιου έτους το μαλτέζικο δεξαμενόπλοιο πετρελαίου και χημικών Ovit προσάραξε στο Varne Bank στο Στενό του Ντόβερ. Οι έρευνες αποκάλυψαν ακατάλληλη διαμόρφωση των συναγερμών ECDIS και ανεπαρκή γνώση χρήσης του.

Μια πειραματική μελέτη που αναφέρθηκε τον Ιανουάριο του 2014, αξιολόγησε τα τρωτά σημεία στο ECDIS που εκτελείται σε υπολογιστή Windows 7 και διαπίστωσε ότι οι επιθέσεις στον κυβερνοχώρο θα μπορούσαν να οδηγήσουν σε τροποποίηση ή διαγραφή δεδομένων του χρησιμοποιώντας επικίνδυνες μεθόδους HTTP ως ενέσεις κεφαλίδας. Επιπλέον, το ECDIS βρέθηκε να είναι ευάλωτο λόγω ενός ξεπερασμένου διακομιστή Web Apache που χρησιμοποιείται από το σύστημα.

Στις 3 Δεκεμβρίου του 2016, το πλοίο μεταφοράς χύδην φορτίου Muros καθηλώθηκε στο Haisborough Sand, 8 μίλια από την ακτή του Norfolk στο Ηνωμένο Βασίλειο λόγω της κακής χρήσης της ηλεκτρονικής απεικόνισης χαρτών και του συστήματος πληροφοριών (ECDIS). Αυτό συνδεόταν με πολλά ζητήματα ασφάλειας. (Ghamdi, 2022) Για την ακρίβεια, δεν ακολουθούσε τις οδηγίες από τον προμηθευτή του συστήματος ούτε από τις ρυθμιστικές αρχές. Το Τμήμα Διερεύνησης Ναυτικών Ατυχημάτων (MAIB) της κυβέρνησης του Ηνωμένου Βασιλείου είπε ότι οι διασφαλίσεις ECDIS αγνοήθηκαν ή απενεργοποιήθηκαν. (Wingrove, ACCIDENT REPORT: Ship damaged due to incorrect ECDIS use, 2022)



Εικόνα 57 - Πορεία Wakashio στον Ινδικό Ωκεανό (Degnarain, 2022)

Τέλος, ένα άρθρο που κοινοποιήθηκε τον Οκτώβριο του 2020 αναφέρει πως τον Ιούλιο του ίδιου έτους, το πλοίο Wakashio προσάραξε στους υφάλους του Μαυρικίου με αποτέλεσμα την δημιουργία πετρελαιοκηλίδας. Υπήρχαν ισχυρισμοί ότι έπεσε θύμα κυβερνοασφάλειας με το σύστημα ECDIS να έχει παραβιαστεί και τα δεδομένα του να έχουν τροποποιηθεί. Η δορυφορική ανάλυση αποκάλυψε ότι το Wakashio ήταν εκτός πορείας από τη στιγμή που εισήλθε στον Ινδικό Ωκεανό, αλλά η διόρθωση πορείας κατά 13 μοίρες στις 21 Ιουλίου ήταν αυτή που το έβαλε στη καταστροφική πορεία. (Degnarain, 2022)

3.2.5 Radar

Μέχρι στιγμής τα συστήματα radar που χρησιμοποιούνται στη ναυτιλία δεν έχουν πέσει θύματα κυβερνοεπίθεσης. Ωστόσο, έχουν προκύψει περιστατικά από λάθος του αξιωματικού βάρδιας το οποίο θα μπορούσε να οφείλεται σε κάποια μορφή κυβερνοεπίθεσης. Από την στιγμή απόκτησης πρόσβασης στο σύστημα ο επιτιθέμενος μπορεί να τροποποιήσει τα δεδομένα, να διαταράξει τις λειτουργίες του και να το μπλοκάρει. (Junior, Moraes, Albuquerque, Machado, & Sá, 2022).

Στις αρχές του Ιουλίου του 2014 ένα πλοίο γενικού φορτίου συγκρούστηκε με ένα ιστιοφόρο. Ένας από τους λόγους που οδήγησαν στη σύγκρουση ήταν ότι το radar δεν ήταν προσαρμοσμένο στο κέντρο, με αποτέλεσμα ο αξιωματικός φρουράς στην γέφυρα να έχει λανθασμένη εικόνα. (Reports, 2022) Στις 7 Σεπτεμβρίου του 2020 ένα άρθρο δημοσιοποιήθηκε για μία σύγκρουση μεταξύ ενός σκάφους Ro-Ro και ενός αγκυροβολημένου containership με αποτέλεσμα να σφηνώσουν. Αυτό το συμβάν προκλήθηκε από πολλούς και διάφορούς λόγους, ένας από τους οποίους ήταν η σίγαση των ηχητικών ειδοποιήσεων του radar. (Network, 2022)

Ένα περιστατικό επίθεσης που όμως δεν σχετίζεται με τη ναυτιλία, έλαβε μέρος στην Συρία τον Σεπτέμβριο του 2007. Η επονομαζόμενη επιχείρηση Περιβόλι (Operation Orchard) διεξήχθη από το υπουργείο άμυνας του Israel με σκοπό να προκαλέσει δυσλειτουργικά προβλήματα στο σύστημα ραντάρ αεράμυνας της Συρίας. Για το εν λόγω συμβάν δύο είναι οι τα σενάρια για τις τεχνικές που χρησιμοποιήθηκαν.

Το πρώτο, γνωστό ως δικτυοκεντρική συνεργατική στόχευση (Network-Centric Collaborative Targeting), προσδιορίζει και εντοπίζει τους στόχους, και το δεύτερο είναι μέρος του προγράμματος Big Safari, το οποίο είναι γνωστό ως Senior Suter. Το Suter εκμεταλλεύεται τα τρωτά σημεία και διακόπτει τη λειτουργία του επιτιθέμενου συστήματος αεράμυνας εκπέμποντας ηλεκτρονικούς παλμούς στις κεραίες του στόχου. Αφού εισβάλουν στο δίκτυο και φτάσουν στον

βρόχο επικοινωνιών, οι χειριστές καταστρέφουν το σύστημα εισάγοντας παραπλανητικά δεδομένα, όπως κατασκευασμένα μηνύματα ή φανταστικούς στόχους, με σκοπό την πρόκληση εξαπάτησης. (Cyber Law, 2022)

3.3 Περιστατικά στα συστήματα επικοινωνίας

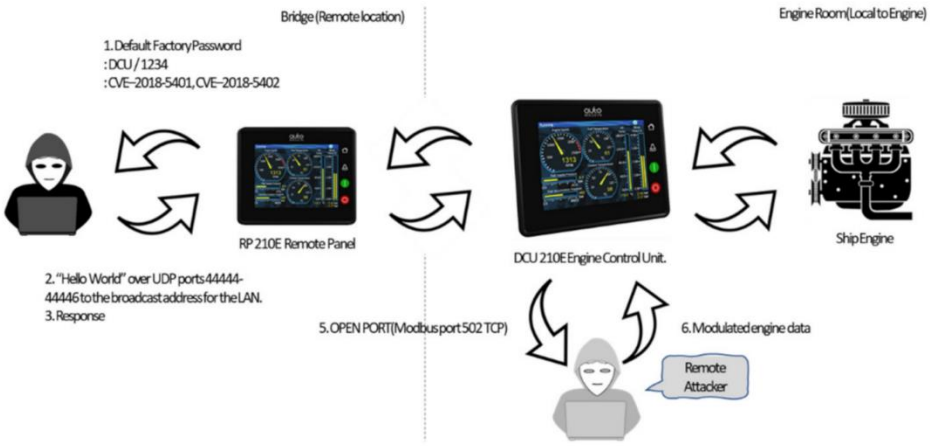
Στην ενότητα αυτή θα παρουσιαστούν ορισμένες τρωτότητες που αφορούν τα συστήματα επικοινωνίας. Με βάση την ανάλυση του MITRE ATT&CK, όπως φαίνεται και στην παρακάτω εικόνα, στα πιθανά τελικά αποτελέσματα περιλαμβάνονται η αποτυχία επικοινωνίας ή η σύγκρουση του πλοίου. Αυτά προέκυψαν γιατί ο επιτιθέμενος μπορεί να εκμεταλλευτεί αδύναμα πρωτοκόλλα, όπως το HTTP και το Telnet, αλλά και τις προεπιλεγμένες ρυθμίσεις και τους κωδικούς πρόσβασης που έχει ορίσει ο κατασκευαστής. Στη συνέχεια, με επίθεση στη διεπαφή Ιστού που χρησιμοποιείται στο πλοίο και εκτελώντας στοχευμένες επιθέσεις phishing σε μέλη του πληρώματος μπορεί να αποκτήσει την αρχική πρόσβαση. Αυτό μπορεί να οδηγήσει σε υποκλοπή δικτύου στο Πρωτόκολλο Voice over Internet (VoIP) ακόμη και σε άρνηση υπηρεσίας με σκοπό την διακοπή επικοινωνίας του κύτους.

Tactic	Description
Command and Control	• The use of a weak protocol is susceptible to data falsification. • The adversary attacks vulnerable protocols such as HTTP and TELNET.
Lateral Movement	• The adversary takes advantage of the default settings and passwords set by the manufacturer on the ICS system device. • The factory default password is written in the manual.
Execution	• The adversary attacks the web interface used on the ship.
Initial Access	• The adversary executes targeted phishing attacks on crew members using malware.
Discovery	• Network eavesdropping on Voice over Internet Protocol (VoIP) can expose sensitive information.
Inhibit Response Function	• It is difficult to rapidly update software for OT systems. • The denial-of-service attack on VoIP disrupts hull communication.
Impact	• Communication failure occurs. • The ship collides.

Εικόνα 58 - Αποτελέσματα ανάλυσης MITRE ATT&CK στα συστήματα επικοινωνίας (Jo, Choi, You, Cha, & Lee, 2022)

Σχετικά με την αποκάλυψη ευαίσθητων πληροφορίων, κοινά πρωτόκολλα αναλύθηκαν από τους Pavur et al., οι οποίοι παρατήρησαν την κίνηση επικοινωνίας VSAT. Διαπίστωσαν ότι τα θαλάσσια VSAT ήταν ευάλωτα σε επιθέσεις υποκλοπής και πλαστογράφησης λόγω της χρήσης μη κρυπτογραφημένων πρωτοκόλλων. Επίσης, το 2017, ένας ερευνητής μιας εταιρείας ασφαλείας εντόπισε ένα τέτοιο ελάττωμα στην εφαρμογή web του CommBox. Αυτό θα μπορούσε να οδηγήσει σε επιθέσεις spear phishing με βάση τα προσωπικά δεδομένα των μελών του πληρώματος.

Οι Tierney et al. βρήκαν μια ευπάθεια ασφαλείας στο Dualog, ένα λογισμικό που παρέχει υπηρεσίες που επιτρέπει στο πλήρωμα να συνδέεται στο Διαδίκτυο, να χρησιμοποιεί μεταφορές αρχείων και να στέλνει email στα πλοία. Αυτά τα τρωτά σημεία περιλάμβαναν τα CVE-2020-26576, CVE-2020-26577, CVE-2020-26578, CVE-2020-26579, CVE-2020-26580 και CVE-2020-26581. Συγκεκριμένα, διαπιστώθηκε ότι ήταν δυνατή η αύξηση του επιπέδου των δικαιωμάτων μέσω σύνδεσης με τον προεπιλεγμένο λογαριασμό (admin.g4@g4.dulog.no) και τον κωδικό πρόσβασης.



Εικόνα 59 - Σενάριο επίθεσης μέσω CVE (Jo, Choi, You, Cha, & Lee, 2022)

Ένα άλλο περιστατικό με τους Tierney et al. ήταν όταν επιβιβάστηκαν σε ένα επιβατηγό πλοίο και κατάφεραν να συνδεθούν στο VSAT χρησιμοποιώντας τον προεπιλεγμένο κωδικό πρόσβασης και το Wi-Fi του επιβάτη. Εξακρίβωσαν ότι ήταν δυνατή η πρόσβαση στο σύστημα διαχείρισης φόρτωσης φορτίου, καθώς και στο σύστημα διαχείρισης τηλεόρασης κλειστού κυκλώματος. Το πιο σοβαρό πρόβλημα ήταν ότι όλες οι πληροφορίες μπορούσαν να υποκλαπούν με sniffing, έχοντας πρόσβαση στο δίκτυο και χρησιμοποιώντας τον προεπιλεγμένο κωδικό πρόσβασης. (Jo, Choi, You, Cha, & Lee, 2022)

Η ασφάλεια των συσκευών επικοινωνίας των πλοίων (SATCOM) έχει πολλά τρωτά σημεία σύμφωνα με τον Ruben Santamarta. Η λίστα των αδυναμιών που εντόπισε στα πιο ευρέως διαδεδομένα τερματικά Inmarsat και Iridium δεν περιλαμβάνει μόνο ελαττώματα σχεδιασμού, αλλά και χαρακτηριστικά στις ίδιες τις συσκευές που θα μπορούσαν να χρησιμοποιηθούν για τους εισβολείς. Αυτά είναι πολλαπλές κερκόπορτες, διαπιστευτήρια, μη τεκμηριωμένα ή/και ανασφαλή πρωτόκολλα και αδύναμοι αλγόριθμοι κρυπτογράφησης.

Αυτά τα τρωτά σημεία επιτρέπουν σε απομακρυσμένους, μη πιστοποιημένους εισβολείς να παραβιάσουν τα επηρεαζόμενα προϊόντα. Σε ορισμένες περιπτώσεις δεν απαιτείται αλληλεπίδραση με τον χρήστη για την εκμετάλλευση της ευπάθειας. Αρκεί η αποστολή ενός απλού SMS ή ενός ειδικά κατασκευασμένου μηνύματος από ένα πλοίο σε ένα άλλο για να είναι επιτυχής. (Zorz, The dismal state of SATCOM security, 2022)

Επίσης ένας άλλος σύμβουλος ασφαλείας της IOActive, ο Mario Ballano, ανακάλυψε δύο κρίσιμα τρωτά σημεία στον κυβερνοχώρο που επηρεάζουν την πλατφόρμα επικοινωνίας πλοίων AmosConnect της Stratos Global. Η πλατφόρμα AmosConnect λειτουργεί σε συνδυασμό με τον δορυφορικό εξοπλισμό των πλοίων και ενσωματώνει εφαρμογές γραφείου που βασίζονται σε σκάφη και στην ξηρά, καθώς και παρέχει υπηρεσίες όπως πρόσβαση στο Διαδίκτυο για το πλήρωμα, email, αναφορά θέσης κ.λπ.

Τα τρωτά σημεία που εντόπισε ήταν η δυνατότητα για SQL Injection και backdoors. Με το πρώτο οι εισβολείς μπορούν να ανακτήσουν διαπιστευτήρια για να συνδεθούν στην υπηρεσία και να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες που είναι αποθηκευμένες σε αυτήν. Ενώ με το δεύτερο επιτρέπεται στους εισβολείς να εκτελούν εντολές με δικαιώματα SYSTEM. Αυτές οι ευπάθειες μπορούν να γίνουν αντικείμενο εκμετάλλευσης μέσω των δικτύων «επισκέπτη» πάνω

σε ένα πλοίο ή μέσω της δορυφορικής σύνδεσης που αναφέρθηκε. (Zorz, Critical flaws in maritime comms system could endanger entire ships, 2022)

Το 2020 σε ένα άρθρο ο Ewan Robinson, διευθυντής της εταιρείας παροχής θαλάσσιων επικοινωνιών Yangosat, ανέφερε πως κατάφεραν να αποκτήσουν πρόσβαση σε ένα σκάφος μέσω του προεπιλεγμένου ονόματος χρήστη και κωδικού πρόσβασης στο σύστημα VSAT. Αφού επιτεύχθηκε η πρόσβαση στην περιοχή διαχείρισης, άλλαξαν όλα τα ονόματα και τους κωδικούς των χρηστών για να μην έχουν εκείνοι πρόσβαση. Επίσης, εντόπισαν ότι ήταν διαθέσιμη η πρόσβαση στο σύστημα μέσω FTP, το όποιο είναι ένα σημαντικό ελάττωμα ασφαλείας. Αυτό γιατί μέσω αυτής υπάρχει η δυνατότητα για πρόσβαση σε ολόκληρο το λειτουργικό σύστημα της συσκευής, και όχι μόνο στην περιοχή FTP.

Ένα δεύτερο ελάττωμα ασφαλείας ήταν ένα αρχείο κειμένου σε κάθε φάκελο με ολόκληρη την δομή του λειτουργικού συστήματος. Αυτό επέτρεψε την εύρεση και αντιγραφή του «κρυφού» αρχείου κωδικού πρόσβασης στον τοπικό υπολογιστή. Αν και κρυπτογραφημένο μετά από διαδικασίες 2 ωρών κατάφεραν να το αποκρυπτογραφήσουν. Έτσι αποκτήθηκαν τα ονόματα των χρηστών όπως και οι κωδικοί πρόσβασης όλων των κατασκευαστών, και μετέπειτα η πρόσβαση στα δημόσια διαθέσιμα μηχανήματα.

Στη συνέχεια διερευνήθηκαν οι συνδέσεις δικτύου που αναφέρονται στη ρύθμιση της κεραίας. Πάλι με προεπιλεγμένες συνδέσεις στο SSH κατάφεραν να συνδεθούν στο VSAT Modem, με δημόσια διαθέσιμα ονόματα χρήστη και κωδικούς πρόσβασης. Η πρόσβαση στη γραμμή εντολών στο μόντεμ επιτεύχθηκε, επιτρέποντάς τους τον έλεγχο και τη διαμόρφωση. Με αυτά πλέον έχουν την δυνατότητα ελέγχου επικοινωνιών σε 2 διαφορετικά σημεία. (Robinson, We hacked a ship. The owner is liable., 2022) (Robinson, Hacked – a real life story of exploiting vessel VSAT, 2022)

Το 2017, ένας ανεξάρτητος ερευνητής κυβερνοασφάλειας με έδρα τη Γαλλία, ο οποίος χρησιμοποιεί το ψευδώνυμο x0rz , κατάφερε να εισέλθει στο σύστημα δορυφορικών επικοινωνιών ενός πλοίου. Ο ερευνητής χρησιμοποίησε τη μηχανή αναζήτησης Shodan για να βρει εύκολους διαδικτυακούς στόχους στη θάλασσα και την εφαρμογή Ship Tracker για να βρει το πλοίο στόχο του. Κατ' αυτόν τον τρόπο εντόπισε ένα VSAT σε ένα πραγματικό πλοίο στα ύδατα της Νότιας Αμερικής που είχε προεπιλεγμένα διαπιστευτήρια - το όνομα χρήστη «admin» και τον κωδικό πρόσβασης «1234».

Μπόρεσε να αποκτήσει πρόσβαση στο κέντρο επικοινωνίας του πλοίου και στη συνέχεια έκανε γνωστά τα ευρήματά του στο Twitter λέγοντας ότι είναι συνδεδεμένος με ένα μητρικό πλοίο ως διαχειριστής. Πρόσθεσε ότι το να χακάρεις τα πλοία είναι εύκολο και ότι μπορεί ακόμη και να ανεβάσει το δικό του υλικολογισμικό στο VSAT για να το χειριστεί. Μια στοχευμένη επίθεση θα μπορούσε ακόμη και να αλλάξει τις συντεταγμένες που μεταδίδονται από το σύστημα, επιτρέποντας ενδεχομένως σε κάποιον να παραπλανήσει τη θέση του πλοίου. (Champers, 2022) (Baraniuk, 2022)

3.4 Περιστατικά σε άλλα συστήματα

3.4.1 ECR

Το 2007 η δοκιμή γεννήτριας Aurora του Εθνικού Εργαστηρίου του Αϊντάχο απέδειξε ότι μια κυβερνοεπίθεση θα μπορούσε να καταστρέψει μια γεννήτρια συνδέοντάς την με το δίκτυο εκτός φάσης, γεγονός που οδηγεί σε ακραία ροπή και βλάβη του μηχανήματος. Ακόμη, μια γνωστή κυβερνοεπίθεση σημειώθηκε το 2015 όταν χάκερ απέκλεισαν την τροφοδοσία σε ένα μεγάλο τμήμα του πληθυσμού της Ουκρανίας. Η επίθεση επιτεύχθηκε επειδή δεν υπήρχε σωστή απομόνωση μεταξύ των συστημάτων IT και OT. (Walton, 2022) Η αναφορά σε αυτά τα 2 γεγονότα γίνεται για να δείξει την καταστροφή που μπορεί να επιφέρει μια κυβερνοεπίθεση στα συστήματα τροφοδοσίας.

Εικόνα 60 - Κυβερνοεπίθεση εναντίον μιας γεννήτριας ενέργειας (Averous, 2022)

Ένα πλοίο πρέπει να έχει τουλάχιστον 2 γεννήτριες τόσο για την πρόωση του όσο και για την υποστήριξη όλων των συστημάτων του και χώρια εφεδρικές σε περίπτωση ανάγκης (Modius, 2022). Ένα περιστατικό το οποίο προκλήθηκε λόγω ηλεκτρικής βλάβης ή κάποιο άλλο μηχανικό πρόβλημα έλαβε χώρα στις 5 Δεκεμβρίου του 2020 στο λιμάνι Bejaia της Αλγερίας. Σύμφωνα με πηγές, το πλοίο μεταφοράς εμπορευματοκιβωτίων Vega Sigma άρχισε να κάνει ελιγμούς για να φύγει από το λιμάνι, μέχρις ότου έχασε τον έλεγχο. Μη μπορώντας να σταματήσει τον ελιγμό του, το πλοίο χτύπησε ένα δεύτερο που με την σειρά του αυτό ένα τρίτο πλοίο μεταφοράς εμπορευματοκιβωτίων τα οποία βρίσκονταν στην αποβάθρα. Επιπλέον, συγκρούστηκε με μία γερανογέφυρα με αποτέλεσμα να κατεδαφιστεί και να τραυματιστεί ο άνθρωπος που την έλεγχε (Safety4Sea T. E., Vessel loses control, causes triple collision and crane crash, 2022).

Περιστατικό κυβερνοεπίθεσης αποτελεί ένα συμβάν σε ένα πλοίο ξηρού χύδην φορτίου. Με το πέρας τον εργασιών του στο λιμάνι, οι επιθεωρητές αποθηκών επιβιβάστηκαν και ζήτησαν πρόσβαση στον υπολογιστή στο δωμάτιο ελέγχου κινητήρα για να εκτυπώσουν ορισμένα έγγραφα για την απογραφή από ένα USB stick. Ο εξωτερικός όμως αυτός δίσκος ήταν μολυσμένος με αποτέλεσμα την εισαγωγή ιού σε αυτό το σύστημα. (Osler, 2022) Το κακόβουλο λογισμικό παρέμεινε απαρατήρητο έως ότου πραγματοποιήθηκε αξιολόγηση στον κυβερνοχώρο στο πλοίο λόγω αναφοράς προβλήματος από το πλήρωμα που επηρέαζε τα επιχειρηματικά δίκτυα.

Ένα παρόμοιο περιστατικό, στο οποίο όμως δεν ήταν γνωστό σε ποιο σύστημα έγινε η σύνδεση, συνέβη σε ένα νεότευκτο πλοίο του 2018. Αυτό ήταν εξοπλισμένο με ένα σύστημα διαχείρισης ενέργειας που με την σύνδεση του στο διαδίκτυο μπορούσε να αποκτήσει δυνατότητα για ενημερώσεις λογισμικού και επιδιορθώσεις, απομακρυσμένα διαγνωστικά, συλλογή δεδομένων και απομακρυσμένη λειτουργία. Όμως, το συγκεκριμένο σύστημα λόγω πρόσφατης κατασκευής δεν ήταν ακόμη συνδεδεμένο στο διαδίκτυο. Το τμήμα πληροφορικής της εταιρείας πήρε την απόφαση να επισκεφθεί το πλοίο και πραγματοποίησε σαρώσεις ευπάθειας για να διαπιστώσει εάν το σύστημα είχε στοιχεία μόλυνσης και να καθορίσει εάν ήταν ασφαλής η σύνδεση.

Η ομάδα ανακάλυψε ένα αδρανές ιό σκουλήκι που θα μπορούσε να ενεργοποιηθεί από μόνο του όταν το σύστημα συνδεόταν στο διαδίκτυο και αυτό θα είχε σοβαρές συνέπειες. Η εταιρεία ζήτησε από επαγγελματίες ασφάλειας στον κυβερνοχώρο να πραγματοποιήσουν ιατροδικαστική ανάλυση και αποκατάσταση. Διαπιστώθηκε ότι όλοι οι διακομιστές που σχετίζονται με τον εξοπλισμό ήταν μολυσμένοι και ότι ο ιός βρισκόταν στο σύστημα χωρίς να ανακαλυφθεί για 875 ημέρες. Τα εργαλεία σάρωσης αφαίρεσαν τον ιό. Μια ανάλυση απέδειξε ότι ο πάροχος υπηρεσιών ήταν η πηγή και ότι το σκουλήκι είχε εισαγάγει το κακόβουλο λογισμικό στο σύστημα του πλοίου μέσω μιας μονάδας USB κατά τη διάρκεια μιας εγκατάστασης λογισμικού. Η ανάλυση απέδειξε επίσης ότι αυτό το worm λειτουργούσε στη μνήμη του συστήματος και καλούσε ενεργά στο Διαδίκτυο από τον διακομιστή. Εφόσον το worm φορτώθηκε στη μνήμη, θα μπορούσε να επηρεάσει την απόδοση του διακομιστή και των συστημάτων που είναι συνδεδεμένα στο Διαδίκτυο. (Cimpanu, 2022)

Ο Patrick Rossi, ο οποίος εργάζεται στην ομάδα ηθικής hacking στον ανεξάρτητο συμβουλευτικό οργανισμό DNV GL, δήλωσε για ένα άλλο περιστατικό τα εξής: «Γνωρίζουμε ένα εμπορευματοκιβώτιο φορτίου, όπου ο πίνακας διανομής έκλεισε αφού το ransomware βρήκε το δρόμο του στο σκάφος». Το κακόβουλο λογισμικό είναι συχνά σχεδιασμένο να εξαπλώνεται από υπολογιστή σε υπολογιστή σε ένα δίκτυο. Αυτό σημαίνει ότι οι συνδεδεμένες συσκευές στα πλοία είναι δυνητικά ευάλωτες. Εξηγεί ότι ο πίνακας διανομής διαχειρίζεται την παροχή ρεύματος στην προπέλα και σε άλλα μηχανήματα επί του σκάφους. Το εν λόγω πλοίο, αγκυροβολημένο σε λιμάνι της Ασίας, έμεινε εκτός λειτουργίας για κάποιο διάστημα. (Baraniuk, 2022)

Επιπλέον, το 2018, διαπιστώθηκε ότι ένα ευρέως χρησιμοποιούμενο σύστημα παρακολούθησης και ελέγχου κινητήρα είχε σημαντικά ελαττώματα σχεδιασμού ασφάλειας. Από τις αναφορές προέκυψαν ότι ο ελεγκτής κινητήρα Auto-Maskin DCU 210E RP 210E και η εφαρμογή Marine Pro Observer είχαν αρκετές ευπάθειες και ταξινομήθηκαν ως κρίσιμα. Ο χειρισμός μιας άγνωστης εισόδου οδηγεί σε μια ευπάθεια αποκάλυψης πληροφοριών. Οι συσκευές μεταδίδουν ευαίσθητα ή κρίσιμα για την ασφάλεια δεδομένα σε καθαρό κείμενο σε ένα κανάλι επικοινωνίας που μπορούν να εκμεταλλευτούν μη εξουσιοδοτημένοι παράγοντες. (AUTO-MASKIN DCU 210E/RP-210E/MARINE PRO OBSERVER ANDROID APP INFORMATION DISCLOSURE, 2022)

Οι μονάδες έχουν πολλά τρωτά σημεία ελέγχου ταυτότητας και κρυπτογράφησης που μπορούν να επιτρέψουν στους εισβολείς να έχουν πρόσβαση σε αυτές. Ένας εισβολέας μπορεί να εκμεταλλευτεί αυτήν την ευπάθεια για να παρατηρήσει πληροφορίες σχετικά με διαμορφώσεις, ρυθμίσεις, αισθητήρες εν χρήσει και άλλες πληροφορίες. Επίσης μπορεί να στείλει αυθαίρετες πληροφορίες ελέγχου ModBus στις μονάδες κινητήρα. (Auto-Maskin DCU 210E RP 210E and Marine Pro Observer App, 2022)

Σημαντικό ρόλο στον εντοπισμό και την επίλυση προβλημάτων διαδραματίζουν και οι ίδιοι οι μηχανικοί με τη γνώση και την εμπειρία που διαθέτουν να ερμηνεύουν τους συναγερμούς. Σε αντίθετη περίπτωση, ενδέχεται να προκύψουν λάθη. Για παράδειγμα, μία αναφορά σχετικά με τη διερεύνηση του ατυχήματος του πλοίου Savannah Express κατέληξε στο συμπέρασμα ότι οι μηχανικοί απέτυχαν να συνειδητοποιήσουν ότι τα «υποδεικνύοντα σφάλματα ταχύμετρου δεν ήταν η βασική αιτία της βλάβης του κινητήρα» και παρερμήνευσαν τη σχέση μεταξύ των συναγερμών ταχύμετρου και των συναγερμών υδραυλικής πίεσης λόγω της ανεπαρκούς κατανόησης των συστημάτων του κινητήρα.

Τα λάθη συχνά προκύπτουν είτε από παρερμηνείες του συστήματος από ανεπαρκή κατανόηση από τους χειριστές του όπως στην περίπτωση του Savannah Express είτε από αλλοίωση των δεδομένων του ίδιου του συστήματος. Το σίγουρο πάντως είναι ότι η συνεχής εμφάνιση καινοτόμων λύσεων τεχνολογίας πληροφοριών (IT), τεχνολογικών τεχνουργημάτων αιχμής και προηγμένων gadgets που στοχεύουν στην παροχή υποστήριξης αποφάσεων θέτουν στο επίκεντρο την ανάγκη για περισσότερες γνωστικές και πρακτικές απαιτήσεις. (Man, Lundh, & MacKinnon, 2022)

3.4.2 BMWS

Στην Κύπρο, και πιο συγκεκριμένα στην Λάρνακα βρίσκεται βυθισμένο το πλοίο Zenobia, το οποίο ανατράπηκε κατά τη διάρκεια του ταξιδιού του από το Μάλμε προς τη Συρία. Καθώς το πλοίο πλησίαζε στην Ελλάδα, άρχισε να αποκτάει κλίση προς τα αριστερά. Προφανώς μια δυσλειτουργία του υπολογιστή προκαλούσε την άντληση υπερβολικού νερού στις δεξαμενές έρματος. Με το πρόβλημα να φαίνεται ότι ήταν υπό έλεγχο, το πλοίο συνέχισε για Κύπρο. Ενώ βρισκόταν στο λιμάνι της Λάρνακας, όμως, η κλίση επανήλθε και ο καπετάνιος έλαβε εντολή να βγάλει το πλοίο από το λιμάνι σε περίπτωση που βυθιζόταν και γινόταν κίνδυνος για άλλα πλοία.

Καθώς ήταν αγκυροβολημένο στην ανοικτή θάλασσα, η κλίση αυξήθηκε και ο καπετάνιος διέταξε το πλήρωμα να αποβιβαστεί από το πλοίο. Τα ξημερώματα της 7ης Ιουνίου 1980, το Zenobia ανατράπηκε και βυθίστηκε. (Newman, 2020) Η πιο δημοφιλής θεωρία για τη βύθιση του πλοίου περιλαμβάνει το ηλεκτρονικό σύστημα έρματος, το οποίο φαινόταν να έχει αναπτύξει ένα σφάλμα. Μια ομάδα συντήρησης στάλθηκε στο πλοίο για να διορθώσει το εν λόγω πρόβλημα και

η κλίση μειώθηκε με επιτυχία σε μόλις δύο βαθμούς. Όμως δεν κράτησε για πολύ αφού επανήλθε, με αποτέλεσμα την μετατόπιση του φορτίου και τη βύθιση του πλοίου. (HHVFerry, 2022)

Ένα πιο πρόσφατο γεγονός ήταν τον Γενάρη του 2015 όπου το Hoegh Osaka, σκάφος 51.000 τόνων, αναχώρησε από το Σαουθάμπτον και ανέπτυξε μια σημαντική κλίση προς τα δεξιά, προκαλώντας κάποια μετατόπιση φορτίου και συνακόλουθη πλημμύρα. Ο πιλότος έδωσε εντολή να «σβήσουν οι μηχανές» και το πλοίο συνέχισε να κλίνει υπό γωνία 40 μοιρών, αφήνοντας το πηδάλιο και την προπέλα έξω από το νερό. Από το εμπόρευμα τότε ένας κόφτης λύθηκε, πέφτοντας πάνω στην γάστρα του πλοίου και δημιουργώντας μια τρύπα, προκαλώντας την είσοδο θαλασσινού νερού.

Ο επικεφαλής επιθεωρητής του Τμήματος Διερεύνησης Ναυτικών Ατυχημάτων (Marine Accident Investigation Branch - MAIB), Steve Clinch, δήλωσε ότι η σταθερότητα του πλοίου δεν πληρούσε τις ελάχιστες διεθνείς απαιτήσεις και «κυρίως, η υποτιθέμενη κατανομή του έρματος στο πλοίο δεν είχε καμία ομοιότητα με την πραγματικότητα, με αποτέλεσμα το πλοίο να φύγει από το Σαουθάμπτον με υψηλότερο κέντρο βάρους από το κανονικό». (Hoegh Osaka ship was 'unstable' when it left Southampton port, 2022)

Αν και για τα παραπάνω δεν έχει ειπωθεί κάτι για κυβερνοεπίθεση θα μπορούσαν να είναι αποτέλεσμά της. Οι περισσότερες συσκευές συνδέονται με τον δίαυλο NMEA, όποτε η πρόσβασή σε αυτόν συνεπάγεται και την πρόσβαση στο σύστημα ελέγχου έρματος. Με την παροχή απομακρυσμένου ελέγχου των συστημάτων αυτών, ένας εισβολέας θα μπορούσε απλά να στείλει τα κατάλληλα σειριακά δεδομένα στους ελεγκτές της αντλίας έρματος, αναγκάζοντας τες να προσθέτουν ή να αφαιρούν νερό.

Βέβαια, υπάρχει η περίπτωση αυτή η αλλαγή στο έρμα να μην είναι αρκετή για την βύθιση του σκάφους. Το παραπάνω σενάριο θα μπορούσε να εξελιχθεί πολύ χειρότερα εάν μέσα σε αυτό συνδυαζόταν η αλλαγή στη σταθερότητα κατά τη στροφή. Αυτό θα μπορούσε να επιτευχθεί στέλνοντας μήνυμα NMEA στον αυτόματο πιλότο ή στο τιμόνι που δίνει εντολή για στροφή προς την ανάλογη κατεύθυνση. (Threat Post, 2022)

3.4.3 Bay/Stowage Plan

Όπως και προηγουμένως δεν υπάρχουν αρκετά έγγραφα τα οποία να αναφέρουν επιθέσεις στα συστήματα του πλοίου έτσι και στο σύστημα φορτο-εκφόρτωσης. Αυτό μπορεί να συμβαίνει είτε επειδή δεν έχει πέσει κανένα θύμα κυβερνοεπίθεσης είτε επειδή οι πληροφορίες αυτές είναι εμπιστευτικές και η δημοσίευσή τους θα προκαλούσε πλήγμα στο κύρος των εταιρειών. Ένα επίκαιρο γεγονός είναι η ανατροπή του Sea Eagle, ενός φορτηγού πλοίου, στο λιμάνι Iskenderun της Τουρκίας. Στις 18 Σεπτεμβρίου του 2022, κατά την εκφόρτωση εμπορευματοκιβωτίων, εισχώρησε νερό στο πλοίο με αποτέλεσμα την απώλεια της σταθερότητάς του, την ανατροπή του και την πτώση εμπορευματοκιβωτίων στην θάλασσα. (Voytenko, 2022)

Σε μία από τις έρευνες που έχει κάνει ο Munro αναφέρει ένα περιστατικό που συνέβη σε έναν συνάδελφό του αναφορικά με το ότι τα σχέδια φόρτωσης από το πλοίο στο λιμάνι ανταλλάσσονται μέσω δισκέτας ή/και USB. Βασικά, χάλασε ο υπολογιστής του πλοίου που υποστήριζε και τις 2 θύρες και το λιμάνι υποστήριζε μόνο δισκέτες. Χωρίς δισκέτα δεν υπήρχε τρόπος μεταφοράς των σχεδίων φόρτωσης μεταξύ του πλοίου και του λιμένα, οπότε υπήρχε αναμονή μέχρι να μεταφερθούν όλα με email, προκειμένου να ξεκινήσει η εκφόρτωση. Το λιμάνι, η ακτή, το πλοίο κ.λπ. όλα πρέπει να συνεργαστούν για να είναι επιτυχές το σχέδιο, αν και είναι σημαντικό να σημειωθεί ότι ο τελευταίος λόγος για τη φόρτωση είναι πάντα του πλοίου. (Munro, Sinking container ships by hacking load plan software, 2022)

Τον Αύγουστο του 2011, οι Ναυτιλιακές Γραμμές Ισλαμικής Δημοκρατίας του Ιράν (IRISL), υπέστησαν ζημιές από μια κυβερνοεπίθεση, θέτοντας σε κίνδυνο ολόκληρο τον στόλο (170 πλοία) και τα συστήματα που βρίσκονται στην ξηρά. Ως αποτέλεσμα, χάθηκαν οι πληροφορίες και τα δεδομένα επικοινωνίας πελατών. Επίσης, η εταιρεία έχασε όλο το εσωτερικό δίκτυο επικοινωνίας, υπέστη σημαντικές διακοπές στις λειτουργίες, καταστρέφοντας όλες τις ημερομηνίες που σχετίζονται με ναύλους, φόρτωση, εκφόρτωση, πληροφορίες φορτίου, τοποθεσίες ολόκληρου του στόλου. Κατά συνέπεια, κανείς δεν μπορούσε να γνωρίζει τη σωστή θέση κάθε κοντέινερ και η

παρακολούθηση του καθενός έγινε πιο δύσκολη και απρόβλεπτη. Έτσι, ένας τεράστιος όγκος φορτίου παραδόθηκε σε λάθος προορισμούς ή ακόμη και χάθηκε.

Μια άλλη κυβερνοεπίθεση έγινε κατά του αυστραλιανού συστήματος φορτίου Custom and Border Protection το 2012. Ο επιτιθέμενος με πρόσβαση στο σύστημα φορτίου μπόρεσε να χρησιμοποιήσει τη μεταφορά του για να διακινήσει ναρκωτικά. Με τη δυνατότητα παρακολούθησης των κινήσεων φορτίου, ο εισβολέας ήταν σε θέση να προσδιορίσει πότε το κοντέινερ χαρακτηρίστηκε ως ύποπτο ή κακόβουλο από την αστυνομία και να εγκαταλείψει τη λειτουργία του.

Ένα ακόμη ενδιαφέρον περιστατικό αφορούσε το λιμάνι της Αμβέρσας στο Βέλγιο, ένα από τα μεγαλύτερα λιμάνια της Ευρώπης και του κόσμου, το οποίο χρησιμοποιήθηκε για λαθρεμπόριο ναρκωτικών στα τέλη του 2013. Η επιχείρηση λάμβανε δράση από το 2011 και ανακαλύφθηκε επειδή ένα κοντέινερ εξαφανίστηκε από το λιμάνι. Ο χάκερ, μέσω ενός ιού, διείσδυσε στο ηλεκτρονικό σύστημα παρακολούθησης και απελευθέρωσης φορτίου τουλάχιστον δύο εταιρειών που λειτουργούν στο λιμάνι, αποκτώντας πλήρη τηλεχειρισμό και πρόσβαση στο τερματικό σύστημα. Στην πραγματικότητα, το δίκτυο υπολογιστών του λιμανιού είχε κατασκοπευθεί όταν το δίκτυο φέρεται να δέχθηκε κακόβουλο λογισμικό, συγκεκριμένα ένα keylogger (το οποίο επέτρεπε στους χάκερ να καταγράφουν τα πλήκτρα που χρησιμοποιούσαν οι χειριστές φόρτωσης/εκφόρτωσης και έτσι να αποκτήσουν ονόματα χρήστη και κωδικούς πρόσβασης).

Ο χάκερ ήταν σε θέση να εντοπίσει εμπορευματοκιβώτια αποστολής όπου είχαν κρυφτεί ναρκωτικά και να τα απελευθερώσει σε έναν φορτηγατζή χωρίς την άδεια ή τη γνώση του λιμανιού ή των ναυτιλιακών γραμμών. Στη συνέχεια ο δράστης διέγραψε πληροφορίες και την ύπαρξη του κοντέινερ από το λιμενικό σύστημα. Όταν οι αρχές αποκάλυψαν την επίθεση, βρήκαν 1044 κιλά κοκαΐνης, 1099 κιλά ηρωίνης, όπλα και περισσότερα από 1,3 εκατομμύρια ευρώ σε μια βαλίτσα, που αντιπροσωπεύουν μόνο ένα μικρό μέρος της ποσότητας που μπόρεσαν να μεταφέρουν οι εγκληματίες για δύο χρόνια. (Silgado, 2022) (Kapalidis, 2022)

Ορισμένα σχόλια του Munro σχετικά με την επίθεση στο λιμάνι της Αμβέρσας:

1. Για πρώτη φορά στο λιμάνι τα εμπορευματοκιβώτια απελευθερώνονται στους μεταφορείς με την παροχή ενός κωδικού PIN, το οποίο κοινοποιείται με διαφορετικούς τρόπους όπως email ή εφαρμογή για κινητά.
2. Οι εγκληματίες συνειδητοποίησαν ξεκάθαρα ότι το σύστημα αυτό - αποδέσμευσης PIN - ήταν ευάλωτο σε συμβιβασμούς.
3. Μέσω phishing attack οι κωδικοί PIN παραβιάστηκαν.
4. Υπάρχει πιθανότητα οι εγκληματίες να είχαν εξαγάγει εμπιστευτικές πληροφορίες από υπαλλήλους. (Munro, Container theft, the legal system and poor maritime security, 2022)

3.4.4 Security Systems

Τον Φεβρουάριο του 2017 πειρατές χάκερ απέκτησαν τον έλεγχο των συστημάτων πλοήγησης ενός γερμανικού πλοίου μεταφοράς εμπορευματοκιβωτίων, 8.250 teu που εκτελούσε δρομολόγιο από την Κύπρο στο Τζιμπουτί. Το σύστημα πληροφορικής του σκάφους παραβιάστηκε εντελώς με τον καπετάνιο να μην μπορεί να κάνει ελιγμούς. Αν και οι λεπτομέρειες είναι περιορισμένες, σύμφωνα με την πηγή, η 10ωρη επίθεση που πραγματοποιήθηκε είχε ως απώτερο σκοπό να το κατευθύνουν σε μια περιοχή όπου μπορούσαν να επιβιβαστούν και να το καταλάβουν. Το πλήρωμα προσπάθησε να ανακτήσει τον έλεγχο του συστήματος πλοήγησης, αλλά χρειάστηκαν πιο δραστικά μέτρα από έμπειρους γνώστες της πληροφορικής, οι οποίοι τελικά κατάφεραν να το επαναφέρουν σε λειτουργία μετά από ώρες εργασίας. (Asket, 2022) (Resilient Navigation and Timing Foundation, 2022)

Επιπροσθέτως, μια μεγάλη ιταλική ομάδα ασφάλειας υπολογιστών κατά τη διάρκεια της διάσκεψης ασφαλείας Hack In the Box 2013 δήλωσαν πως το AIS μπορεί εύκολα να χακαριστεί με σκοπό την εξαφάνιση ενός πλοίου ή και την αλλαγή της διαδρομής του. Για να το αποδείξουν, έδειξαν πώς μπόρεσαν να δημιουργήσουν ένα φανταστικό πλοίο στα ανοιχτά του ιταλικού λιμανιού της Γένοβας. Εκτός από την καταχώρηση πλαστών πλοίων σε γεωγραφικές συντεταγμένες ανέφεραν ότι μπορούν να δημιουργήσουν πλαστές ειδοποιήσεις σύγκρουσης και μετεωρολογικές προβλέψεις.

Σε μια περίπτωση έδειξαν πώς ένας εισβολέας θα μπορούσε να μεταμφιεστεί σε λιμενική αρχή και να πει στα πλοία να αλλάξουν τις ραδιοφωνικές συχνότητες AIS, απομονώνοντάς τα από τον υπόλοιπο κόσμο. Ονομάζοντάς το άλμα συχνότητας (frequency-hopping), ο ανεξάρτητος ερευνητής Alexandro Pasta είπε πως οι λιμενικές αρχές έχουν την εξουσία να ελέγχουν εξ αποστάσεως το AIS για εναλλαγή συχνοτήτων. Έτσι με το παραπάνω θα ήταν δυνατόν να απομονωθεί εντελώς ένα σκάφος και μόνο ο επιτιθέμενος θα γνωρίζει την κατάσταση του πλοίου, καθιστώντας το ευάλωτο σε φυσικές πειρατικές επιθέσεις. (Easy hacking on the AIS system puts global shipping at risk, 2022)

Μια από τις πιο σοβαρές υποθέσεις που έχει δημοσιοποιηθεί αφορά έναν παγκόσμιο ναυτιλιακό όμιλο ετερογενών δραστηριοτήτων που παραβιάστηκε από πειρατές, οι οποίοι ήθελαν να μάθουν ποια πλοία μετέφεραν το συγκεκριμένο φορτίο που σχεδίαζαν να καταλάβουν. Η ομάδα κυβερνοασφάλειας της εταιρείας τηλεπικοινωνιών Verizon περιγράφει το συμβάν. «Επιβιβάζονταν σε ένα σκάφος, εντόπιζαν με γραμμοκώδικα συγκεκριμένα περιζήτητα κιβώτια που περιείχαν τιμαλφή, έκλεβαν το περιεχόμενο αυτού του κιβωτίου και στη συνέχεια αναχωρούσαν από το πλοίο χωρίς περαιτέρω επεισόδια». (Baraniuk, 2022)

Ακόμη, τα συστήματα καμερών ασφαλείας έχουν γίνει στόχος κακόβουλων χρηστών. Το 2017, μια ναυτιλιακή εταιρεία με έδρα τη Λουϊζιάνα ανέφερε ότι οι κάμερες ενός μέρους του στόλου της είχαν παραβιαστεί. Σε αυτήν την περίπτωση, τα συστήματα Dahua DHI-HCVR προσπελάστηκαν εξ αποστάσεως μέσω του Ιστού, εκμεταλλευόμενα μια αδυναμία στις διαδικασίες ελέγχου ταυτότητας της κάμερας. Ρυθμίστηκαν οι επιλογές αντίθεσης της κάμερας για να σκουρύνουν την ανάλυση, τυφλώνοντας ουσιαστικά την κάμερα. Άλλες αναφορές υπογράμμισαν ότι αυτή η ίδια κάμερα είχε προηγούμενα ζητήματα όπως ότι οι απομακρυσμένοι χρήστες μπορούσαν να παρακάμψουν τον έλεγχο ταυτότητας και άλλα 13 τρωτά σημεία που χρονολογούνταν από το 2013.

Το 2018, εικόνες κάμερας από αλιευτικό σκάφος Mist με σημαία Μαρόκου δημοσιεύτηκαν στο Twitter και δηλώθηκε ότι τραβήχτηκαν εξ αποστάσεως μέσω Διαδικτύου. Το παραπάνω δεν μπόρεσε να επιβεβαιωθεί λόγω έλλειψης μεταδεδομένων, αλλά οι εικόνες φάνηκαν νόμιμες. Όπως όλες οι συσκευές IoT, αυτές οι λεγόμενες έξυπνες κάμερες είναι τόσο ασφαλείς όσο τις κάνει ο εγκαταστάτης και ο διαχειριστής του συστήματος, και ακόμη και αυτό εξαρτάται από τον έλεγχο του χρήστη που ενσωματώνει ο κατασκευαστής στις συσκευές. (Kessler & Zorri, 2022)

3.4.5 VDR

Το VDR ισοδυναμεί με το μαύρο κουτί ενός αεροσκάφους, αλλά η σύγκριση τελειώνει εκεί. Σε μια πτήση, ακόμη και ο κυβερνήτης δεν μπορεί να πειράξει το μαύρο κουτί, το οποίο συνήθως ρίχνει φως στην αιτία ενός ατυχήματος. Δεν φαίνεται το ίδιο όμως και στην υπόθεση Enrica Lexie. Στις 15 Φεβρουαρίου 2012, δύο Ινδοί ψαράδες σκοτώθηκαν στα ανοικτά των ακτών της Ινδίας, στο St. Antony. Η Ινδία ισχυρίστηκε ότι οι δύο Ιταλοί πεζοναύτες που επέβαιναν στο υπό ιταλική σημαία εμπορικό πετρελαιοφόρο σκότωσαν τους ψαράδες ενώ οι ίδιοι υποστήριξαν ότι βρίσκονταν σε διεθνή ύδατα και ότι είχαν ανοίξει πυρ εναντίον ενός σκάφους νομίζοντας ότι ήταν πειρατές. Αυτό θα μπορούσε να είχε επαληθευτεί από το VDR, αλλά μια προκαταρκτική έρευνα για το περιστατικό διαπίστωσε ότι το VDR είχε παραβιαστεί. (The times of India, 2022)

Ένα ακόμη περιστατικό έγινε την 1η του Μάρτη το 2012, όταν το φορτηγό πλοίο MV Prabhu Daya ενεπλάκη σε ένα περιστατικό εμβολής με μία αλιευτική τράτα στα ανοιχτά της ακτής της Kerala, και διέφυγε από τον τόπο της εμπλοκής αφήνοντας πίσω τα θύματά του. Επίσης, ένα ακόμη συμβάν με το εν λόγω πλοίο είναι η πτώση του δεύτερου αξιωματικού Prasobh Sugathan από το πλοίο κοντά στο Trincomalee στην ανατολική Σρι Λάνκα. Ένα από τα μέλη του πληρώματος του πλοίου φέρεται να εισέβαλε (hacked into) στο Furuno VR-3000 VDR και διέγραψε όσα θα μπορούσαν να ήταν ενοχοποιητικά δεδομένα.

Ο αξιωματικός ανέφερε πως το βασικό σύστημα υπολογιστή είχε μολυνθεί από ιό και δεν διέθετε κατάλληλο λογισμικό προστασίας. Κατά την επαλήθευση, διαπιστώθηκε ότι το σύστημα ηχογράφησης φωνής ήταν άθικτο, υποδεικνύοντας ότι κάποιος μπορεί να είχε διαγράψει τις ηχογραφήσεις που αφορούσαν τις κρίσιμες στιγμές. Ένα από τα μέλη του πληρώματος είπε ότι το πλήρωμα ενήργησε με ύποπτο τρόπο μετά την πτώση του Sugathan στη θάλασσα, καθώς οι

επιχειρήσεις έρευνας και διάσωσης συνεχίστηκαν μόνο για λίγες ώρες και όχι σύμφωνα με τους κανονισμούς που ορίζουν ότι οι έρευνες πρέπει να συνεχιστούν για 48 έως 72 ώρες (The Hindu, 2022) (NDTV, 2022)

3.5 Περιστατικά στο Σύστημα Θαλάσσιων Μεταφορών

3.5.1 Επιβατηγά πλοία

Βέβαια, να μην ξεχνάμε επίσης και την ύπαρξη των επιβατηγών πλοίων (cruise ships) που μπορεί να αποτελούνται από 1200 άτομα πληρώματος, και από περισσότερο από 2000 επιβάτες. Για να μην έχει δυσαρεστημένους πελάτες ένα τέτοιο πλοίο όσον αφορά την διασκέδασή τους, πρέπει να είναι και κατάλληλα εξοπλισμένο με τα αντίστοιχα Wi-Fi Access Points. Αυτό γιατί δεν είναι μόνο ένα πλωτό μέσω μεταφοράς, αλλά και παράλληλα ένα ξενοδοχείο, ένα κέντρο ψυχαγωγίας, ένα εμπορικό κέντρο. Ως εκ τούτου, καθίστανται περισσότερο ευάλωτα σε κυβερνοεπιθέσεις (Area41, 2020).

Έτσι, όπως ένα πλοίο χωρίζεται σε διαμερίσματα για ασφάλεια από τυχόν πυρκαγιά ή πλημύρα, ανάλογα με το μέγεθος του, έτσι και το δίκτυο χωρίζεται σε τμήματα απομακρυσμένων σημείων διανομής (“RDP”). Το καθένα από αυτά διακρίνεται σε υποδίκτυα που ονομάζονται «Διακόπτες καμπίνας» (“Cabin Switches”), τα οποία μπορεί να συνδέονται μεταξύ τους μέσω ενσύρματου ethernet οπτικών ινών. Κάθε διακόπτης σε κάθε καμπίνα μπορεί να παρέχει τηλεόραση πρωτοκόλλου διαδικτύου IPTV[40], μεταδίδοντας ζωντανά θεατρικές παραστάσεις στο πλοίο μέσω IP σε ένα VLAN συνδεδεμένο στην καμπίνα.

Επίσης, υπάρχει ένα τηλέφωνο VOIP, καθώς και το σύστημα ελέγχου καμπίνας το οποίο ελέγχει τον φωτισμό, το HVAC[41], την πρόσβαση στην πόρτα και το ζεστό νερό. Στην έρευνά του, ο Andrew Tierney, ανιχνευτής ασφάλειας πληροφορικής που δημοσίευσε στο Defcon28, μέσω αυτών των δυνατοτήτων που του παρέχονταν στο πλοίο, δηλαδή από το guest Wi-Fi κατάφερε να συνδεθεί στο VSAT και μάλιστα με πρόσβαση root. Πιο συγκεκριμένα, είχε την δυνατότητα να αναχαιτίσει οτιδήποτε συμβαίνει εντός και εκτός του σκάφους.

Τα περισσότερα κρουαζιερόπλοια διαθέτουν ενσωματωμένο σύστημα ελέγχου και παρακολούθησης ή ICMS (Integrated Control and Monitoring System) που τρέχει όλες τις οθόνες στη γέφυρα, καθώς και τα HMI και τα PLC κάτω στο μηχανοστάσιο. Συνδέει όλο τον βιομηχανικό εξοπλισμό του πλοίου – την ισχύ, τις γεννήτριες, την πρόωση, το πηδάλιο, τα πάντα συγκρατούνται από αυτό το πολύπλοκο σύστημα. Επειδή τα πλοία είναι πιο σύνθετα, για τον έλεγχο του έρματος υπάρχει το Load Computer (υπολογιστής φόρτωσης). Ο Tierney με τον συνεργάτη του κατάφεραν να εισβάλουν σε αυτόν τον υπολογιστή και στην πορεία βρήκαν επίσης έναν τρόπο να προκαλέσουν άρνηση υπηρεσίας σε συστήματα γέφυρας που είναι απαραίτητα για τις καθημερινές λειτουργίες.

Αυτό συνέβη γιατί ο υπολογιστής αυτός χρειάζεται πρόσβαση στο δίκτυο. Γενικά, πάνω σε ένα πλοίο είναι δύσκολο να δημιουργηθούν νέες καλωδιώσεις, οπότε αρκεί μία καλωδιακή σύνδεση του υπολογιστή στο ίδιο δίκτυο από οποιοδήποτε άλλο μέρος και οποιοσδήποτε θα μπορεί να συνδεθεί στο σύστημα,. Έπειτα, επειδή πρέπει να είναι ευκολοπροσβάσιμοι οι υπολογιστές στην γέφυρα, συνήθως έχουν και απλούς κωδικούς. Στην συνέχεια, μέσω σειριακού μετατροπέα και εισαγωγής μετρήσεων δεξαμενής στο δίκτυο ελέγχου, θα μπορούσαν να στέλνουν ανεπιθύμητη αλληλογραφία στο ICMS, spam σε όλες τις οθόνες στη γέφυρα δίνοντάς τους λάθος μετρήσεις δεξαμενής έρματος (Defcon28, 2022).

---

40 Η τηλεόραση Πρωτοκόλλου Διαδικτύου (IPTV) είναι η παροχή περιεχομένου τηλεόρασης μέσω δικτύων πρωτοκόλλου διαδικτύου (IP). Πρόκειται για παραδοσιακές επίγειες, δορυφορικές και καλωδιακές τηλεοπτικές μορφές. Σε αντίθεση με τα ληφθέντα μέσα, η IPTV προσφέρει τη δυνατότητα συνεχούς ροής των πηγών μέσων. (Wikipedia, 2022)

41 Heating, ventilation, and air conditioning

3.5.2 Ναυτιλιακές εταιρείες

Στον ναυτιλιακό κλάδο όμως, δεν υπάρχουν μόνο τα πλοία αλλά και τα λιμάνια, οι ναυτιλιακές εταιρίες αλλά και οι προμηθευτές αυτών. Απευθυνόμενος σε φορείς εκμετάλλευσης λιμένων και τερματικών σταθμών κατά τη διάρκεια ενός διαδικτυακού φόρουμ, ο Robert Rizika, επικεφαλής επιχειρήσεων Βόρειας Αμερικής της Naval Dome με έδρα τη Βοστώνη ανέφερε πως οι κυβερνοεπιθέσεις στα συστήματα λειτουργικής τεχνολογίας της ναυτιλιακής βιομηχανίας έχουν αυξηθεί κατά 900% τα τελευταία τρία χρόνια. Είπε ότι το 2020 ένας φορέας εκμετάλλευσης αγωγού φυσικού αερίου με έδρα τις ΗΠΑ και η ναυτιλιακή εταιρεία MSC έχουν πληγεί από κακόβουλο λογισμικό. Το αποτέλεσμα του πλήγματος της MSC ήταν να κλείσουν τα κεντρικά γραφεία του πλοιοκτήτη στη Γενεύη για πέντε ημέρες.

Τα λειτουργικά συστήματα μιας μονάδας φορτίου που εδρεύει στις ΗΠΑ μολύνθηκαν με το Ryuk ransomware και τον Ιούνιο του 2020 τα OT συστήματα στο λιμάνι Shahid Rajee του Ιράν παραβιάστηκαν, περιορίζοντας όλες τις κινήσεις υποδομής, δημιουργώντας μεγάλες καθυστερήσεις. Επίσης, τόνισε δύο πτυχές του θέματος. Από την μία υπήρξε μεγάλο οικονομικό αντίκτυπο, θέτοντας σαν παράδειγμα τα δεκάδες φορτηγά πλοία και πετρελαιοφόρα που περίμεναν να φορτώσουν/εκφορτώσουν στο ιρανικό λιμάνι λόγω της επίθεσης που κατέστρεψε τους υπολογιστές που ρυθμίζουν την ροή. Από την άλλη έθιξε το περιβαλλοντολογικό αντίκτυπο, σκεπτόμενος ότι οι χάκερ μπορούν εύκολα να παρακάμψουν συστήματα και να προκαλέσουν διαρροές κατά την διάρκεια εργασιών ή αναμονής όλων αυτών των πλοίων στα λιμάνια. (Offshore Energy, 2022)

Τον Σεπτέμβριο του 2020, η CMA CGM έπεσε θύμα κυβερνοεπίθεσης. Μάλιστα οι ιστότοποι τόσο του γαλλικού κολοσσού όσο και των θυγατρικών της είχαν «πέσει» όλο το Σαββατοκύριακο. «Ο Όμιλος CMA CGM (εξαιρουμένης της Ceva Logistics) αντιμετωπίζει κυβερνοεπίθεση, η οποία έχει επηρεάσει τους περιφερειακούς διακομιστές, καθιστώντας την εξωτερική πρόσβαση στις εφαρμογές μη διαθέσιμη. Η ομάδα IT εργάζεται προκειμένου να διασφαλίσει την ομαλή λειτουργία της επιχείρησης», ήταν το μήνυμα της εταιρείας. (Η CMA CGM, το τελευταίο θύμα κυβερνοεπίθεσης στη ναυτιλία , 2022)

Η Princess Cruises και η Holland America Line ενημέρωσαν για μια παραβίαση της ασφάλειας στον κυβερνοχώρο, κατά την οποία χάκερ είχαν πρόσβαση σε προσωπικές πληροφορίες, όπως διαβατήρια και αριθμούς κοινωνικής ασφάλισης επισκεπτών, πληρώματος και υπαλλήλων. Σύμφωνα με την Carnival Corp., τη μητρική εταιρεία των κρουαζιέρων Princess and Holland America, χάκερ απέκτησαν μη εξουσιοδοτημένη πρόσβαση σε λογαριασμούς email εργαζομένων μεταξύ 11 Απριλίου και 23 Ιουλίου 2019. Οι λογαριασμοί περιλάμβαναν τα προσωπικά δεδομένα όσων ταξίδεψαν και εργάστηκαν στα εν λόγω πλοία, εκθέτοντας διάφορα δεδομένα, όπως:

- Ονόματα,
- Διευθύνσεις,
- Αριθμοί Κοινωνικής Ασφάλισης,
- Πληροφορίες ταυτότητας, όπως αριθμοί διαβατηρίου και αριθμοί άδειας οδήγησης,
- Πιστωτικές κάρτες και πληροφορίες οικονομικών λογαριασμών,
- Πληροφορίες σχετικά με την υγεία.

Σχολιάζοντας την είδηση, ο Jim Van Dyke, συνιδρυτής και Διευθύνων Σύμβουλος της Breach Clarity, είπε ότι πρόκειται για μια δυσάρεστη παραβίαση. Το Breach Clarity αξιολόγησε το επίπεδο κινδύνου «επτά» στα δέκα τόσο για το Princess όσο και για το Holland America. (Holland America, Princess report cyber security breach, 2022)

Ένα περιστατικό που είχε συμβεί τον Οκτώβριο του 2018, το οποίο δημοσιεύθηκε στον περιοδικό Safety4Sea, ήταν η κυβερνοεπίθεση που δέχθηκε η Austal, μια παγκόσμια ναυπηγό-επισκευαστική εταιρία της Αυστραλίας και μάλιστα ο κύριος εργολάβος στον τομέα της άμυνας και ο εκλεκτός συνεργάτης της ναυτιλιακής τεχνολογίας. (Safety4Sea, 2018) Αυτό που συνέβη στην εταιρία είναι να πουληθούν διαπιστευτήρια χρηστών στο μαύρο διαδίκτυο, και από κει ο επιτιθέμενος να τα εκμεταλλευτεί για χρηματικό αντάλλαγμα από την εταιρία. Μέχρι εκείνο το διάστημα υπάλληλοι της εταιρίας αλλά και πελάτες δεν μπορούσαν να στείλουν email και να ανταλλάξουν δεδομένα. (IT News, 2022) Ακριβώς το ίδιο συνέβη, πάλι για λίτρα, και σε αρκετές ελληνικές ναυτιλιακές εταιρίες που χρησιμοποιούσαν τα συστήματα επικοινωνίας Danaos

Management Consultants. Πιο συγκεκριμένα, το 2021 την ημέρα του Halloween, μπλοκαρίστηκαν οι επικοινωνίες μεταξύ πλοίων, πρακτόρων, ναυλωτών κ.λπ. και χάθηκαν αρχεία με την αλληλογραφία τους. (MonoNews, 2022)

Μια από τις πιο γνωστές επιθέσεις που έχουν συμβεί στον ναυτιλιακό τομέα είναι αυτή της Maersk. Τον Ιούνιο του 2017, η AP Moller – Maersk έπεσε θύμα που προκλήθηκε από το κακόβουλο λογισμικό NotPetya και είχε ως αποτέλεσμα την διακοπή των δραστηριοτήτων οδηγώντας σε αδικαιολόγητες επιπτώσεις. Η κατάρρευση επηρέασε όλες τις επιχειρηματικές μονάδες της, συμπεριλαμβανομένων των θαλάσσιων μεταφορών εμπορευματοκιβωτίων, λιμενικών και ρυμουλκών, παραγωγής πετρελαίου και φυσικού αερίου, υπηρεσιών γεώτρησης και πετρελαιοφόρων. Η ανάκαμψη ήταν γρήγορη, αλλά μέσα σε σύντομο χρονικό διάστημα ο οργανισμός υπέστη οικονομικές απώλειες έως και 300 εκατ. δολάρια καλύπτοντας, μεταξύ άλλων, απώλεια εσόδων, κόστος αποκατάστασης πληροφορικής και έκτακτες δαπάνες που σχετίζονται με τις λειτουργίες. (Safety4Sea, 2022)

Σε μια σειρά από χακαρίσματα υψηλού προφίλ στην Αμερική, συμπεριλαμβανομένων των Deloitte, Yahoo και Equifax, οι Clarksons, ο μεγαλύτερος ναυλομεσίτης στον κόσμο, υπέστη κυβερνοεπίθεση τον Νοέμβριο του 2017 μέσω μιας «μη εξουσιοδοτημένης πρόσβασης που αποκτήθηκε από έναν μοναδικό και απομονωμένο λογαριασμό χρήστη», ανέφερε η εταιρεία. Οι έρευνες για την παραβίαση της ασφάλειας στον κυβερνοχώρο ξεκίνησαν αμέσως μετά την ανακάλυψη. Ευτυχώς το συμβάν αυτό δεν επηρέασε τόσο τους ετήσιους προϋπολογισμούς τους αντί αυτού όμως συνέβαλε στην ανάπτυξη καλύτερων μέτρων ασφαλείας. (Kapalidis, 2022)

Μια άλλη υπόθεση αφορούσε την BW Group Singapore, μια από τις μεγαλύτερες ναυτιλιακές εταιρείες στον κόσμο με στόλο που περιλαμβάνει δεξαμενόπλοια, πλοία μεταφοράς χύδην φορτίου, αερίου και υπεράκτιες πλωτές μονάδες. Η επίθεση ήταν σοβαρή. Το σύστημα υπολογιστή της εταιρείας παραβιάστηκε, γεγονός που οδήγησε στην προσωρινή αναστολή των συστημάτων Διαδικτύου και Intranet. Κατά τη διάρκεια της επίθεσης, το σύστημα της εταιρείας ήταν απρόσιτο από έξω, επηρεάζοντας τις λειτουργίες της, συμπεριλαμβανομένων λιμένων, εμπορευματοκιβωτίων, πλοίων πετρελαιοφόρων, ρυμουλκών, εργασιών γεώτρησης και παραγωγής πετρελαίου και φυσικού αερίου, προκαλώντας οικονομικές ζημίες εκατομμυρίων δολαρίων. (Silgado, 2022)

Ένα ακόμη παράδειγμα είναι η Hapag-Lloyd που ενημέρωσε ότι η ομάδα ασφαλείας πληροφορικής της βρήκε ένα αντίγραφο του ιστοτόπου της στο διαδίκτυο, το οποίο είναι πολύ πιθανό να χρησιμοποιηθεί για επίθεση spear phishing. Αυτό σημαίνει ότι τα μηνύματα ηλεκτρονικού ταχυδρομείου χρησιμοποιούνται για να ανακατευθύνουν τους χρήστες σε αυτόν τον ιστότοπο και όταν συνδέονται με τα προσωπικά τους δεδομένα, αυτά στη συνέχεια αξιοποιούνται από εγκληματίες. Αυτού του είδους οι ψεύτικοι ιστότοποι είναι συνήθως ένα αντίγραφο των πραγματικών σελίδων και επομένως μπορούν συνήθως να αναγνωριστούν ως κακόβουλες σελίδες μόνο μέσω του τομέα ή της διεύθυνσης Διαδικτύου. (Safety4Sea T. E., How to identify phishing emails, 2022)

Τέλος, όταν το προσωπικό της CyberKeel ερεύνησε τη δραστηριότητα ηλεκτρονικού ταχυδρομείου σε μια μεσαίου μεγέθους ναυτιλιακή εταιρεία, έκανε μια συγκλονιστική ανακάλυψη. «Κάποιος είχε χακάρει τα συστήματα της εταιρείας και είχε φυτέψει έναν μικρό ιό», εξηγεί ο συνιδρυτής Λαρς Τζένσεν. «Στη συνέχεια παρακολουθούσε όλα τα email του οικονομικού τμήματος». Κάθε φορά που ένας από τους προμηθευτές καυσίμων της εταιρείας έστελνε ένα email ζητώντας πληρωμή, ο ιός απλώς άλλαζε το κείμενο του μηνύματος προτού διαβαστεί, προσθέτοντας έναν διαφορετικό αριθμό τραπεζικού λογαριασμού. «Πολλά εκατομμύρια δολάρια», λέει ο κ. Jensen, μεταφέρθηκαν στους χάκερ προτού η εταιρεία το συνειδητοποιήσει. (Baraniuk, 2022)

3.5.3 Λιμάνια

Οι πιο γνωστές κυβερνοεπιθέσεις τα τελευταία 10 χρόνια στα λιμάνια είναι:

Στις 30 Ιουνίου 2017, το λιμάνι του Ρότερνταμ μολύνθηκε από το Petrwrap, μια τροποποιημένη έκδοση του NotPetya ransomware. Συγκεκριμένα, δύο τερματικοί σταθμοί εμπορευματοκιβωτίων που διαχειρίζεται η APMT, θυγατρική του ομίλου Møller-Maersk, είδαν τις δραστηριότητές τους

να έχουν παραλύσει εντελώς. Πιο συγκεκριμένα, το ολλανδικό τηλεοπτικό κανάλι RTV Rijnmond αναφέρει ότι εκτός από τα 2 τερματικά που βρίσκονται στο Ρότερνταμ, είχαν παραβιαστεί και άλλα 15 με τους υπολογιστές να έχουν μολυνθεί από ransomware που κρυπτογραφούσε τους σκληρούς δίσκους. (Gronholt-Pedersen, 2022) Ένα χρόνο μετά, το λιμάνι του Long Beach στις Ηνωμένες Πολιτείες ήταν το πρώτο που χτυπήθηκε, συγκεκριμένα ένας τερματικός σταθμός που ανήκε στην China Ocean Shipping Company (COSCO), είδε το σύστημα πληροφοριών της να έχει μολυνθεί από ransomware.

Στις 20 Σεπτεμβρίου 2018, το λιμάνι της Βαρκελώνης ήταν το επόμενο που χτυπήθηκε. Από τότε έχουν διαρρεύσει ελάχιστες πληροφορίες, αλλά φαίνεται ότι τα εσωτερικά συστήματα πληροφορικής δέχθηκαν επίθεση, γεγονός που επηρέασε τις διαδικασίες φορτοεκφόρτωσης. Μια εβδομάδα αργότερα, το λιμάνι του Σαν Ντιέγκο διαταράχθηκε επίσης από μια «πολύ εξελιγμένη» κυβερνοεπίθεση, που προκάλεσε περιορισμένη λειτουργικότητα, κάτι που επηρέασε την εξυπηρέτηση του λιμανιού στους τομείς των αδειών στάθμευσης, των αιτημάτων δημοσίων αρχείων και των επιχειρηματικών υπηρεσιών. (Two Iranians behind Port of San Diego cyber attack, 2022)

Το 2018 το λιμάνι του Βανκούβερ υπέστη brute force επίθεση τον Οκτώβριο, λίγους μήνες μετά από άλλη επίθεση του ίδιου τύπου. Σύμφωνα με τον γαλλικό ιστότοπο cybermaretique.fr, σχεδόν 225.000 λογαριασμοί χρηστών εξετάστηκαν εκείνη την ημέρα, αν και δεν δόθηκαν περισσότερες πληροφορίες σχετικά με τις συνέπειες αυτής της άρνησης υπηρεσιών επίθεσης. Τον Μάρτιο του 2020, το λιμάνι της Μασσαλίας ήταν το επόμενο θύμα που χτυπήθηκε με ransomware, πιο συγκεκριμένα το Mespinoza/Pysa. Στην περίπτωση αυτή, οι θαλάσσιες υποδομές δεν στοχοποιήθηκαν άμεσα, αλλά επηρεάστηκαν λόγω της διασύνδεσής τους με συστήματα πληροφοριών στην Aix-Marseille-Provence, που ήταν ο κύριος στόχος της επίθεσης.

Τον Ιούνιο του 2020, ένα ναυπηγείο στο Λάνγκστεν της Νορβηγίας, που ανήκει στην εταιρεία Vard, έπεσε θύμα επίθεσης ransomware. Η εταιρεία δεν αποκάλυψε τις ακριβείς συνέπειες και τις τεχνικές λεπτομέρειες της επίθεσης, ο εκπρόσωπός της παραδέχτηκε ότι έκτοτε οι επιχειρήσεις ήταν υποτονικές. Εκτός από την κρυπτογράφηση, η εταιρεία παραδέχτηκε επίσης παραβίαση της βάσης δεδομένων, χωρίς να παρέχει περισσότερες λεπτομέρειες σχετικά με το ποσό ή τη σημασία των δεδομένων που έχουν κλαπεί. Τον Νοέμβριο του ίδιου έτους, το λιμάνι του Kennewick χτυπήθηκε με ransomware, το οποίο κλείδωσε εντελώς την πρόσβαση στους διακομιστές του. Το περιστατικό ήταν μια μεγάλη έκπληξη για αυτό το μικρό λιμάνι της ενδοχώρας, που βρίσκεται στον ποταμό Κολούμπια στην Πολιτεία της Ουάσιγκτον, καθώς το στρατηγικό του πεδίο είναι πολύ μικρότερο από τα μεγάλα εμπορικά λιμάνια.

Τον Ιούλιο του 2021, τέσσερα μεγάλα λιμάνια στη Νότια Αφρική (Κέιπ Τάουν, Ngqura, Port Elizabeth και Durban) παρέλυσαν μετά από μια μαζική επίθεση στην Εθνική Λιμενική Αρχή Transnet, τον κύριο διαχειριστή εμπορευμάτων της χώρας. Το επίσημο δελτίο τύπου χαρακτήρισε την επίθεση ως περίπτωση «ανωτέρας βίας» που έκανε το σύστημα υπολογιστή άχρηστο, παρόμοια με τα αποτελέσματα μιας επίθεσης ransomware. Αξίζει να σημειωθεί πως αυτή η επίθεση σημειώθηκε τη στιγμή που η Transnet και οι εθνικές αρχές ξεκινούσαν ένα φιλόδοξο, εξαιρετικά ασφαλές πρόγραμμα Smart Port, με πιλότο την πόλη του Durban.

Το λιμάνι του Χιούστον τον Αύγουστο 2021 αντιστάθηκε σε επίθεση που εκμεταλλευόταν ένα κρίσιμο ελάττωμα σε μια λύση διαχείρισης κωδικών πρόσβασης. Αναγνωρισμένο ως CVE-2021-40539, αυτό το ελάττωμα λογισμικού (με βαθμολογία CVSS 9,8 στα 10) επιτρέπει στους χάκερ να εμφυτεύουν εύκολα web shells στο σύστημα πληροφοριών ενός οργανισμού για να διευκολύνουν διάφορες ενέργειες, από την εξαγωγή κρίσιμων δεδομένων έως την εγκατάσταση κακόβουλου λογισμικού. (Nicaise, 2022)

Το πιο πρόσφατο περιστατικό συνέβη τον Φεβρουάριο του 2022 όταν μεγάλοι τερματικοί σταθμοί πετρελαίου σε ορισμένα από τα μεγαλύτερα λιμάνια της Δυτικής Ευρώπης, συμπεριλαμβανομένης της Αμβέρσας, έπεσαν θύματα κυβερνοεπίθεσης σε μια εποχή που οι τιμές της ενέργειας εκτινάσσονται στα ύψη. Η επίθεση προκάλεσε βραχυπρόθεσμες ελλείψεις καυσίμων σε αρκετά ευρωπαϊκά λιμάνια, διακόπτοντας την εκφόρτωση των φορτηγίδων σε αυτή την ήδη τεταμένη αγορά. (France24, 2022)

3.5.4 Εξέδρες πετρελαίου

Σε ένα συνέδριο για την ασφάλεια στον κυβερνοχώρο το 2013, οι ερευνητές χρησιμοποίησαν ένα μοντέλο μιας εξέδρας πετρελαίου για να δείξουν την ικανότητά τους να χακάρουν προγραμματιζόμενους ελεγκτές λογικής (PLC) και να ενεργοποιούν και να απενεργοποιούν εξ αποστάσεως τις αντλίες, κάτι που θα μπορούσε να προκαλέσει ρήξη του αγωγού εάν ενεργοποιηθεί σε ένα σύστημα υψηλής πίεσης. Σε στοχευμένες επιθέσεις, οι χάκερ μπορούν να εκμεταλλευτούν ελαττώματα ασφαλείας στα PLC συστήματα Εποπτικού Ελέγχου και Απόκτησης Δεδομένων (SCADA) της εξέδρας. Αυτά τα συστήματα είναι πανταχού παρόντα στις βιομηχανικές λειτουργίες, καθιστώντας τα βολικούς στόχους για τους χάκερ.

Σύμφωνα με ένα στέλεχος ασφαλείας της Siemens, το Stuxnet, το worm των υπολογιστών, ανακαλύφθηκε στα PLC σε τουλάχιστον δύο εξέδρες άντλησης πετρελαίου στην Αγκόλα και την Ινδονησία προτού γίνει πρωτοσέλιδο για τη διακοπή της παραγωγής στις πυρηνικές εγκαταστάσεις του Ιράν. Σύμφωνα με τους ερευνητές, τα περισσότερα PLC που βρίσκονται σε εξέδρες άντλησης πετρελαίου χρησιμοποιούν μονάδες Ethernet που λειτουργούν σε εύκολα εκμεταλλεύσιμες παλιές εκδόσεις του λειτουργικού συστήματος Linux. Μόλις αποκτηθεί η πρόσβαση, οι χάκερ μπορούν να αντικαταστήσουν τη λογική ασφάλειας του PLC, η οποία εμποδίζει την εξέδρα πετρελαίου να εκτελεί επικίνδυνες εντολές.

Μια άλλη περίπτωση είναι αυτή στην οποία εργαζόμενοι σε μια κινητή μονάδα υπεράκτιων γεωτρήσεων (MODU) στον Κόλπο του Μεξικού είχαν εισαγάγει κατά λάθος κακόβουλο λογισμικό στο σύστημα υπολογιστών της εξέδρας. Μόλις εισήλθε στο σύστημα, απενεργοποίησε τα σήματα προς τους προωθητές δυναμικής τοποθέτησης, έτσι το MODU απομακρύνθηκε από την τοποθεσία του φρεατίου και για λόγους ασφαλείας έκλεισε προσωρινά. Αποδεικνύεται ότι το σύστημα ελέγχου πλοήγησης του MODU είναι το ίδιο σύστημα που χρησιμοποιούν οι εργαζόμενοι για να συνδέσουν smartphone και άλλες συσκευές προσωπικών υπολογιστών.

Ανυποψίαστα άτομα είχαν κατεβάσει μολυσμένα αρχεία από διαδικτυακούς ιστοτόπους μουσικής και πορνογραφίας, τα οποία στη συνέχεια πέρασαν στα συστήματα υπολογιστών της εξέδρας όταν συνδέθηκαν οι συσκευές. Τα δίκτυα εξέδρων άντλησης πετρελαίου είναι τόσο περίπλοκα όσο και ελάχιστα προστατευμένα, γεγονός που τα καθιστά εύκολους στόχους για πειρατές και άλλους εγκληματίες στον κυβερνοχώρο. Σε ένα πρόσφατο περιστατικό, χάκερ προκάλεσαν την κλίση προς τη μία πλευρά μιας εξέδρας πετρελαίου στα ανοικτά των ακτών της Αφρικής, διακόπτοντας την παραγωγή για μια εβδομάδα καθώς οι μηχανικοί εργάζονταν για τον εντοπισμό και την επίλυση του προβλήματος.

Εικόνα 61 – Κλίση εξέδρας πετρελαίου. (Gonidec, 2022)

Σε μια άλλη περίπτωση, οι ειδικοί του δικτύου χρειάστηκαν 19 ημέρες για να απαλλάξουν μια εξέδρα πετρελαίου καθ' οδόν από τη Νότια Κορέα στη Βραζιλία από κακόβουλο λογισμικό που είχε θέσει εκτός σύνδεσης το σύστημά της. Κανένας από τους εργάτες δεν γνώριζε τις λεπτομέρειες του συστήματος υπολογιστή που χρησιμοποιούσαν για τη λειτουργία της, γεγονός που συνέβαλε στην καθυστερημένη απόκριση. Οποιαδήποτε δυσλειτουργία σε μια εξέδρα πετρελαίου θα μπορούσε να αποδειχθεί καταστροφική. (Kapalidis, 2022) (Swanbeck, 2022)

3.5.5 Emotet

Σύμφωνα με δημοσίευση των Πατσάκη και Χρυσάνθου το Emotet αναφέρεται ως η κορυφαία απειλή κακόβουλου λογισμικού η οποία επηρεάζει την ΕΕ. Το Emotet είναι ένα modular trojan που είναι γνωστό από το 2014, αφού μολύνει τα θύματά του, τα μολύνει και με άλλο κακόβουλο λογισμικό. Για την ακρίβεια δημιουργεί έσοδα σύμφωνα με το μοντέλο Malware-as-a-Service (MaaS) ή Access-as-a-Service (AaaS), δηλαδή οι ελεγκτές Emotet εκμισθώνουν μολυσμένες συσκευές σε κακόβουλα μέρη, προκειμένου οι τελευταίες να πραγματοποιήσουν περαιτέρω επιθέσεις στον κυβερνοχώρο.

Η πιο πρόσφατη καμπάνια για τον Emotet βασίζεται στη γνωστή μέθοδο πειρατείας μηνυμάτων ηλεκτρονικού ταχυδρομείου. Ουσιαστικά, ο αντίπαλος χρησιμοποιεί νόμιμα προηγούμενα μηνύματα ηλεκτρονικού ταχυδρομείου, που έχουν κλαπεί από παραβιασμένους πελάτες email, για να διαδοθούν στα επιδιωκόμενα θύματα. Ο αντίπαλος μεταμφιέζει τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου ως προερχόμενα από νόμιμο χρήστη και τα στέλνει σε πρόσφατους παραλήπτες ηλεκτρονικού ταχυδρομείου. Με αυτόν τον τρόπο, ο αντίπαλος αυξάνει σημαντικά τις πιθανότητες κάποιου από τα πιθανά θύματα να ανοίξει το συνημμένο έγγραφο και στη συνέχεια να μολυνθεί. Το έγγραφο του Microsoft Word παραδίδεται με τρεις τρόπους:

a) ένα έγγραφο που επισυνάπτεται απευθείας στο ηλεκτρονικό ταχυδρομείο,
b) έναν σύνδεσμο URL που περιέχεται στο σώμα του ηλεκτρονικού ταχυδρομείου και
c) εντός ένα κρυπτογραφημένο συμπιεσμένο αρχείο που επισυνάπτεται στο e-mail.

Το οπλισμένο αρχείο Microsoft Word κατεβάζει κακόβουλα εκτελέσιμα αρχεία από διάφορες διευθύνσεις URL. Αυτά τα εκτελέσιμα χρησιμοποιούνται για την επίθεση σε υπολογιστές στο ίδιο τοπικό δίκτυο, την εξαγωγή δεδομένων από τον παραβιασμένο κεντρικό υπολογιστή και τη λήψη άλλων «συνδεδεμένων» κακόβουλων προγραμμάτων, όπως το Trickbot και το Ryuk, για περαιτέρω εξάπλωση της μόλυνσης στον κεντρικό υπολογιστή. (Patsakis & Chrysanthou)

Το 2019 δημοσιεύθηκε ένα άρθρο στην «The Wall Street Journal» από τον James Rundle, το οποίο αναφέρει ένα συμβάν κυβερνοασφάλειας που οφειλόταν σε μόλυνση με κακόβουλο λογισμικό γνωστό ως Emotet. Αυτό ήταν ιδιαίτερα αποτελεσματικό στην επίθεση σε κυβερνητικά και εταιρικά δίκτυα και όπως το έχει χαρακτηρίσει το Υπουργείο Εσωτερικής Ασφάλειας «ένα από τα πιο δαπανηρά και καταστροφικά κακόβουλα προγράμματα που επηρεάζουν τις κρατικές, τοπικές, φυλετικές και εδαφικές κυβερνήσεις» και κοστίζει κατά μέσο όρο 1 εκατομμύριο δολάρια για την επιδιόρθωση ανά επίθεση.

Το πλήρωμα του συγκεκριμένου πλοίου, του οποίου το όνομα δεν ειπώθηκε, ανέφερε ότι το δίκτυο τους είχε «εξουθενωθεί πλήρως», αλλά τα βασικά συστήματα ελέγχου σκαφών δεν είχαν επηρεαστεί, και κανείς δεν μπόρεσε να επιλύσει το πρόβλημα. Ούτε οι διαχειριστές συστήματος της ναυτιλιακής εταιρείας που εργάζονται στην ξηρά κατάφεραν κάτι, και έτσι τους παραχωρήθηκε βοήθεια από ειδικούς του FBI έπειτα από επικοινωνία με την Ακτοφυλακή. Μόλις επιβιβάστηκαν, συνειδητοποίησαν ότι τα συστήματα του πλοίου είχαν πέσει θύμα ενός ιού εξόρυξης διαπιστευτηρίων, του Emotet.

Να σημειωθεί επίσης ότι το πλοίο από ό,τι διαπιστώθηκε δεν ήταν ο κύριος στόχος του επιτιθέμενου αλλά και πάλι αποτέλεσε ένα από τα θύματά του. Με την ίδια ευκολία θα μπορούσε να μεταφερθεί και σε άλλα μέρη της εφοδιαστικής αλυσίδας, όπως το λιμάνι της Νέας Υόρκης - Νιου Τζέρσεϋ, επιφέροντας καταστροφικά προβλήματα μιας που διακινεί φορτίο 1 έως 2 δισεκατομμυρίων δολαρίων την ημέρα. Για αυτόν τον λόγο έγινε η έρευνα προτού το πλοίο ελλιμενιστεί. Πιθανή εισβολή του ιού ειπώθηκε ότι είναι από την επίσκεψη του πλοίου στα λιμάνια του Πακιστάν, της Ινδίας και του Ομάν, όπου ακολουθούν μια κοινή πρακτική να μοιράζονται

memory sticks για την ανταλλαγή δεδομένων (φορτίου, διαδρομής, καυσίμων, και πληροφορίες ανθρώπινου δυναμικού). (Rundle, 2022)

Από την έρευνα που έγινε από το Λιμενικό Σώμα και το FBI διαπιστώθηκε ότι υπήρχε μια ενιαία σύνδεση στον υπολογιστή του πλοίου από κοινού σε όλο το πλήρωμα, οι εξωτερικοί σκληροί δίσκοι και οι συσκευές μνήμης ήταν συνήθως συνδεδεμένοι χωρίς μέτρα ασφαλείας και δεν υπήρχε εγκατεστημένο λογισμικό προστασίας από ιούς. Βέβαια, ισχυρίστηκαν ότι τα περισσότερα μέλη του πληρώματος δεν χρησιμοποιούσαν υπολογιστές επί του σκάφους για να ελέγχουν προσωπικά μηνύματα ηλεκτρονικού ταχυδρομείου, να κάνουν ηλεκτρονικές αγορές ή να ελέγχουν τους τραπεζικούς τους λογαριασμούς. Το δίκτυο του πλοίου χρησιμοποιήθηκε για επίσημες δραστηριότητες - για ενημέρωση ηλεκτρονικών χαρτών, διαχείριση δεδομένων φορτίου και επικοινωνία με εγκαταστάσεις στην ξηρά, πιλότους, πράκτορες και το Λιμενικό Σώμα.

Είναι άγνωστο εάν αυτό το σκάφος αντιπροσωπεύει την τρέχουσα κατάσταση της κυβερνοασφάλειας στα πλοία. Ωστόσο, με κινητήρες που ελέγχονται με κλικ του ποντικιού και με αυξανόμενη εξάρτηση από ηλεκτρονικά συστήματα χαρτογράφησης και πλοήγησης, η προστασία αυτών των συστημάτων με κατάλληλα μέτρα κυβερνοασφάλειας είναι εξίσου σημαντική με τον έλεγχο της φυσικής πρόσβασης στο πλοίο ή την τακτική συντήρηση σε παραδοσιακά μηχανήματα (Guard, 2022). Πόσο μάλλον τώρα που είναι η εποχή των έξυπνων πλοίων, με δυνατότητα επεξεργασίας διαφόρων πραγμάτων πάνω στο πλοίο όπως είναι τα φώτα, οι γερανοί, αλλά και η πρόσβαση στην μηχανή του για έλεγχο ποσότητας καυσίμων, θερμοκρασία στις δεξαμενές, στροφές κινητήρα (RPM).

Κεφάλαιο 4: Κυβερνοασφάλεια και Ναυτιλία

4.1 Ρυθμιστικό πλαίσιο στη Ναυτιλία

Η ανάγκη για ασφάλεια στον κυβερνοχώρο είναι ένα όλο και πιο επιτακτικό θέμα για τις ναυτιλιακές και υπεράκτιες βιομηχανίες. Για το λόγο αυτό απαιτεί και τη δημιουργία αντίστοιχου ρυθμιστικού και νομικού πλαισίου, που προϋποθέτει από τους ιδιοκτήτες, τους χειριστές και τους διαχειριστές να λαμβάνουν υπόψη τους κινδύνους στον κυβερνοχώρο. (DNV, 2021) Γενικότερα, τα μέρη ή και οι οργανισμοί οι οποίοι συμβάλουν στους κανονισμούς, στην νομοθεσία αλλά και σε προτάσεις - κατευθυντήριες γραμμές για την αντιμετώπιση ή μείωση του φαινομένου των κυβερνοεπιθέσεων στην ναυτιλία είναι οι παρακάτω:

Το **Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology - NIST)** ιδρύθηκε το 1901 και τώρα αποτελεί τμήμα του Υπουργείου Εμπορίου των ΗΠΑ. Αναπτύσσει πρότυπα κυβερνοασφάλειας, κατευθυντήριες γραμμές, βέλτιστες πρακτικές και άλλους πόρους για να καλύψει τις ανάγκες της βιομηχανίας των ΗΠΑ, των ομοσπονδιακών υπηρεσιών και του ευρύτερου κοινού. (NIST, 2022) Το πλαίσιο μπορεί να χρησιμοποιηθεί ως πρότυπο για δημιουργία προφίλ λειτουργιών, κατηγοριών και προτεινόμενων πρακτικών, που σχετίζονται με συγκεκριμένους οργανισμούς ή εργασίες. Οι ΗΠΑ, για παράδειγμα, με την υιοθέτηση του στο Σύστημα Θαλάσσιων Μεταφορών αντιμετωπίζουν και βοηθούν τη βιομηχανία να μετριάσει τους κινδύνους στους τομείς κοινής αποστολής της Ναυτιλιακής Μεταφοράς Υγρών Μαζικής Μεταφοράς (MBLT), των Υπεράκτιων Επιχειρήσεων και των Επιβατηγών Πλοίων. (Collaborate with Us: Government Organizations, 2022)

Το **Βαλτικό και Διεθνές Ναυτιλιακό Συμβούλιο (Baltic and International Maritime Council - BIMCO)** είναι μία από τις μεγαλύτερες διεθνείς ναυτιλιακές ενώσεις που εκπροσωπούν πλοιοκτήτες. Τα μέλη της καλύπτουν πάνω από το 60% του παγκόσμιου στόλου και αποτελούνται από τοπικές, παγκόσμιες, μικρές και μεγάλες εταιρείες. Είναι ένας οργανισμός και μια παγκόσμια ναυτιλιακή κοινότητα με περίπου 2.000 μέλη συμπεριλαμβανομένων μάνατζερ, μεσιτών και πρακτόρων σε περισσότερες από 130 χώρες. Κύριος στόχος είναι η εύρεση πρακτικών λύσεων οι οποίες θα βοηθούν στην διαχείριση του κίνδυνου σε έναν κόσμο που αλλάζει. (BIMCO, 2022) Έτσι, με τη δημιουργία κατευθυντήριων γραμμών προσπαθούν να επιτύχουν στην βελτίωση της ασφάλειας των ναυτικών, του περιβάλλοντος, του φορτίου και των πλοίων, βοηθώντας στην ανάπτυξη μιας κατάλληλης στρατηγικής διαχείρισης κινδύνων στον κυβερνοχώρο σύμφωνα με τους σχετικούς κανονισμούς και τις βέλτιστες πρακτικές επί ενός πλοίου με έμφαση στις διαδικασίες εργασίας, τον εξοπλισμό, την εκπαίδευση, την αντιμετώπιση περιστατικών και τη διαχείριση ανάκτησης. (The Guidelines On Cyber Security Onboard Ships, 2021)

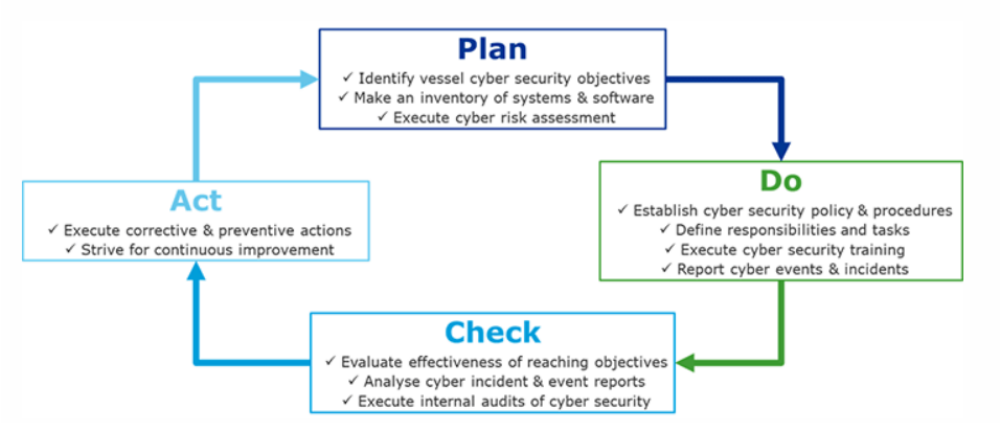
Ο **Διεθνής Οργανισμός Ναυσιπλοΐας (International Maritime Organization – IMO)**, είναι ένας πολυεθνικός, διακυβερνητικός Διεθνής Ναυτιλιακός Οργανισμός, ο οποίος επιβλέπει την σωστή και ασφαλή επικοινωνία και συνεργασία μεταξύ των χωρών-μελών του στον τομέα της ναυσιπλοΐας. Τα κατευθυντήρια έγγραφα που παρέχονται από τον IMO για την ασφάλεια στον κυβερνοχώρο είναι ένα σύνολο συστάσεων υψηλού επιπέδου για την προστασία της ναυτιλίας από τρέχουσες και αναδυόμενες κυβερνοαπειλές και ευπάθειες. Αυτά τα έγγραφα καθοδήγησης περιγράφουν ευάλωτα συστήματα πλοίων, συμπεριλαμβανομένων συστημάτων γεφυρών και συστημάτων επικοινωνίας και περιγράφουν τα βήματα διαχείρισης κινδύνου που πρέπει να χρησιμοποιούνται κατά τη δημιουργία κυβερνοάμυνας. (IMO, 2021)

Επίσης, στις 5 Ιουλίου 2017, εξέδωσε κατευθυντήριες γραμμές για τη διαχείριση θαλάσσιων κινδύνων στον κυβερνοχώρο[42]. Αυτές παρέχουν συστάσεις υψηλού επιπέδου για τη διαχείριση τρεχουσών και αναδυόμενων απειλών, τρωτών σημείων και κινδύνων στον κυβερνοχώρο και περιλαμβάνουν λειτουργικά στοιχεία για την αποτελεσματική διαχείριση τους. Βάσει του Διεθνούς Κώδικα Διαχείρισης Ασφάλειας (International Safety Management – ISM) και του Διεθνούς Κώδικα Ασφάλειας Πλοίων και Λιμενικών Εγκαταστάσεων (International Ship and Port Facility

42 (International Maritime Organization - MSC-FAL.1/Circ.3 "Guidelines On Maritime Cyber Risk Management", 2021)

Security – ISPS), ο IMO συμφώνησε ότι οι συστάσεις για την διαχείριση κινδύνων στον κυβερνοχώρο πρέπει να ενσωματωθούν στις υπάρχουσες διαδικασίες διαχείρισης και να συμπληρώνουν τις πρακτικές διαχείρισης ασφάλειας που έχουν ήδη θεσπιστεί.

Κατά συνέπεια, πρέπει να εφαρμοστεί η διαδικασία PDCA (Plan, Do, Check, Act). Πρώτο βήμα είναι να προσδιοριστούν οι στόχοι ασφάλειας λαμβάνοντας υπόψιν τις απαιτήσεις τόσο του IMO όσο και των άλλων εμπλεκόμενων. Βάσει αυτών των στόχων να καθοριστεί ένα σχέδιο εφαρμογής για την εξάλειψη κατάλληλων εμποδίων. Επόμενο βήμα είναι να ελέγχεται σε συνεχή βάση η αποτελεσματικότητα των μέτρων ασφάλειας στον κυβερνοχώρο. Τέλος, καλό είναι να εφαρμοστούν διορθωτικές και προληπτικές ενέργειες με βάση τα πορίσματα των εκθέσεων εσωτερικής και εξωτερικής αναθεώρησης. (DNV, 2021)



Εικόνα 62- Διαδικασία PDCA (DNV, 2021)

Επιπλέον οδηγίες και πρότυπα που εισάγονται από τον IMO είναι:

a) οι κατευθυντήριες γραμμές για την ασφάλεια στον κυβερνοχώρο πάνω στα πλοία που εκδίδονται από BIMCO, ICS, INTERCARGO, INTERTANKO κλπ., που αναλύουν απειλές, ευπάθειες, αξιολόγηση πιθανότητας, εκτίμηση επιπτώσεων καθώς και ανάπτυξη μέτρων προστασίας και ανίχνευσης[43],
b) το πρότυπο ISO / IEC 27001:2018[44] σχετικά με την Τεχνολογία Πληροφοριών, τις Τεχνικές Ασφαλείας, τα Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών κα το οποίο δημοσιεύθηκε από κοινού από τον Διεθνή Οργανισμό Τυποποίησης (ISO) και τη Διεθνή Ηλεκτροτεχνική Επιτροπή (IEC) και
c) το Πλαίσιο για τη Βελτίωση των Κρίσιμων Υποδομών Ασφάλειας στον Κυβερνοχώρο του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας των Ηνωμένων Πολιτειών (NIST Framework), το οποίο αναφέρει αναλυτικότερα τα λειτουργικά στοιχεία για την αποτελεσματική διαχείριση της κυβερνοαπειλής, που χρησιμοποιούνται για την κατανόηση, τον εντοπισμό και την ιεράρχηση δράσεων για τη μείωση του κινδύνου ασφάλειας[45]. Η κύρια δομή του πλαισίου φαίνεται στην παρακάτω εικόνα. (IMO, 2021)

43 (The Guidelines On Cyber Security Onboard Ships, 2021)

44 (ISO/IEC 27001 - Information Security Management, 2021)

45 (NIST Framework for Improving Critical Infrastructure Cybersecurity, 2021)

Εικόνα 63 - Κύρια Δομή Πλαισίου (NIST Framework for Improving Critical Infrastructure Cybersecurity, 2021)

Ο **Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (European Union Agency for Cybersecurity – ENISA)** το 2011 δημοσίευσε την πρώτη έκθεση της ΕΕ για τις προκλήσεις της κυβερνοασφάλειας στον Ναυτιλιακό Τομέα. Αυτή η κύρια ανάλυση υπογραμμίζει βασικές γνώσεις, καθώς και υπάρχουσες πρωτοβουλίες, ως βάση για την ασφάλεια στον κυβερνοχώρο. Τέλος, δίνονται συστάσεις υψηλού επιπέδου για την αντιμετώπιση αυτών των κινδύνων. (First EU-report on Maritime Cyber Security, 2022) Είναι επίσης μία από τις ελάχιστες υπηρεσίες που εκπονούν συστάσεις για την κυβερνοασφάλεια στους λιμένες. Το 2020, δημοσίευσε κατευθυντήριες γραμμές για την παροχή στους φορείς εκμετάλλευσης λιμένων ενός συνόλου καλών πρακτικών για την βοήθεια εντοπισμού και αξιολόγησης κινδύνων στον κυβερνοχώρο και προσδιορισμού κατάλληλων μέτρων ασφαλείας. Οι νέες κατευθυντήριες γραμμές του ENISA - Διαχείριση Κινδύνου Κυβερνοχώρου για Λιμάνια συντάχθηκαν σε συνεργασία με πολλά λιμάνια σε κράτη μέλη της ΕΕ. (Cybersecurity in the Maritime Sector: ENISA Releases New Guidelines for Navigating Cyber Risk, 2022)

Όπως έχει αναφερθεί και στο κεφάλαιο 1.4, η **οδηγία για την ασφάλεια συστημάτων δικτύου και πληροφοριών (Network and Information Security - NIS Directive[46])** είναι η πρώτη προσπάθεια της ΕΕ να νομοθετήσει την ασφάλεια στον κυβερνοχώρο και ισχύει για όλες τις χώρες της Ευρωπαϊκής Ένωσης. Στο πεδίο εφαρμογής αυτής της νομοθεσίας υπάγονται οργανισμοί ζωτικών τομέων που βασίζονται σε μεγάλο βαθμό σε δίκτυα πληροφοριών και αναφέρονται ως Χειριστές Βασικών Υπηρεσιών (Operators of Essential Services - OES). Μέσα σε αυτές είναι και η ναυτιλία όπως και οι μεταφορές, τομείς ενέργειας κ.λπ. Ως OES του ναυτιλιακού τομέα ορίζονται οι ναυτιλιακές εταιρείες, οι λιμενικές αρχές, οι λιμενικές εγκαταστάσεις και οι υπηρεσίες κυκλοφορίας πλοίων. Για να συμμορφωθεί κάθε OES από την οδηγία NIS καλό θα ήταν πρώτα να έχει δημιουργηθεί ένας μηχανισμός αναφοράς περιστατικών καθώς και να έχει ολοκληρωθεί μια αυτοαξιολόγηση. Συνεπώς, θα πρέπει να ληφθούν υπόψη τα εξής βήματα:

1. Έμφαση στις καθοδηγήσεις του διοικητικού συμβουλίου και των ανώτερων ενδιαφερόμενων μερών, καθώς και της εθνικής ρυθμιστικής αρχής κάθε οργανισμού.
2. Καθιέρωση διαδικασίας ειδοποίησης σε ολόκληρο τον οργανισμό για τυχόν περιστατικά.
3. Κατανόηση επιπέδου συμμόρφωσης μέσω επικοινωνίας των ενδιαφερόμενων φορέων και εξειδικευμένων τεχνικών.
4. Κατανόηση του κινδύνου των υφιστάμενων κενών (ανάλογα με το σύστημα) μέσω δημιουργίας ενός προγράμματος διαχείρισής του.
5. Υποστήριξη από ειδικούς τόσο στην ασφάλεια στον κυβερνοχώρο όσο και στην εφαρμογή της Οδηγίας. (Kalfigkopoulos, 2022)

[46] Βλέπε Οδηγία (ΕΕ) 2016/1148 http://data.europa.eu/eli/dir/2016/1148/oj

Οι κανονισμοί της ΕΕ όπως ο κανονισμός GDPR και η οδηγία NIS έχουν σημαντικό αντίκτυπο στη ναυτιλιακή βιομηχανία. Ο πρώτος επειδή η ναυτιλιακή βιομηχανία χρησιμοποιεί Προσωπικά Δεδομένα και Πληροφορίες Απορρήτου επιβατών, πληρώματος και επισκεπτών. Η δεύτερη επειδή οι θαλάσσιες μεταφορές είναι ένας τομέας που εμπίπτει στις διατάξεις της οδηγίας NIS και, ως εκ τούτου, ορισμένες ναυτιλιακές εταιρείες ενδέχεται να έχουν αναγνωριστεί ως Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών (OES). Παράλληλα, ορισμένα κράτη μέσω των Κρατικών Αρχών Ελέγχου Λιμένων (Port State Control) έχουν ήδη αρχίσει να διενεργούν εντατικούς ελέγχους και να επιβάλλουν αυστηρά μέτρα προκειμένου να διασφαλιστεί ότι η διαχείριση κινδύνων στον κυβερνοχώρο αντιμετωπίζεται και εφαρμόζεται σωστά. (Σπανός, 2022)

Το **Ίδρυμα Μηχανικής και Τεχνολογίας (Institution of Engineering and Technology – IET)** ιδρύθηκε το 2006 από δύο ξεχωριστά ιδρύματα, το Ίδρυμα Ηλεκτρολόγων Μηχανικών και το Ινστιτούτο Ενσωματωμένων Μηχανικών. Δημοσίευσε έναν Κώδικα Πρακτικής ο οποίος εξετάζει την απαίτηση για την ασφάλεια στον κυβερνοχώρο για πλοία που βρίσκονται σε εξέλιξη, ελλιμενισμένα ή αγκυροβολημένα, υποστηρίζοντας μια συνεκτική προσέγγιση σε επίπεδο πλοίου – ή στόλου. Προορίζεται να συμπληρώσει τα πρότυπα ασφάλειας πλοίων και τις αντίστοιχες απαιτήσεις τους, παρέχοντας πρόσθετη καθοδήγηση σχετικά με τα μέτρα ασφαλείας που ορίζονται για τον κυβερνοχώρο. Τα μέτρα που εφαρμόζονται θα πρέπει να εξαρτώνται από το προφίλ του πλοίου, τη χρήση του και τη φύση των φορτίων που διακινούνται. Ενώ αυτός ο Κώδικας Πρακτικής αφορά αποκλειστικά την ασφάλεια στον κυβερνοχώρο των πλοίων, αναγνωρίζει ότι, με ένα μεγάλο ποσοστό παραβιάσεων ασφάλειας που προκαλούνται από άτομα και κακές διαδικασίες, είναι σημαντικό το προσωπικό, οι διαδικασίες και οι φυσικές πτυχές να σχετίζονται άμεσα με τα τεχνολογικά θαλάσσια συστήματα. (Boyes & Isbell, 2022)

Η **Διεθνής Ένωση Λιμένων (International Association of Ports and Harbors – IAPH)** ιδρύθηκε το 1955 και είναι μια μη κερδοσκοπική παγκόσμια συμμαχία 170 λιμένων και 140 οργανισμών που σχετίζονται με λιμάνια που καλύπτουν 90 χώρες. Τα λιμάνια μέλη της διαχειρίζονται περισσότερο από το 60 τοις εκατό του παγκόσμιου θαλάσσιου εμπορίου και περίπου το 80 τοις εκατό της παγκόσμιας κυκλοφορίας εμπορευματοκιβωτίων. Ανακοίνωσαν την έναρξη των Οδηγιών για την Κυβερνοασφάλεια για Λιμένες και Λιμενικές εγκαταστάσεις, ένα έγγραφο 84 σελίδων όπου αποτελεί το αποκορύφωμα τεσσάρων μηνών εντατικής εργασίας μεταξύ 22 εμπειρογνωμόνων από λιμάνια-μέλη της IAPH από όλο τον κόσμο καθώς και συνεργαζόμενων μελών ειδικών στον τομέα της κυβερνοασφάλειας και συντελεστών από την Παγκόσμια Τράπεζα. Το έγγραφο στοχεύει να βοηθήσει τα λιμάνια και τις λιμενικές εγκαταστάσεις να καθορίσουν το πραγματικό οικονομικό, εμπορικό και λειτουργικό αντίκτυπο μιας κυβερνοεπίθεσης, να κάνουν μια αντικειμενική αξιολόγηση της ετοιμότητάς τους να αποτρέψουν, να σταματήσουν ή και να ανακάμψουν από μια κυβερνοεπίθεση. (IAPH launches Cybersecurity Guidelines for Ports and Port Facilities as part of industry call to action to digitalize the maritime transport chain, 2022)

Από το 1790, η **Ακτοφυλακή των Ηνωμένων Πολιτειών (US Coast Guard – USCG)** προστατεύει τον αμερικανικό λαό και προωθεί την εθνική ασφάλεια, την ασφάλεια των συνόρων και την οικονομική ευημερία σε ένα περίπλοκο και εξελισσόμενο θαλάσσιο περιβάλλον. Το 2021 δημιουργήθηκε η πρώτη Ομάδα Κυβερνοπροστασίας της Αμερικανικής Ακτοφυλακής (CGCYBER) που είναι αναπτυσσόμενες ειδικές δυνάμεις που αξιολογούν απειλές και τρωτά σημεία, εντοπίζουν την παρουσία αντιπάλων σε δίκτυα και συστήματα και ανταποκρίνονται σε περιστατικά στον κυβερνοχώρο. (CGCYBER, 2022) Επίσης, υπάρχει και το Maritime Cyber Readiness Branch (MCRB) το οποίο είναι ένα στοιχείο του CG Cyber, και υποστηρίζει την αποστολή κυβερνοασφάλειας στην κοινότητα εμπορικών θαλάσσιων μεταφορών. Χρησιμοποιεί μια προσέγγιση βάσει κινδύνου για την αξιολόγηση των απειλών, των τρωτών σημείων και των επιπτώσεων της απώλειας στο Σύστημα Θαλάσσιων Μεταφορών (MTS) για να συντονίσει τον προσδιορισμό των πιο κρίσιμων δεδομένων και συστημάτων. Με έδρα την Αλεξάνδρεια της Βιρτζίνια, η Cyber Protection Team (CPT) είναι η αναπτυσσόμενη μονάδα της Ακτοφυλακής που παρέχει τέσσερις βασικές υπηρεσίες: Assess, Hunt, Clear και Harden. Η αποστολή της CPT είναι να ενισχύσει την ανθεκτικότητα της Υποδομής Ζωτικής Σημασίας του MTS έναντι της διαταραχής στον κυβερνοχώρο μέσω συνεπών ενεργών δεσμεύσεων με δημόσιους και ιδιωτικούς οργανισμούς της βιομηχανίας (Maritime Cyber Readiness Branch, 2022)

Η **Υπηρεσία Κυβερνοασφάλειας και Ασφάλειας Υποδομών (Cybersecurity and Infrastructure Security Agency – CISA)** ηγείται της εθνικής προσπάθειας για την κατανόηση, τη διαχείριση και τη μείωση του κινδύνου για τον κυβερνοχώρο και τη φυσική υποδομή. Συνδέει τους μετόχους στη βιομηχανία και την κυβέρνηση και με πόρους, αναλύσεις και εργαλεία τους βοηθάει να δημιουργήσουν τη δική τους ασφάλεια στον κυβερνοχώρο, στις επικοινωνίες και στη φυσική τους ασφάλεια και ανθεκτικότητα. (CISA, 2022) Επίσης, επιβλέπει και το Συντονιστικό Συμβούλιο Ναυτιλιακού Τομέα (Maritime SCC) που σκοπός του είναι να διευκολύνει την ετοιμότητα έκτακτης ανάγκης και τον συντονισμό αντίδρασης μεταξύ του εγχώριου ναυτιλιακού τομέα και της κυβέρνησης. (Maritime Modal Sector Coordinating Council Charter , 2022)

Αφοσιωμένη σε ασφαλή πλοία και καθαρές θάλασσες, η **Διεθνής Ένωση Νηογνωμόνων (International Association of Classification Societies – IACS)** είναι ένας μη κερδοσκοπικός οργανισμός που συνεισφέρει μοναδικά στην ασφάλεια και τη ρύθμιση της θάλασσας μέσω τεχνικής υποστήριξης, επαλήθευσης συμμόρφωσης, έρευνας και ανάπτυξης. Περισσότερο από το 90% της παγκόσμιας χωρητικότητας μεταφοράς φορτίου καλύπτεται από τους κανόνες και τα πρότυπα συμμόρφωσης με τον σχεδιασμό, την κατασκευή και τη διάρκεια ζωής της ταξινόμησης που ορίζονται από τις έντεκα Εταιρείες Μέλη του IACS, ορισμένων εκ των οποίων οι ABS, BV, China classification society, Lloyd's Register, ClassNK, DNV και Russian Maritime Register of Shipping. Παρέχει ένα Σύστημα Πιστοποίησης Συστήματος Ποιότητας (QSCS) με το οποίο συμμορφώνονται τα Μέλη του, ως εγγύηση επαγγελματικής ακεραιότητας και διατήρησης υψηλών επαγγελματικών προτύπων. Το IACS αναγνωρίζεται ως ο κύριος τεχνικός σύμβουλος του IMO.

Το IACS έχει δημοσιεύσει συστάσεις για την ασφάλεια στον κυβερνοχώρο, με στόχο να καταστεί δυνατή η παράδοση πλοίων ανθεκτικών καθ' όλη τη διάρκεια της εργασιακής τους ζωής. Οι συστάσεις αυτές, συλλογικά, όχι μόνο παρέχουν καθοδήγηση στους πιο πιεστικούς τομείς ανησυχίας, αλλά λειτουργούν ως δομικά στοιχεία για τον ευρύτερο στόχο της ανθεκτικότητας του συστήματος. Το IACS αναγνωρίζει ότι η παράδοση αυτής της σημαντικής σειράς Συστάσεων είναι μόνο η αρχή στον συνεχιζόμενο αγώνα για τη διατήρηση της ακεραιότητας των πλοίων στον κυβερνοχώρο. (12 Iacs Recommendations On Cyber Safety Mark Step Change In Delivery Of Cyber Resilient Ships, 2022) Επιπλέον, υιοθέτησε δύο νέες Ενοποιημένες Απαιτήσεις (UR E26 και UR E27) σε μια προσπάθεια να παράσχει στο πλήρωμα και στα πλοία τις δυνατότητες για την αποτελεσματική αντιμετώπιση των περιστατικών στον κυβερνοχώρο που συμβαίνουν σε συστήματα που βασίζονται σε υπολογιστές επί του σκάφους. Αυτές θα εφαρμοστούν σε νέα πλοία που έχουν συναφθεί για ναυπήγηση την 1η Ιανουαρίου 2024 και μετά. (IACS adopts two new Unified Requirements on cyber resilience of Ships, 2022)

Ένα από τα μέλη του IACS, ο οργανισμός τεχνικών και επιχειρηματικών υπηρεσιών και ναυτικός νηογνώμονας **Lloyd's Register**, τον Φεβρουάριο του 2016 κοινοποίησε την προσέγγισή του για τα «Πλοία με δυνατότητα Κυβερνοχώρου - Ανάπτυξη τεχνολογίας πληροφοριών και επικοινωνιών στη ναυτιλία», στην οποία αναφέρει ποια συστήματα του πλοίου βασίζονται στον κυβερνοχώρο (βλέπε κεφάλαιο 2) και περιγράφει τους έξι βασικούς τομείς κινδύνου που πρέπει να εξεταστούν και να αντιμετωπιστούν προκειμένου να διασφαλιστεί η ασφάλεια και η αξιοπιστία των πλοίων. Οι βασικοί τομείς που πρέπει να ληφθούν υπόψη είναι:

I. Σύστημα
II. Άνθρωπος – Σύστημα
III. Λογισμικό
IV. Δίκτυα και Επικοινωνίες
V. Διασφάλιση Δεδομένων
VI. Ασφάλεια (Lloyd's Register, 2021)

Τα παραπάνω δημιούργησαν την ανάγκη ύπαρξης ενός νομοθετικού πλαισίου το οποίο θα είναι ικανό να ανταπεξέλθει στις περισσότερες αν όχι σε όλες τις προσκλήσεις που μπορεί να επέρθουν στην ναυτιλιακή βιομηχανία. Τον Ιούνιο του 2017, κατά την 98η σύνοδο της Επιτροπής Ασφάλειας της Ναυσιπλοΐας εγκρίθηκε το ψήφισμα για την Διαχείριση κινδύνων στον κυβερνοχώρο στα συστήματα διαχείρισης ασφάλειας[47], το οποίο απαιτεί από τους ιδιοκτήτες

47 (Resolution Msc.428(98) - Maritime Cyber Risk Management In Safety Management Systems, 2021)

πλοίων και τους διαχειριστές να αξιολογούν τον κίνδυνο στον κυβερνοχώρο και να εφαρμόζουν σχετικά μέτρα σε όλες τις λειτουργίες του συστήματος διαχείρισης της ασφάλειας (όπως ορίζονται στον κώδικα ISM).

Το **Αμερικανικό Γραφείο Ναυτιλίας (American Bureau of Shipping – ABS)** ιδρύθηκε το 1862 και είναι παγκόσμιος ηγέτης στην παροχή υπηρεσιών ταξινόμησης για θαλάσσια και υπεράκτια περιουσιακά στοιχεία. Αποστολή του είναι η εξυπηρέτηση του δημόσιου συμφέροντος καθώς και των αναγκών των μελών και των πελατών προάγοντας την ασφάλεια της ζωής και της περιουσίας και τη διατήρηση του φυσικού περιβάλλοντος. Το ABS παρέχει πρακτικές οδηγίες για τον μετριασμό και την προστασία από τους κινδύνους κυβερνοασφάλειας για τα θαλάσσια και υπεράκτια περιουσιακά στοιχεία. Το πρόγραμμα CyberSafety προσφέρει υποστήριξη σε κάθε στάδιο του κύκλου ζωής ενός περιουσιακού στοιχείου, έτσι ώστε οι ιδιοκτήτες να μπορούν να κατανοήσουν και να αντιμετωπίσουν τους κινδύνους του κυβερνοχώρου. Παρέχει σε ιδιοκτήτες περιουσιακών στοιχείων, χειριστές, ναυπηγεία, προμηθευτές συστημάτων εξοπλισμού και ολοκληρωτές (integrators) μια σαφή και απλή μέθοδο για την κατανόηση, τη μέτρηση και τον μετριασμό των κινδύνων. Βοηθά τους κατασκευαστές εξοπλισμού να εντοπίσουν και να διορθώσουν τα τρωτά σημεία της κυβερνοασφάλειας στις διαδικασίες διαχείρισης κινδύνου, τη διακυβέρνηση και το ίδιο το τελικό σύστημα. (ABS, 2022)

Ένα άλλο μέλος, ο **Νορβηγικός Νηογνώμονας (Det Norske Veritas - DNV GL)** είναι μια ναυτιλιακή εταιρεία που παρέχει σε διάφορους τομείς μια υπηρεσία τεχνογνωσίας συμβούλων, με στόχο την προστασία της ανθρώπινης ζωής, του περιβάλλοντος και της ιδιοκτησίας. Τον Ιούνιο του 2018, δημοσιεύτηκε μια εργασία για την ασφάλεια στον κυβερνοχώρο, «Μια προτεινόμενη προσέγγιση που εφαρμόζεται στη σύγχρονη κατασκευή κρουαζιερόπλοιων». Αυτό το δωδεκασέλιδο έγγραφο προορίζεται ρητά για σύγχρονα και έξυπνα κρουαζιερόπλοια, τα οποία απαιτούν τεχνολογία για την αποτελεσματικότητα των σκαφών και την εμπειρία των επιβατών. Αυτό το έγγραφο συνεπάγεται τη συμμετοχή του χειριστή κρουαζιέρας, των ναυπηγείων και των θαλάσσιων συστημάτων στον κυβερνοχώρο ως ενδιαφερόμενων μερών που εμπλέκονται στη διαδικασία παράδοσης αυτών των τύπων σκαφών. (Paper: Cyber security by design, 2022)

Επιπλέον, να μην ξεχνάμε και τον **Γαλλικό Νηογνώμονα (Bureau Veritas -BV)** που ιδρύθηκε το 1828 και δραστηριοποιείται σε διάφορους τομείς, ένας από αυτούς η ναυτιλία, και ειδικεύεται στις δοκιμές, τις επιθεωρήσεις και την πιστοποίηση. Οι κανόνες και οι σημειώσεις του BV αναπτύχθηκαν σε συνεργασία με τους θαλάσσιους φορείς και παρέχουν ένα ολοκληρωμένο πλαίσιο για την ασφάλεια στον κυβερνοχώρο. Η ολιστική προσέγγιση καλύπτει οργανωτικά και τεχνικά μέτρα, επιτρέποντας στους πλοιοκτήτες να προστατεύουν τα περιουσιακά τους στοιχεία, να καθορίζουν τις προσδοκίες για τα ναυπηγεία και τους κατασκευαστές και να συμμορφώνονται με τις απαιτήσεις του IMO και του IACS. Για να βοηθήσει τους πλοιοκτήτες να προστατεύσουν τα περιουσιακά στοιχεία και τα δεδομένα τους, η Bureau Veritas έχει αναπτύξει δύο ολοκληρωμένες ενδείξεις ασφάλειας, το CYBER MANAGED και το CYBER SECURE. Οι κανόνες τους, το NR 659[48], και οι σχετικές οδηγίες βοηθούν περαιτέρω τους πελάτες να περιορίσουν τον κίνδυνο, να ασφαλίσουν τα δεδομένα πλοίων και να εκπαιδεύσουν το προσωπικό. Συμμορφώνονται, επίσης, με τον IMO.

Χρησιμοποιείται μια μεθοδολογία βασισμένη στον κίνδυνο και ένα τυποποιημένο πλαίσιο για την ανάλυση του χερσαίου και υπεράκτιου κινδύνου, την αξιολόγηση της κρισιμότητας του και τον καθορισμό των κατάλληλων μέτρων. Οι πλοιοκτήτες και οι εργολάβοι καλούνται να αναπτύξουν έναν πλήρη χάρτη συστημάτων πληροφορικής και OT (Cyber Repository), αρχές διαχείρισης υψηλού επιπέδου (Cyber Policy) και λεπτομερείς διαδικασίες επί του σκάφους (Cyber Handbook). (Cyber Safety And Security, 2022) (Maritime Industry 4.0, 2022). Οι κανόνες της BV ισχύουν για το σχεδιασμό, την κατασκευή, τη θέση σε λειτουργία και τη συντήρηση συστημάτων που βασίζονται σε υπολογιστές (CBS) βάσει λογισμικού για τη σωστή επίτευξη των λειτουργιών τους. Οι απαιτήσεις επικεντρώνονται στη λειτουργικότητα του λογισμικού και στο υλικό που υποστηρίζει. (Rules on Cyber Security for the Classification of Marine Units, 2022)

[48] (Rules on Cyber Security for the Classification of Marine Units, 2022)

Το **Διεθνές Εμπορικό Επιμελητήριο (International Chamber Of Commerce - ICC)** είναι ένας παγκόσμιος επιχειρηματικός οργανισμός, ένα αντιπροσωπευτικό όργανο για λογαριασμό επιχειρήσεων από όλους τους τομείς. Η αποστολή του είναι να προωθήσει το ανοιχτό διεθνές εμπόριο και τις επενδύσεις και να βοηθήσει τις επιχειρήσεις να αντιμετωπίσουν τις προκλήσεις και τις ευκαιρίες της παγκοσμιοποίησης. Οι δράσεις του σχετίζονται με την θέσπιση κανόνων, επίλυση διαφορών και υπεράσπιση πολιτικής. Όσον αφορά την ναυτιλία έχει δημιουργήσει ένα εξειδικευμένο τμήμα το **Διεθνές Ναυτιλιακό Γραφείο (International Maritime Bureau - IMB)**, έναν μη κερδοσκοπικό οργανισμό, ο οποίος ιδρύθηκε το 1981 για να λειτουργεί ως κομβικό σημείο στην καταπολέμηση όλων των τύπων θαλάσσιου εγκλήματος και κακής πρακτικής. Ο IMO προέτρεψε τις κυβερνήσεις και τους οργανισμούς να συνεργαστούν και να ανταλλάξουν πληροφορίες μεταξύ τους με σκοπό τη διατήρηση και την ανάπτυξη συντονισμένης δράσης για την καταπολέμηση της θαλάσσιας απάτης. (International Maritime Bureau, 2022)

Το 2015, το ICC ανέπτυξε τον οδηγό Cyber Security για επιχειρήσεις, ως έναν ρεαλιστικό οδηγό συνομιλίας για την ασφάλεια στον κυβερνοχώρο μεταξύ των ειδικών της τεχνολογίας πληροφοριών και της διοίκησης της εταιρείας. Αυτό χρησιμεύει ως ζωντανή βάση δεδομένων και παρέχει συμβουλές, βήματα και διαδικασίες που θα μπορούσαν να ενθαρρύνουν κάθε μέλος να αντιμετωπίσει πιθανή κυβερνοεπίθεση. (Cybersecurity, 2022) Αναπτύχθηκε και ένα ερωτηματολόγιο αυτοαξιολόγησης ως εργαλείο για να βοηθήσει τη διοίκηση κάθε εταιρείας να εκτιμήσει τα δυνατά και τα αδύναμα σημεία της όσον αφορά τις ικανότητές της στον κυβερνοχώρο. (ICC Cyber Security , 2022)

Σαφώς υπάρχει και η συνεργασία μεταξύ των παραπάνω μερών όπως για παράδειγμα, η Ακτοφυλακή των ΗΠΑ παρακολουθεί την καθοδήγηση και τα προϊόντα από την CISA. Πιο συγκεκριμένα, το «Shields Up» που είναι η κύρια πηγή για πληροφορίες και συστάσεις για την προσαρμογή μιας αυξημένης στάσης ασφάλειας στον κυβερνοχώρο, μετά από την παρατήρηση αυξημένων κακόβουλων παραγόντων που χρησιμοποιούν ψευδείς επιχειρηματικούς ιστοτόπους για να στοχεύσουν το Σύστημα Θαλάσσιων Μεταφορών (MTS). Πολλοί συνεργάτες του MTS έχουν ανακαλύψει καλοσχεδιασμένους, ψεύτικους ιστοτόπους που μεταμφιέζονται ως νόμιμοι. Αυτοί οι ιστότοποι δημιουργούνται πιθανώς για την κλοπή πληροφοριών ή την εγκατάσταση κακόβουλου λογισμικού σε συσκευές πελατών. (USA issues a Cybersecurity Alert, 2022)

Επίσης, η **Δημοκρατία Νήσων Marshall** συγκέντρωσε όλους τους πόρους σχετικά με την διαχείριση των κινδύνων στον κυβερνοχώρο. Για τους κανονισμούς που δημιουργήθηκαν από τον Διεθνή οργανισμό Ναυτιλίας, για τα πρότυπα και πλαίσια για το κυβερνορίσκο καθώς επίσης και για προτάσεις από νηογνώμονες, κυβερνητικές και ασφαλιστικές υπηρεσίες. Στο τέλος, προτρέπει να σταλούν και άλλες πηγές στην διαχείριση προκειμένου να συμπληρωθεί ένα ολοκληρωμένο αρχείο (Republic Of The Marshall Islands - Maritime Cyber Risk Management Resources, 2021)[49].

Τέλος, στην 1 Ιανουαρίου 2018, τέθηκε σε ισχύ η τρίτη έκδοση της Tanker Management and Self-Assessment (TMSA) που παρέχει στις εταιρείες ένα μέσο για τη βελτίωση και τη μέτρηση των δικών τους συστημάτων διαχείρισης ασφάλειας. Μία από τις εμφανείς αλλαγές στην έκδοση TMSA 3 είναι η προσθήκη του 13ου στοιχείου επιδόσεων που εστιάζει στη θαλάσσια ασφάλεια. Αυτό το νέο στοιχείο θα απαιτήσει από τα μέλη που είναι εγγεγραμμένα στο πρόγραμμα Ship Inspection Reporting Program (SIRE), να ενσωματώσουν πολιτικές και διαδικασίες ασφάλειας κινδύνου στον κυβερνοχώρο στις διαδικασίες λειτουργίας της εταιρείας / του πλοίου. Για να είμαστε πιο συγκεκριμένοι, οι χειριστές θα πρέπει να έχουν:

- ✓ διαδικασίες διαχείρισης λογισμικού
- ✓ οδηγίες για τον εντοπισμό και τον μετριασμό των απειλών στον κυβερνοχώρο
- ✓ διαθεσιμότητα των πιο πρόσφατων οδηγιών για την ασφάλεια στον κυβερνοχώρο από τη βιομηχανία και την κοινωνία ταξινόμησης
- ✓ διαδικασίες διαχείρισης κωδικού πρόσβασης

49 Το αναφερόμενο αρχείο βρίσκεται στο https://www.register-iri.com/wp-content/uploads/SS-200-Maritime-Cyber-Risk-Management-Resources.pdf

- ✓ και ένα σχέδιο ασφάλειας στον κυβερνοχώρο που μπορεί να μοιραστεί με το προσωπικό για την προώθηση της κυβερνο-επίγνωσης επί του σκάφους. (ShipOwners, 2021)

4.2 Λύσεις στον ναυτιλιακό τομέα

Στα προηγούμενα κεφάλαια έγινε μια προσπάθεια ολιστικής προσέγγισης των συστημάτων που βρίσκονται πάνω στα πλοία και των ευπαθειών τους καθώς και των πιθανών κινδύνων. Σε αυτό το σημείο θα παρουσιαστούν ενδεικτικές προτάσεις για την πρόβλεψη και αντιμετώπιση του κυβερνο-εγκλήματος στη ναυτιλία. Κάποιες από τις οποίες μπορεί να τις δοκιμάσει και ένας μέσος χρήστης. Οι λύσεις που προτείνονται εναρμονίζονται με τις κατευθυντήριες γραμμές που έχουν ορίσει τα αρμόδια μέλη και οι οργανισμοί που αναφέρθηκαν στην προηγούμενη ενότητα και με τις προϋποθέσεις που έχουν ορίσει οι νηογνώμονες.

Είναι αλήθεια ότι τα μέτρα ασφαλείας δεν υπόσχονται την μη προσπέλαση των συστημάτων. Ως επί το πλείστον, ένας κακόβουλος χρήστης από την στιγμή που θέλει να εισβάλει στο εκάστοτε σύστημα, θα βρει τον τρόπο και θα τα καταφέρει. Αυτό όμως δεν πρέπει να λειτουργήσει ως αποτρεπτικός παράγοντας για την προστασία του. Αντίθετα, από την στιγμή που η απόλυτη προφύλαξη δεν είναι πάντοτε και απολύτως δυνατή, τουλάχιστον να είναι όσο το δυνατόν πιο ασφαλισμένο, ώστε να δυσχεράνει την πρόσβαση με σκοπό ο εισβολέας να εγκαταλείψει την προσπάθεια ή να μετριαστεί τουλάχιστον το αντίκτυπο της επίθεσης.

Πολλές φορές ανάλογα με το μέγεθος της κυβερνοεπίθεσης, η αντιμετώπιση της οποίας μπορεί να κρατήσει από ώρες μέχρι και εβδομάδες, μεγάλο μέρος των εταιρειών, επειδή δεν μπορούν να ανταπεξέλθουν, υπόκεινται στην βοήθεια τρίτων ειδικών επί του θέματος. Πρόκειται για εταιρίες (π.χ Riviera) ή ηθικούς χάκερς (π.χ. Munro) που προγραμματίζουν ελέγχους διείσδυσης, εντοπίζοντας τις τρωτότητες του συστήματος και προτείνοντας πιθανούς τρόπους αντιμετώπισης αλλά και μέλη του ρυθμιστικού πλαισίου (π.χ. η Ακτοφυλακή των ΗΠΑ) που έχουν ως κύριο μέλημα την βελτίωση της ανθεκτικότητας των πλοίων και των εγκαταστάσεων και την προστασία της ασφάλειας των πλωτών οδών στις οποίες λειτουργούν.

Μια έκθεση που δημοσιεύθηκε από το Inmarsat υπογραμμίζει τον ρόλο του κώδικα διαχείρισης κινδύνων στον κυβερνοχώρο του 2021 του IMO στην παροχή ενός πλαισίου για την ανθεκτικότητα. Θεωρείται φυσική επέκταση των τρεχουσών πρακτικών διαχείρισης λειτουργικού κινδύνου που ενσωματώνονται στα υπάρχοντα Συστήματα Διαχείρισης Ασφάλειας στο πλαίσιο του υφιστάμενου Κώδικα ISM (MSC.428(98)).Το Σχέδιο Κυβερνοασφάλειας θα πρέπει, τουλάχιστον, να περιλαμβάνει:

1. Μια διαδικασία για την αρχική διαλογή συμβάντος
2. Βήματα για την καραντίνα όλης της ηλεκτρονικής κίνησης από και προς το πλοίο ή τον στόλο. Διαδικασίες για την ειδοποίηση και το αίτημα από τους προμηθευτές επικοινωνίας για έλεγχο της κυκλοφορίας
3. Διαδικασίες για την παρακολούθηση της κατάστασης του τμήματος ασφάλειας πληροφορικής
4. Διαδικασίες για την ασφάλεια/καθιέρωση εφεδρικών επικοινωνιών με τα πληττόμενα σκάφη
5. Βήματα σταθεροποίησης και απομόνωσης του μολυσμένου συστήματος για προστασία από περαιτέρω εξάπλωση
6. Βήματα για τη συλλογή πληροφοριών και αποδεικτικών στοιχείων από επηρεαζόμενα συστήματα
7. Διαδικασίες για την εξ αποστάσεως εκτέλεση ανάκτησης κρίσιμων συστημάτων
8. Ρυθμίσεις για την πλήρη αντικατάσταση του συστήματος στο επόμενο ασφαλές λιμάνι μετά από ένα συμβάν στον κυβερνοχώρο

Καλό θα ήταν να υπάρχουν σχέδια αντιμετώπισης για πιθανές αστοχίες σε κρίσιμα συστήματα του πλοίου, με τις διαδικασίες να περιγράφονται στα εγχειρίδια έκτακτης ανάγκης ενός σκάφους, έτσι ώστε ο καπετάνιος να μπορεί να ανταποκριθεί χωρίς να χρειάζεται να ζητήσει βοήθεια από συναδέλφους στην ξηρά. Αυτά τα σχέδια θα πρέπει να παρέχουν στον καπετάνιο οδηγίες ή/και μια λίστα ελέγχου για το τι πρέπει να κάνει. Πιο συγκεκριμένα, μπορεί να περιλαμβάνουν:

1. Ενέργειες για την επαναφορά κατεστραμμένων/αποτυχημένων προγραμμάτων-πελατών email ή υποβαθμισμένων/αποτυχημένων συνδέσμων επικοινωνίας πλοίου-ακτής π.χ. η χρήση εφεδρικού FleetBroadband για email/φωνή μέχρι την ανάκτηση
2. Ενέργειες για την αντιμετώπιση/ανάκτηση αποτυχημένων υπολογιστών
3. Χρήση τηλεφώνου ακρόπολης (citadel) για αποστολή τέλεξ. Δοκιμή εφεδρικού αναγνωριστικού email από πλοίο σε ακτή και αντίστροφα.
4. Επιστροφή στους εκτυπωμένους χάρτες σε περίπτωση παραβιασμένου ECDIS

Σε όλες τις περιπτώσεις το Εγχειρίδιο Fleet ICT που εισάγεται στην τεκμηρίωση του Κώδικα SMS/ISM του πλοίου θα πρέπει να παρέχει πλήρη καθοδήγηση και να τεκμηριώνει το Σχέδιο Ασφάλειας στον Κυβερνοχώρο για όλα τα κρίσιμα συστήματα επί του πλοίου. (Safety4Sea T. E., INMARSAT: Cyber Risk Management after IMO 2021, 2022)

Οι παρακάτω συστάσεις παρέχουν μια γενική επισκόπηση των κρίσιμων βημάτων που πρέπει να ληφθούν, εάν δεν υπάρχουν ήδη. Καλό θα ήταν να τηρηθούν όχι μόνο από τις ναυτιλιακές εταιρίες αλλά από όλους τους οργανισμούς και τα μέλη που απαρτίζουν το Σύστημα Θαλάσσιων Μεταφορών, όπως είναι οι ιδιοκτήτες, οι χειριστές, οι εργολάβοι, οι πωλητές, οι φορείς εκμετάλλευσης λιμένων και άλλα αρμόδια μέρη

4.2.1 Πιστοποιητικά προμηθευτών

Με τους νέους ισχύοντες νόμους και κανονισμούς όλες οι εταιρίες, ναυτιλιακές και μη, πρέπει να είναι πιστοποιημένες αφού βεβαιωθούν οι εκάστοτε ελεγκτές ότι οι διαδικασίες που ακολουθούν είναι σύμφωνα με τα πλαίσια - πρότυπα IMO, ISO ή/και NIST προκειμένου να τους χορηγηθούν τα αποδεικτικά στοιχεία διαπιστεύσεων ασφαλείας, όπως το ISO27001. Συνήθως μπορεί να διαρκέσει αρκετό χρόνο όχι μόνο ο έλεγχος και οι διαδικασίες της πιστοποίησης όσο η αναμόρφωση της όλης νοοτροπίας και των πρακτικών που εφάρμοζαν οι εταιρείες πρωτύτερα. Ωστόσο, αυτή η πολιτική ανάπτυξης προστασίας είναι άκρως σημαντική. Κατά αυτόν τον τρόπο εξασφαλίζεται τόσο η ακεραιότητα του συστήματος όσο και η αξιοπιστία του ίδιου του προμηθευτή απέναντι στη ναυτιλιακή εταιρεία.

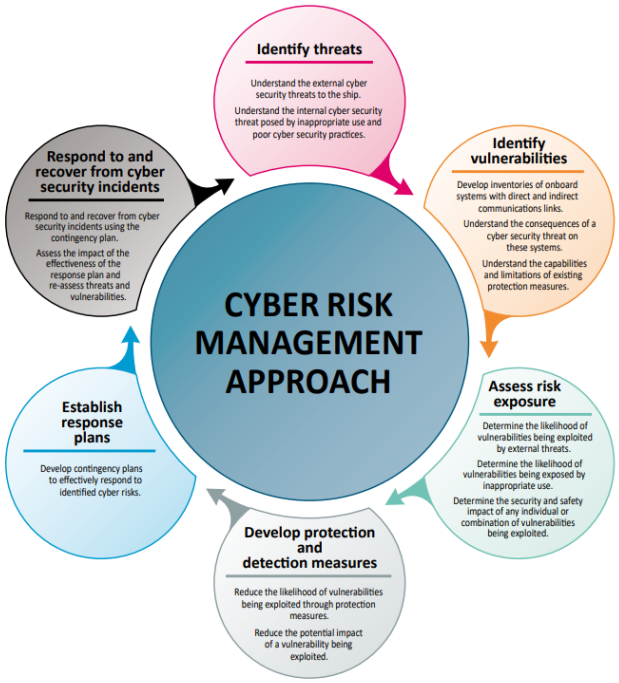
Βέβαια, μετά την εγκατάσταση των συστημάτων στο πλοίο, όσο αυτό είναι αγκυροβολημένο στο λιμάνι, καλό θα ήταν να γίνει ένας επανέλεγχος από εμπειρογνώμονες για τυχόν αστοχίες, παραλείψεις ή νέες νουθετήσεις, καθώς τότε είναι πιο εύκολο να εντοπιστούν και να διορθωθούν τυχόν τρωτά σημεία. Στην περίπτωση που βρεθεί κάτι, η καταγραφή του είναι σημαντική ώστε να επανεξεταστεί στο μέλλον ή σε άλλο πλοίο, καθώς τα ζητήματα ασφάλειας στη θάλασσα συχνά είναι συστημικά, δηλαδή δεν επηρεάζουν μόνο ένα πλοίο του στόλου, το ίδιο ζήτημα μπορεί να τα επηρεάσει όλα (Munro, Tactical Advice for Maritime Cyber Security – Top 10, 2022).

4.2.2 Εκτίμηση κινδύνου

Στο τεύχος Phish and Ships του Μαΐου 2019, στο Be Cyber Aware at Sea υπάρχει μια εικόνα για την έκθεση Cost of Data Breach της Ponemon του 2018, σύμφωνα με την οποία η μέση παραβίαση δεδομένων κοστίζει 3,8 εκατομμύρια δολάρια και η πιθανότητα επαναλαμβανόμενης παραβίασης τα επόμενα δύο χρόνια είναι 27,9%. Και αυτός είναι ένας από τους λόγους που οι εταιρείες θέτουν την ασφάλεια στον κυβερνοχώρο προτεραιότητα. Συν τοις άλλοις η επίθεση μπορεί να συντελέσει στην απώλεια των δεδομένων τους και όχι μόνο`. Καλό θα ήταν όλοι, ιδιοκτήτες, χειριστές σκαφών και εγκαταστάσεων να διεξάγουν αξιολογήσεις κυβερνοασφάλειας για καλύτερη κατανόηση της έκτασης των ευπαθειών τους στον κυβερνοχώρο. Μια καλή πρακτική τόσο για μετριασμό της επίθεσης αλλά και για κατευθυντήριες γραμμές εφόσον γίνει είναι η εκτίμηση κινδύνου (risk assessment). Η εκτίμηση κινδύνου είναι ένας όρος που χρησιμοποιείται για να περιγράψει τη συνολική διαδικασία ή μέθοδο όπου προσδιορίζεται ο κίνδυνος και οι

παράγοντες του. Αναλύεται, αξιολογείται η σοβαρότητα και η επικινδυνότητα του και καθορίζονται οι τρόποι αντιμετώπισης ή ελέγχου του. (Risk Assessment, 2022)

Η εκτίμηση κινδύνου πρέπει να διεξάγεται μεμονωμένα για κάθε εταιρεία, προκειμένου να εντοπιστούν οι μοναδικές ανάγκες της για την προστασία κρίσιμων συστημάτων. Ας μην ξεχνάμε άλλωστε πως τα κρίσιμα συστήματα στο πλοίο είναι κυρίως εκείνα που συμβάλλουν στην πρόωση και την πλοήγησή του. Θα πρέπει να προσδιοριστεί σε σχέση με τα συστήματα και τις

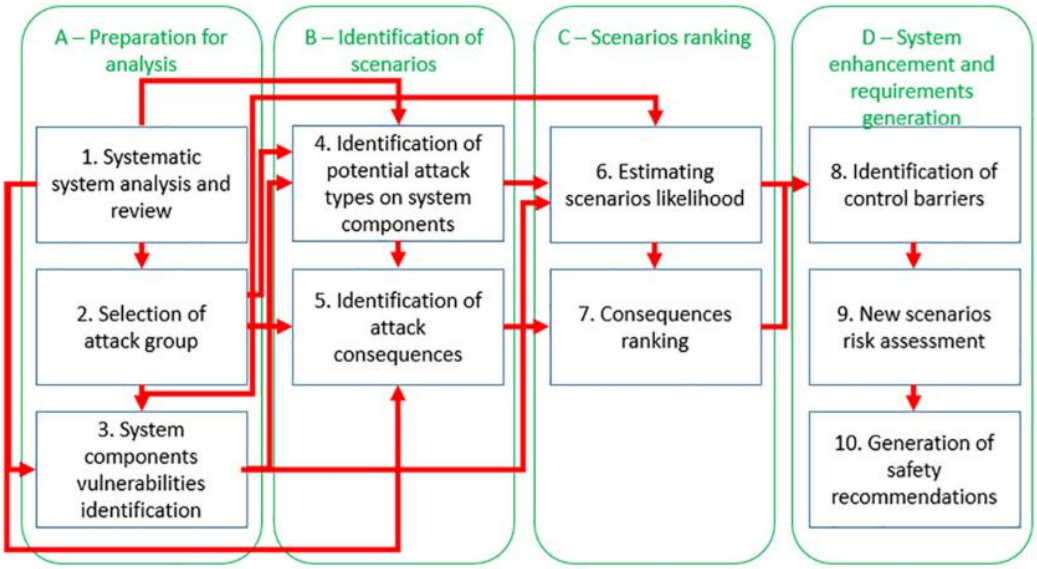


Εικόνα 64 - Προσέγγιση διαχείρισης κινδύνων στον κυβερνοχώρο όπως ορίζεται στις κατευθυντήριες γραμμές BIMCO. (The Guidelines On Cyber Security Onboard Ships, 2021)

λειτουργίες του οργανισμού, να αναλυθούν οι συνέπειες των βλαβών του συστήματος σε όλα τα επίπεδα προκειμένου να εκτιμηθούν οι επιπτώσεις στο σύνολό τους. Η διαδικασία της εκτίμησης κινδύνου θα πρέπει, επίσης, να αναγνωρίζει πιθανά μέτρα μείωσής του και να καθορίζει τις απαραίτητες ενέργειες που θα πρέπει να ακολουθηθούν. Οι οργανισμοί θα πρέπει να κοινοποιούν με σαφήνεια την προσέγγισή τους στη διαχείριση κινδύνων με την ανάπτυξη εφαρμοστέων πολιτικών και πρακτικών. Αυτές στοχεύουν στη διατήρηση της θαλάσσιας ασφάλειας στον κυβερνοχώρο, διασφαλίζοντας ότι το προσωπικό επί του σκάφους και της ξηράς γνωρίζει την προσέγγιση, τον τρόπο λήψης αποφάσεων και τυχόν ισχύοντα όρια κινδύνου.

Ο Akash Bharadia, ειδικός τεχνολογίας στο τμήμα Cyber & Tech της AXIS Capital, σχολίασε πως όταν μια εταιρεία παραβιάζεται, τότε λαμβάνει δράση ο σχεδιασμός απόκρισης που σαν στόχο έχει την μείωση της ζημιάς και του χρόνου αποθεραπείας. Όπως προτείνει «Καθορίστε τα βασικά άτομα που πρέπει να βρίσκονται στο κατάστρωμα κατά τη διάρκεια ενός περιστατικού στον κυβερνοχώρο. Τεκμηριώστε τους ρόλους και τις αρμοδιότητες, καθώς και τα στοιχεία επικοινωνίας, βεβαιωθείτε ότι υπάρχει ένα σχέδιο επικοινωνίας έκτακτης ανάγκης και μην βασίζεστε σε διευθύνσεις email ή τηλέφωνα γραφείου». Επίσης, συνιστά την εξοικείωση με τις υπηρεσίες αντιμετώπισης παραβίασης, καθώς η εξάσκηση σε ποικίλα σενάρια, ο έλεγχος και η ενημέρωση μετά από κάθε εκτέλεση πρακτικής είναι αυτά που φροντίζουν για την ύπαρξη αρκετής κάλυψης. (Safety4Sea T. E., How to handle data breaching, 2022)

Μια μέθοδος είναι η CYber-Risk Assessment for Marine Systems (CYRA-MS) που αναπτύχθηκε σε μία μελέτη βάσει της Προκαταρκτικής Ανάλυσης Κινδύνου στον Κυβερνοχώρο (CPHA)[50]. Η CYRA-MS αποτελείται από τέσσερις φάσεις (Α έως Δ) και ακολουθεί συνολικά δέκα βήματα, όπως φαίνεται στο διάγραμμα ροής που απεικονίζεται στην παρακάτω εικόνα. Η μέθοδος ξεκινά με την αναγνώριση των στοιχείων του συστήματος και την αντιστοίχιση των σχετικών συνδέσεων/αλληλεπιδράσεων, καθώς είναι σημαντικό πρώτα να κατανοήσουμε επαρκώς το υπό διερεύνηση σύστημα. Η σωστή κατανόηση των λειτουργιών και των αλληλεπιδράσεων των στοιχείων θα υποστηρίξει τον εντοπισμό των συνεπειών της επίθεσης. Στη συνέχεια, επιλέγεται μια συγκεκριμένη ομάδα επίθεσης για την ανάλυση καθώς διαφορετικές ομάδες επίθεσης θα επικεντρωθούν σε διαφορετικά σενάρια επίθεσης. Παράλληλα, βάσει μιας υπάρχουσας βάσης δεδομένων τρωτών σημείων, εντοπίζονται οι υπάρχουσες ευπάθειες για τα στοιχεία του συστήματος.



Εικόνα 65 - Διάγραμμα ροής μεθόδου CYRA-MS (A novel cyber-risk assessment method for ship systems, 2022)

Τα τρωτά σημεία χρησιμοποιούνται για τον εντοπισμό πιθανών επιθέσεων. Με βάση τον συγκεκριμένο στόχο της ομάδας επίθεσης και τα τρωτά σημεία, προσδιορίζονται οι πιθανοί τύποι επιθέσεων μαζί με τις πιθανές συνέπειες. Στο Βήμα 6, παρέχεται μια εκτίμηση για την πιθανότητα επιτυχίας κάθε συγκεκριμένου σεναρίου επίθεσης με βάση τις ακόλουθες παραμέτρους: στόχους ομάδας επίθεσης, επίπεδο δραστηριότητας, τεχνολογικό επίπεδο, επίπεδο συνδεσιμότητας, απαιτούμενους πόρους για την εκμετάλλευση ευάλωτων ικανοτήτων και διαθέσιμα εμπόδια ελέγχου. Οι διαφορετικές συνέπειες ταξινομούνται ως προς τη σοβαρότητά τους στο Βήμα 7. Ακολούθως, προτείνονται μέτρα ελέγχου για κάθε επικίνδυνο σενάριο και αυτό επαναξιολογείται με βάση τα νέα μέτρα ελέγχου. Τέλος, συνοψίζονται οι διαφορετικές απαιτήσεις ασφάλειας και οι

[50] Η CPHA είναι παρόμοια με την κλασική Αναγνώριση Κινδύνου (Hazard Identification - HAZID), η οποία χρησιμοποιείται ευρέως στη ναυτιλιακή βιομηχανία, επομένως μπορεί να γίνει εύκολα κατανοητή και να χρησιμοποιηθεί από τους μηχανικούς ασφαλείας στην αρχική της μορφή ή σε τροποποιημένη. Επιπλέον, παρόμοια προσέγγιση που βασίζεται στο CPHA έχει υιοθετηθεί από την Bureau Veritas (BV) σύμφωνα με τους κανόνες της NR659. Αυτή η προσέγγιση φαίνεται να είναι περισσότερο ευθυγραμμισμένη με τις πρότυπες κατευθυντήριες γραμμές IEC 62433 για την αξιολόγηση του κινδύνου στον κυβερνοχώρο βιομηχανικών συστημάτων, καθώς τα αποτελέσματα HAZID προτείνεται να χρησιμοποιηθούν ως στοιχεία για την αξιολόγηση. Η καινοτομία της μεθόδου CYRA-MS σε σύγκριση με την CPHA περιλαμβάνει: (α) την εξέταση των στόχων της ομάδας επίθεσης στην ανάλυση.(β) την ενσωμάτωση διαφορετικών τύπων επίθεσης. (γ) εκτίμηση της πιθανότητας επιτυχών επιθέσεων λαμβάνοντας υπόψη τους στόχους της ομάδας επίθεσης, το επίπεδο δραστηριότητας, το τεχνολογικό επίπεδο, το επίπεδο συνδεσιμότητας, τους απαιτούμενους πόρους και τα διαθέσιμα εμπόδια ελέγχου·(δ) επέκταση του πίνακα συνεπειών της Επίσημης Αξιολόγησης Ασφάλειας (FSA) για να καταστεί δυνατή η κατάταξη των σεναρίων από οικονομική άποψη, ασφάλεια και περιβαλλοντική άποψη. (Bolbot, Theotokatos, Boulougouris, & Vassalos, 2022)

προτάσεις για το σχεδιασμό του συστήματος με βάση τα προηγούμενα βήματα. (Bolbot, Theotokatos, Boulougouris, & Vassalos, 2022)

Αφότου γίνει η εκτίμηση κινδύνου καθίσταται πιο εφικτή και η διαχείριση του. Η επιδιόρθωση δεν είναι μικρή εργασία, αλλά είναι ο πυρήνας της υγιεινής στον κυβερνοχώρο. Με την χρήση ενός τυπικού πλαισίου όπως αυτό που παρέχεται από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST), μπορεί να γίνει εντοπισμός σε κενά στους ελέγχους. Εκεί με την εκχώρηση μιας πιθανότητας σε ένα ανεπιθύμητο αποτέλεσμα και του πιθανού αντίκτυπου του, το προϊόν και των δύο είναι ο κίνδυνος. Η διαχείριση του μπορεί να περιέχει ενέργειες όπως αποφυγή, αποδοχή, μετριασμός με πρόσθετους ελέγχους ή ακόμα και μεταφορά μέσω ασφάλισης. (Hamilton, 2022)

Άλλος τρόπος εξασφάλισης των δεδομένων είναι η τακτική λήψη αντιγράφων ασφαλείας και η αποθήκευση αυτών σε εξωτερικές μονάδες εκτός δικτύου. Πρέπει επίσης να αποφασιστεί σε ποια κρίσιμα συστήματα θα δοθεί προτεραιότητα καθώς η γρήγορη αποκατάσταση τους είναι απαραίτητη για την ομαλή λειτουργία του οργανισμού. Τα συστήματα που έχουν υψηλές απαιτήσεις διαθεσιμότητας δεδομένων θα πρέπει να είναι όσο το δυνατόν περισσότερο ασφαλή. Τα ΟΤ συστήματα θα πρέπει να διαθέτουν εφεδρικά συστήματα που θα επιτρέπουν στο πλοίο να ανακτήσει γρήγορα και με ασφάλεια τις ικανότητες πλοήγησης και λειτουργίας μετά από μία κυβερνό- επίθεση.

Η διαχείριση του κινδύνου μπορεί να προσδιοριστεί και με οποιαδήποτε εσωτερική ή εξωτερική πηγή εξειδικευμένης εμπειρογνωμοσύνης. Το Υπουργείο Εσωτερικής Ασφάλειας (DHS) Cybersecurity and Infrastructure Security Agency (CISA) παρέχει αρκετούς δωρεάν πόρους για να βοηθήσει τους ιδιοκτήτες πλοίων να αξιολογήσουν την κατάσταση των δικτύων τους και να εντοπίσουν τις ευπάθειες στον κυβερνοχώρο. Ένας τέτοιος πόρος είναι το Εθνικό Κέντρο Ενοποίησης Κυβερνοασφάλειας και Επικοινωνιών (NCCIC) Hunt and Incident Response Team (HIRT). Το NCCIC HIRT είναι η οντότητα πρώτης γραμμής του DHS για την προληπτική αναζήτηση κακόβουλης διαδικτυακής δραστηριότητας και την απόκριση σε περιστατικά στον κυβερνοχώρο. Οι παγκοσμίου φήμης εμπειρογνώμονες της HIRT ηγούνται των προσπαθειών απόκρισης, περιορισμού, αποκατάστασης και ανάκτησης περιουσιακών στοιχείων σε κυβερνητικούς οργανισμούς, υποδομές ζωτικής σημασίας και οργανισμούς του ιδιωτικού τομέα. Οποιαδήποτε εταιρεία μπορεί να ζητήσει υπηρεσίες HIRT επισκεπτόμενος τον ιστότοπο της https://www.us-cert.gov . Μετά από μια δέσμευση DHS HIRT, η εταιρεία θα λάβει μια εμπιστευτική αναφορά με αναλύσεις και συστάσεις μετριασμού, καθώς και βοήθεια για την αποκατάσταση των υπηρεσιών. (Guard, 2022)

4.2.3 Εκπαίδευση – Ανθρώπινο Δυναμικό

Αρχικά, καλό είναι να σημειωθεί ότι παρά την τάση για αυτοματοποίηση, η συμμετοχή και η αξία του ανθρωπογενούς παράγοντα πάνω στα πλοία δεν πρέπει να υποβαθμίζεται. Αυτό σημαίνει ότι ακόμα και αν τα μηχανήματα λειτουργούν όπως επιβάλουν οι προδιαγραφές τους, το πλήρωμα είναι αυτό που τα χειρίζεται. Αν δεν υπάρχει επαρκής γνώση ή σωστή κρίση για τη λειτουργία των μηχανημάτων τότε μπορεί είτε να προγραμματιστούν λανθασμένα ή να παρερμηνευτούν οι ενδείξεις τους. Για τον λόγο αυτό η εκπαίδευση στα συστήματα που υπάρχουν πάνω στο πλοίο είναι ζωτικής σημασίας και μάλιστα θα πρέπει να γίνεται έγκαιρα. Ναι μεν στις σχολές δίδονται οι πρώτες βάσεις, όμως κάθε εταιρία και κάθε πλοίο έχει τις δικές του ιδιαιτερότητες.

Οπότε με την ένταξη του ναυτικού στην εταιρία θα πρέπει να καθοριστεί η γνώση πάνω στα συστήματα και να μην θεωρείται αυτονόητη. Δεδομένου ότι η τεχνολογία συνεχώς εξελίσσεται, έτσι και η γνώση πρέπει διαρκώς να ανανεώνεται. Οι αξιωματικοί βάρδιας πρέπει να ελέγχουν τα δεδομένα πλοήγησης που προέρχονται από την τεχνολογία του πλοίου σε σχέση με τις πραγματικές συνθήκες. Το GPS μπορεί να πλαστογραφηθεί, οι θέσεις ECDIS μπορούν να χειραγωγηθούν και ακόμη και το συνθετικό ραντάρ μπορεί να δημιουργήσει ψευδείς αναφορές όταν παραβιαστεί. Είτε πρόκειται για πλοήγηση, ή για αποφυγή σύγκρουσης ή για φόρτωση, το ανθρώπινο μάτι πρέπει να χρησιμοποιηθεί για να διασφαλιστεί ότι η κατάσταση έξω από τη γέφυρα αντικατοπτρίζει αυτό που αναφέρει η τεχνολογία.

Σύμφωνα με το νέο καθεστώς, θα πρέπει να διεξάγονται περιοδικά ασκήσεις σε όλο τον στόλο τουλάχιστον μία φορά το χρόνο για τη δοκιμή των διαδικασιών απόκρισης και την αξιολόγηση της ετοιμότητας του πληρώματος. Αυτό σημαίνει ότι οι ιδιοκτήτες και οι διαχειριστές πλοίων θα πρέπει να δίνουν στις ασκήσεις για την ασφάλεια στον κυβερνοχώρο την ίδια βαρύτητα που δίνουν σε κάθε κανονική άσκηση διαχείρισης συμβάντων, όπως προσάραξης, πυρκαγιάς ή σύγκρουσης. Φρόνιμο, επίσης, θα ήταν να γίνει εξ αρχής κατανομή των καθηκόντων ανάλογα με τις ικανότητές του εκάστοτε μέλους. Δηλαδή, να ορίζεται ένα άτομο ή μια ομάδα που θα αναλάβει όλες τις πτυχές που σχετίζονται με τον τομέα της ασφάλειας στον κυβερνοχώρο. Για να επιτευχθούν αυτά, ο Διαχειριστής Συμβάντος του πλοίου οφείλει να επιδείξει αποτελεσματική ηγεσία για να διασφαλίσει την ασφάλεια του πλοίου, του πληρώματος και του φορτίου του, επιτρέποντας παράλληλα σε αυτήν την ομάδα να επικεντρωθεί στο δικό της έργο.

Αντίστοιχη εκπαίδευση πρέπει να λαμβάνει και το ανθρώπινο δυναμικό που βρίσκεται στη στεριά. Ένα μέρος της περιλαμβάνει τη διαχείριση και το σωστό φιλτράρισμα των εισερχόμενων μηνυμάτων. Παρόλο που υπάρχουν antivirus και τεχνικοί που ελέγχουν αν τα email είναι spam/phishing, καλό είναι όλα τα μέλη μιας εταιρίας και ενός πλοίου να είναι σε θέση να τα αναγνωρίζουν, ώστε να μην πέσουν θύματα από τέτοιου είδους επίθεση. Το ηλεκτρονικό ψάρεμα (προσπάθειες λήψης διαπιστευτηρίων σύνδεσης μέσω ψεύτικων ιστοτόπων) είναι από τις πιο κοινές επιθέσεις.

Υπάρχουν ορισμένοι πόροι όπως το Be Cyber Aware At Sea – που αναπτύχθηκαν από μια κοινοπραξία πλοιοκτητών και ναυτιλιακών οργανισμών – που βοηθούν στην ευαισθητοποίηση και στην αποφυγή ευπαθειών στον κυβερνοχώρο. Οι τακτικές εκστρατείες κατά του ηλεκτρονικού ψαρέματος και οι δοκιμές διείσδυσης που χρησιμοποιούν προσομοιωμένα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν να διατηρήσουν υψηλά επίπεδα επαγρύπνησης. Ο Σύνδεσμος P&I της Βόρειας Αγγλίας παρέχει ορισμένες χρήσιμες οδηγίες σχετικά με τον τρόπο αναγνώρισης μηνυμάτων ηλεκτρονικού ψαρέματος. Παρακάτω υπάρχουν μερικές χρήσιμες συμβουλές που πρέπει να λαμβάνονται υπόψιν στη λήψη ενός email:

- ✓ Αντιμετώπιση κάθε εισερχόμενου μηνύματος ως ύποπτου πόσο μάλλον όταν παρατηρείται αλλαγή συμπεριφοράς από έναν τακτικό αποστολέα.
- ✓ Αξιολόγηση πλαισίου μηνύματος ηλεκτρονικού ταχυδρομείου, δηλαδή αν είναι γνωστός ο αποστολέας και αν το μήνυμα είναι αναμενόμενο.
- ✓ Δεν πρέπει να υπάρχει βιασύνη, πόσο μάλλον όταν απαιτείται να γίνει και κάποια ενέργεια, όπως λήψη συνημμένου, άνοιγμα συνδέσμου, καταχώρηση οποιωνδήποτε ευαίσθητων δεδομένων προσωπικού χαρακτήρα.
- ✓ Σκανάρισμα συνημμένων πριν το άνοιγμα ή την εκτέλεσή τους.
- ✓ Εξέταση διεύθυνσης email ότι είναι σωστή και ότι δεν είναι παραποιημένα τα στοιχεία ή γραμμένα με διαφορετικό αλφάβητο.
- ✓ Επικοινωνία με τον αποστολέα του μηνύματος με άλλον τρόπο εξακριβώνοντας έτσι την γνησιότητα του email. (Safety4Sea T. E., How to identify phishing emails, 2022)

4.2.4 Λογισμικό προστασίας – Ενημερώσεις Ασφαλείας και εξωτερικά μέσα

Ένα κακόβουλο λογισμικό θα μπορούσε να επηρεάσει σοβαρά τα συστήματα ή τις υπηρεσίες του τόσο επί του σκάφους όσο και στην ξηρά. Οι οργανισμοί θα πρέπει να εφαρμόζουν μια κατάλληλη πολιτική κατά του κακόβουλου λογισμικού για να υπερασπιστούν σε βάθος τα δίκτυά τους και να αποτρέψουν τη μη εξουσιοδοτημένη πρόσβαση. Αυτό μπορεί να επιτευχθεί με την εγκατάσταση βασικού αντιικού λογισμικού προγράμματος. Επιπρόσθετα, ανά τακτά χρονικά διαστήματα θα πρέπει να γίνονται και οι ενημερώσεις ασφαλείας των συστημάτων, εφόσον είναι διαθέσιμες. Συνήθως, ένας κατασκευαστής δημοσιεύει τέτοια ενημέρωση για βελτίωση του συστήματος και διόρθωση τυχόν ευπαθειών. Οπότε καλό είναι να γίνονται έγκαιρα οι ενημερώσεις προτού εντοπιστούν τα τρωτά σημεία του συστήματος από τους κακόβουλους χρήστες.

Είναι κοινή πρακτική ορισμένα δεδομένα να μεταφέρονται στο λιμάνι ή σε τρίτους (προμηθευτές κ.λπ.) μέσω μονάδας USB. Οι θύρες USB είναι μια επικείμενη απειλή καθώς μπορεί από κει να εισαχθεί κακόβουλο λογισμικό στα κρίσιμα συστήματα του πλοίου. Τα USB stick, οι μονάδες flash, ακόμη και τα τηλέφωνα μετακινούνται μεταξύ υπολογιστών και είναι αρκετά

εύκολο να συλλάβουν κακόβουλο λογισμικό. Για την αποτροπή της τυχαίας εισαγωγής του στα, καλό θα ήταν να δημιουργηθούν πολιτικές αφαιρούμενων μέσων και να κλειδωθεί η πρόσβαση USB. Εάν τα κρίσιμα συστήματα μπορούν να ενημερωθούν μόνο μέσω USB, τα μέσα αυτά πρέπει να αποθηκευτούν σε μια ασφαλή τοποθεσία που δεν χρησιμοποιούνται για τίποτα άλλο πέρα για αυτόν τον σκοπό. Αν και αυτή η πρακτική δεν είναι ιδανική, είναι καλύτερη από την ανοιχτή πρόσβαση. Αν όχι, σημαντικό είναι να πραγματοποιείται σε κάθε εξωτερικό μέσο σάρωση για κακόβουλο λογισμικό σε αυτόνομο σύστημα προτού συνδεθεί σε οποιοδήποτε δίκτυο πλοίου, καθώς επίσης και να μην εκτελούνται ποτέ εκτελέσιμα αρχεία από μη αξιόπιστη πηγή.

4.2.5 Τοπολογία – Δίκτυο - Firewalls

Είναι επιτακτική ανάγκη οποιεσδήποτε συσκευές που είναι συνδεδεμένες στο Διαδίκτυο να έχουν ενεργοποιημένο το υψηλότερο επίπεδο ασφάλειας για να αποτρέψουν τη μετατροπή τους σε εργαλεία για τους κακόβουλους χρήστες. (Kessler & Zorri, 2022). Στην περίπτωση, όμως, που το κακόβουλο λογισμικό ή ο κακόβουλος χρήστης έχει εισαχθεί μέσα στο σύστημα, θα επιφέρει λιγότερες ζημίες αν η τοπολογία του δικτύου είναι σωστά αναδιοργανωμένη. Το παραπάνω αναφέρεται και στην στεριά, προκειμένου να μην πέσει όλο το δίκτυο της εταιρίας, αλλά και στα πλοία ώστε να μην επιτραπεί η πρόσβαση σε κρίσιμα συστήματα όπως είναι ο έλεγχος του κινητήρα.

Τα δίκτυα αναψυχής και συναλλαγών των επιβατηγών πλοίων πρέπει να διαχωρίζονται από τα επιχειρησιακά. Ωστόσο, συνήθως δεν διαθέτουν μέτρα προστασίας και τμηματοποίηση. Για αυτό, αυτά τα δίκτυα είναι από τις πιο κοινές ευπάθειες στον κυβερνοχώρο σύμφωνα με έγγραφο που δημοσιεύτηκε από το Διεθνές Επιμελητήριο Ναυτιλίας. Η εφαρμογή απλών πολιτικών και η κατάλληλη αρχιτεκτονική και τεχνική απόκριση μπορούν να βοηθήσουν στη διαχείριση ή/και στην πρόληψη αυτών των επιθέσεων από το να προκαλέσουν βλάβη.

Τα «επίπεδα» δίκτυα επιτρέπουν σε έναν αντίπαλο να ελίσσεται εύκολα σε οποιοδήποτε σύστημα που είναι συνδεδεμένο σε αυτά. Η τμηματοποίηση των δικτύων σε «υποδίκτυα» δυσκολεύει τους επιτιθέμενους να αποκτήσουν πρόσβαση σε βασικά συστήματα και εξοπλισμό. Η βασική ιδέα πίσω από τη δημιουργία μιας βελτιστοποιημένης τοπολογίας δικτύου είναι η εφαρμογή της έννοιας της «άμυνας σε βάθος» για την αύξηση της ανθεκτικότητάς του. Είναι μια στρατηγική διασφάλισης που έχει σχεδιαστεί για να παρέχει πλεονασμό σε περίπτωση που ένας έλεγχος ασφαλείας αποτύχει ή γίνει εκμετάλλευση μιας ευπάθειας. Τα πιο κρίσιμα συστήματα δικτύου που χρειάζονται καλύτερη προστασία πρέπει να βρίσκονται πιο βαθιά στην τοπολογία. Μια βασική ευπάθεια προέρχεται από τις προσωπικές υπολογιστικές συσκευές των μελών του πληρώματος. Θα ήταν συνετό να γίνεται επαναληπτικός έλεγχος προκειμένου να είναι σίγουρο ότι τα ενσωματωμένα συστήματα είναι διαχωρισμένα.

Επίσης, ορισμένες συστάσεις που σχετίζονται με τη ρύθμιση του συστήματος περιλαμβάνουν την εγκατάσταση προστατευτικού λογισμικού, όπως τείχη προστασίας, τη χρήση ασφαλούς δορυφορικής σύνδεσης και την εγκατάσταση συστημάτων ανίχνευσης εισβολής σε διαφορετικές ζώνες καθώς και την εξάλειψη των συνδέσεων επικοινωνίας στο Διαδίκτυο. Εφαρμόζοντας ένα μοντέλο διαχωρισμού δικτύου, οι σχεδιαστές μπορούν να χρησιμοποιούν τείχη προστασίας για να προστατεύουν κάθε ζώνη ξεχωριστά. Τα τείχη προστασίας περιέχουν πολιτικές ασφαλείας που ελέγχουν τις διευθύνσεις IP ώστε ανάλογα να επιτραπεί ή να απαγορευτεί η είσοδος σε κάθε ζώνη.

Βέβαια εάν δεν ρυθμιστούν σωστά, μπορούν να περιορίσουν όχι μόνο την ύποπτη αλλά και τη νόμιμη κυκλοφορία. Αυτό μπορεί να προκαλέσει ορισμένες επιπτώσεις στο σύστημα όπως το να επηρεάσει αρνητικά την παραγωγικότητά του ή να οδηγήσει τους χρήστες να εργαστούν εν αγνοία τους με κακόβουλα μέσα. Επιπλέον, τα τείχη προστασίας που βασίζονται σε λογισμικό έχουν το ελάττωμα ότι μειώνουν τη συνολική απόδοση της συσκευής καθώς χρησιμοποιούν την ισχύ της CPU και τη μνήμη RAM για να λειτουργήσουν. Τα τείχη προστασίας που βασίζονται σε υλικό, από την άλλη, δεν αντιμετωπίζουν το προηγούμενο αλλά είναι πολύ πιο ακριβά και απαιτούν εκπαιδευμένο προσωπικό για την εγκατάσταση, την παρακολούθηση και τη συντήρησή τους.

Εξίσου σημαντικό είναι να ελέγχονται τα δίκτυα που παρέχουν στους προμηθευτές απομακρυσμένη πρόσβαση στα συστήματα ναυσιπλοΐας και σε άλλα OT συστήματα του πλοίου. Αυτά τα δίκτυα ενδέχεται να είναι απαραίτητα για τους προμηθευτές ώστε να επιτρέπουν τη μεταφόρτωση των αναβαθμίσεων του συστήματος ή την απομακρυσμένη εκτέλεση εργασιών συντήρησης. Η απομακρυσμένη πρόσβαση στο σύστημα προσφέρει μεν μεγάλα οφέλη, αλλά εγκυμονεί και νέους κινδύνους. Κατά συνέπεια, θα πρέπει να θεσπιστούν πολιτικές και διαδικασίες για την υποστήριξη της απομακρυσμένης πρόσβασης στα συστήματα, που θα ισχύουν για τους παρόχους υπηρεσιών. Η διαχείριση διαμόρφωσης βελτιώνει την ασφάλεια των συστημάτων και εξαλείφει τον κίνδυνο παραβίασης. Επομένως, οι οργανισμοί θα πρέπει να αναπτύξουν μια στρατηγική για την αφαίρεση περιττών λειτουργιών από τα συστήματα και να διορθώσουν γρήγορα γνωστά τρωτά σημεία.

Ο τρόπος με τον οποίο άλλοι έχουν πρόσβαση στο δίκτυο ενός πλοίου είναι επίσης ένα βασικό στοιχείο. Τα εικονικά ιδιωτικά δίκτυα (VPN) μπορούν να προσφέρουν ένα επιπλέον επίπεδο προστασίας διαχωρίζοντας την κίνηση του πληρώματος ή τρίτων από το δίκτυο του πλοίου. Ωστόσο, η ανθεκτικότητα εξαρτάται από τη σωστή διαμόρφωση και την καλή διαχείριση των VPN. Σε ορισμένες περιπτώσεις, όπου χρησιμοποιούνται πολλά, μπορούν να αυξήσουν την επιφάνεια επίθεσης του πλοίου και να καταφέρουν να διεισδύσουν στο σύστημα του.

4.2.6 Κωδικοί και κρυπτογράφηση

Ένα ίσως από τα πιο σημαντικά μέτρα ασφαλείας είναι οι κωδικοί ασφαλείας. Αρχικά, με το που γίνει εγκατάσταση ενός συστήματος θα πρέπει να αλλάξουν τα διαπιστευτήρια του admin και να μην είναι σε σημείο όπου οποιοσδήποτε θα μπορούσε να έχει πρόσβαση. Η κατάργηση της χρήσης γενικών διαπιστευτηρίων σύνδεσης για πολλαπλό προσωπικό, η δημιουργία προφίλ δικτύου για κάθε εργαζόμενο, η απαίτηση από τους υπαλλήλους για έναν κωδικό πρόσβασης για να συνδεθούν στον εξοπλισμό του σκάφους θα μπορούσαν να είναι από τα πρώτα μέτρα. Ακόμη, οι χρήστες θα πρέπει να μην κοινοποιούν για κανέναν λόγο τους κωδικούς τους και να δημιουργούνται με υψηλό βαθμό δυσκολίας. Επιπρόσθετο μέτρο αποτελεί ο έλεγχος ταυτότητας διπλού παράγοντα.

Επίσης, σε όλους τους χρήστες θα πρέπει να παρέχεται ένα εύλογο επίπεδο προνομίων συστήματος και δικαιωμάτων που είναι απαραίτητα για την επίτευξη του καθορισμένου έργου. Στην περίπτωση παραχώρησης αυξημένων προνομίων συστήματος θα πρέπει να γίνεται πιο προσεκτικός έλεγχος. Σημαντική επιπλέον είναι και η φειδωλή χρήση του λογαριασμού του διαχειριστή, να γίνεται μόνο όταν αύτη κρίνεται απαραίτητη. Επιπρόσθετα, ένα από τα συστήματα με κωδικούς ασφαλείας είναι και το Wi-Fi. Οι ισχυροί κωδικοί πρόσβασής του και του διαχειριστή δρομολογητή είναι απαραίτητοι. Οι προσωπικές συσκευές του πληρώματος δεν πρέπει να συνδέονται σε οτιδήποτε άλλο εκτός από το διαδίκτυο. Οποιαδήποτε συστήματα πλοίων χρησιμοποιούν Wi-Fi (π.χ. tablet για comms και πλοήγηση) πρέπει να έχουν αυξημένα τα επίπεδα ασφάλειας, συμπεριλαμβανομένων ισχυρών μέτρων ελέγχου ταυτότητας.

Τέλος, θα μπορούσε να χρησιμοποιηθεί κρυπτογράφηση για να διασφαλιστεί η εμπιστευτική επικοινωνία μεταξύ δύο κόμβων δικτύου. Ούτε ο δίαυλος CAN ούτε τα PGN NMEA 2000 έχουν πρόβλεψη για κρυπτογράφηση. Η δυνατότητα φυσικής εισαγωγής ενός αδίστακτου κόμβου στο δίαυλο CAN και η έλλειψη εμπιστευτικότητας στις μεταδόσεις παρέχει πολλούς τρόπους με τους οποίους ένας κακόβουλος παράγοντας μπορεί να έχει πρόσβαση και, πιθανώς, να διεισδύσει σε πληροφορίες από το δίκτυο ενός σκάφους, για παράδειγμα, μπορεί να παρακολουθεί όλες ή ένα επιλεγμένο υποσύνολο μεταδόσεων στο δίαυλο επικοινωνιών ή μπορεί να αποθηκεύσει τις πληροφορίες για μεταγενέστερη ανάκτηση ή να μεταδώσει τις πληροφορίες σε άλλο σύστημα εντός ή εκτός του σκάφους σε πραγματικό χρόνο.

4.2.7 Jamming And Spoofing στην Πλοήγηση

Από τα πιο συχνά περιστατικά είναι οι πλαστογραφήσεις των γεωγραφικών συστημάτων του πλοίου ή οι σκόπιμες παρεμβολές στο σήμα. Η NovAtel, πάροχος τεχνολογίας GNSS, και η Hexagon, παγκόσμια εταιρεία τεχνολογίας πληροφοριών δηλώνουν ότι ο πιο αποτελεσματικός

τρόπος προστασίας στην περίπτωση παραπλάνησης από jamming είναι η παρακολούθηση ενός κρυπτογραφημένου σήματος. Αυτό μπορεί να είναι το σήμα του κωδικού Y στο GPS L1 και L2 που μεταδίδεται από αρκετούς από τους αστερισμούς GNSS. Η πρόσβαση στα κρυπτογραφημένα σήματα είναι περιορισμένη και δεν είναι διαθέσιμη σε όλους τους χρήστες, ωστόσο υπάρχουν μέθοδοι μετριασμού που μπορούν να χρησιμοποιηθούν με ανοιχτούς δέκτες σημάτων.

Άλλες στρατηγικές που προτείνουν είναι το φιλτράρισμα στον δέκτη, το οποίο είναι αποτελεσματικό για σήματα εκτός ζώνης, η προσθήκη μιας αδρανειακής μονάδας μέτρησης (IMU) στον δέκτη, η χρήση προσαρμοζόμενης διάταξης κεραίας, όπως οι κεραίες με μοτίβο ελεγχόμενης λήψης (CRPA), η ανάπτυξη προηγμένων τεχνικών μετριασμού με χρήση σημάτων ευρείας ζώνης GNSS και η χρήση των δεκτών E-Loran ως εφεδρικών. Η βοήθεια του δέκτη/εξοπλισμού πλοήγησης με ένα IMU και ένα κατάλληλο σχέδιο διαχείρισης συναγερμού θα βελτιώσει σημαντικά την ικανότητα ανίχνευσης μιας επίθεσης. Όσον αφορά την εμπλοκή, διάφορα GNSS παρέχουν διαφορετικές υπηρεσίες σε διαφορετικές συχνότητες. Για την Ανοιχτή Υπηρεσία και για θαλάσσιους δέκτες εγκεκριμένου τύπου κατά IEC 61108-3, οι συχνότητες είναι στη θέση E1 και E5. Η χρήση διαφορετικών συχνοτήτων θα μετριάσει σε κάποιο βαθμό μια επίθεση, αλλά δεν σημαίνει απαραίτητα ότι το σύστημα θα λειτουργήσει μέσω αυτής.

Σχετικά με την πλαστογράφηση, βιώσιμα αντίμετρα περιλαμβάνουν τη χρήση συστοιχιών κεραιών όπως και στο jamming. Ωστόσο, όταν εξετάζουμε το ενδεχόμενο πλοίων με πολλαπλές κεραίες GNSS να υποστηρίζουν διαφορετικές λειτουργίες, τίθεται το ερώτημα ποιες κεραίες να προστατεύονται. Η απάντηση δεν είναι απλή και το κόστος δεν είναι αμελητέο. Επιπλέον, οι κρυπτογραφικές τεχνικές μπορούν να είναι αποτελεσματικές, εφόσον τα μηνύματα πλοήγησης περιλαμβάνουν ένα σήμα που αποτελείται από ορισμένα συγκεκριμένα μέρη και να μην μπορούν να δημιουργηθούν από μια πλαστογράφηση. Έναντι απλών επιθέσεων πλαστογράφησης, η παρακολούθηση ορισμένων δεικτών βασικής απόδοσης (KPI) του δέκτη GNSS μπορεί να είναι επιτυχής, όπως παρακολούθηση για άλματα ρολογιού, ασυνήθιστες ή απίθανες αναλογίες πυκνότητας σήματος προς θόρυβο ή διαφορές μεταξύ μετρήσεων κώδικα και φορέα. Καλό θα ήταν να γίνει έλεγχος με τον κατασκευαστή του εξοπλισμού πώς ο εξοπλισμός του μπορεί να λύσει αυτά τα ζητήματα. Τέλος, ένα κομμάτι που αφορά το λογισμικό κομμάτι (ECDIS) είναι η χρήση Fly wheel αλγορίθμων για την απαγόρευση του συστήματος από άμεσα άλματα θέσης και χρόνου στον δέκτη GNSS.

Επιπλέον, η Διεθνή Ένωση Πλοιοκτητών Δεξαμενοπλοίων πρόσθεσε ορισμένες προτάσεις τόσο για την κατάσταση του πλοίου αλλά και για τους πλοηγούς, χωρίς όμως να ξεχνάμε την σπουδαιότητα της ύπαρξης των έντυπων χαρτών και τη σχεδίαση της διαδρομής πάνω σε αυτούς. Δηλαδή, όταν η κατάσταση είναι κάπως σταθερή προτείνεται ο τακτικός έλεγχος της θέσης, η αναφορά διακοπών ή ανωμαλιών του GNSS στις αρχές, η λήψη κρίσιμων πληροφορίων, όπως η πραγματική τοποθεσία (γεωγραφικό πλάτος/μήκος), η ημερομηνία/ώρα και η διάρκεια της διακοπής καθώς και η λήψη αποδεικτικών στοιχείων των αστοχιών εξοπλισμού κατά τη διάρκεια μιας διακοπής για τους αναλυτές προκειμένου να εντοπίσουν μια πιθανή αιτία. Οι οδηγίες που αφορούν τους πλοηγούς είναι οι εξής:

- Οι ενέργειες για την ανίχνευση πλαστογράφησης και παρεμβολής GPS θα πρέπει να περιλαμβάνουν τη χρήση ραντάρ και ενδιάμεσου συστήματος απεικόνισης γραφημάτων και πληροφοριών (ECDIS) (επικάλυψη ή υπόστρωμα), που είναι από τις καλύτερες μεθόδους για τον εντοπισμό εμπλοκής και πλαστογράφησης όταν η γη είναι ορατή στο ραντάρ.
- Επαλήθευση θέσης σε κατάλληλα διαστήματα, όπως ορίζεται στον Οδηγό για Ασφαλή Πλοήγηση, συμπεριλαμβανομένου του ECDIS.
- Παρατήρηση σημαντικής διαφοράς μεταξύ της θέσης DR[51] (η θέση έφτασε με διεύθυνση Gyro Course και απόσταση ανά ημερολόγιο ταχύτητας) και της διόρθωσης GNSS.

[51] Dead-Reckoning: Στην πλοήγηση, η νεκρή καταμέτρηση είναι η διαδικασία υπολογισμού της τρέχουσας θέσης κάποιου κινούμενου αντικειμένου χρησιμοποιώντας μια προηγουμένως καθορισμένη θέση ή επιδιόρθωση και στη συνέχεια ενσωματώνοντας εκτιμήσεις της ταχύτητας, της κατεύθυνσης πορείας και της πορείας για το χρόνο που έχει περάσει. (Dead reckoning, 2022)

- Παρατήρηση και επαλήθευση χρησιμοποιώντας ηχώ για σύγκριση των βάθεων κατά την πλεύση σε κατάλληλες περιοχές.

Στην περίπτωση που εντοπιστεί εμπλοκή και πλαστογράφηση τότε θα πρέπει να γίνουν άμεσα οι παρακάτω ενέργειες:

- Επιλογή ενός δευτερεύοντα αισθητήρα θέσης χειροκίνητα
- Εάν παρέχεται επιλογή άλλης εισόδου GNSS και δημιουργία συναγερμού «απόκλισης GNSS» για τον έλεγχο τυχόν οριακής διαφοράς μεταξύ των πηγών εντοπισμού θέσης.
- Εάν ένας δευτερεύων αισθητήρας δεν είναι σε θέση να παρέχει τη θέση ενός σκάφους και δεν υπάρχουν άλλα μέσα για τη στερέωση θέσης εισόδου, ο πλοηγός θα πρέπει να επιλέξει τη λειτουργία DR ή EP[52].
- Προσπάθεια εντοπισμού απόστασης από την ακτή και αναζήτηση μεγαλύτερου θαλάσσιου χώρου.
- Προσεκτική χρήση του συστήματος AIS καθώς ενδέχεται να επηρεαστεί και αυτό από επίθεση παρεμβολών ή πλαστογράφησης.
- Χρήση της μεθόδου παράλληλης ευρετηρίασης κατά τη διάρκεια της ακτοπλοΐας για να διατηρηθούν ασφαλείς αποστάσεις και να καθοριστούν σημεία στροφής.
- Εάν η εξακρίβωση της θέσης του σκάφους είναι ανέφικτη σε σχέση με τους κινδύνους ναυσιπλοΐας, τότε σταμάτημα του σκάφους. (Intertanko, 2022)

Από την άλλη ο καπετάνιος Dana A. Goward και ο καθηγητής Todd Humphreys του Πανεπιστημίου του Τέξας, σε μία δημοσίευση τους αναφέρουν πως υπάρχουν πράγματα που μπορούν να κάνουν οι πλοίαρχοι, οι εταιρείες και τα έθνη για να αποτρέψουν αυτού του είδους τις θαλάσσιες επιθέσεις στον κυβερνοχώρο.

Οι πλοίαρχοι θα πρέπει:

- να γνωρίζουν όλες τις ηλεκτρονικές συσκευές που υπάρχουν στο πλοίο (των επιβατών και του πληρώματος) και να εξετάσουν το ενδεχόμενο να θέσουν τις αμφισβητούμενες συσκευές σε καραντίνα κατά τη διάρκεια του ταξιδιού.
- να σκεφτούν το ενδεχόμενο να αποκτήσουν έναν ανιχνευτή και να τον χρησιμοποιούν τακτικά ενώ βρίσκονται στη θάλασσα.
- να διασφαλίζουν ότι η φυσική ασφάλεια αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση σε τοποθεσίες κοντά σε κεραίες GPS/GNSS.
- να χρησιμοποιούν πολλαπλές πηγές πληροφοριών πλοήγησης όποτε είναι δυνατόν.

Οι εταιρείες θα πρέπει:

- να βεβαιωθούν ότι ο εξοπλισμός δορυφορικής πλοήγησης σκάφους διαθέτει τεχνολογία κατά της εμπλοκής και της πλαστογράφησης.
- να εξασφαλίσουν ότι οι δέκτες έχουν πρόσβαση σε πολλαπλά δορυφορικά συστήματα εκτός από το GPS.
- να εξοπλίσουν τα σκάφη με δύο κεραίες GPS/GNSS και να διαχωρήσουν τα φυσικά όσο το δυνατόν περισσότερο. Αυτό κάνει την πλαστογράφηση του δέκτη πολύ πιο δύσκολη, καθώς απαιτεί από τον εισβολέα να συντονίσει μια συνεπή επίθεση και στις δύο κεραίες ταυτόχρονα.
- να παράσχουν στα σκάφη δέκτες Loran/eLoran για να εκμεταλλευτούν τα σήματα όταν είναι διαθέσιμα.

Τα έθνη θα πρέπει:

- να καταπολεμήσουν επιθετικά την εισαγωγή, πώληση και χρήση εξοπλισμού παρεμβολής και πλαστογράφησης GPS/GNSS.

[52] Estimated Position: Ο υπολογισμός νεκρών καταμετρήσεων χρησιμοποιεί μόνο πορεία, ταχύτητα, χρόνο και απόσταση για να καθορίσει μια κατά προσέγγιση θέση. Απαιτούνται δύο ή περισσότερες γραμμές θέσης για τον καθορισμό της πραγματικής θέσης ενός σκάφους. Μια εκτιμώμενη θέση είναι οτιδήποτε ενδιάμεσο. Ως αποτέλεσμα, μπορεί να είναι μια θέση DR με το set και το drift να λαμβάνονται υπόψη. Μπορεί επίσης να είναι μια ενιαία γραμμή θέσης σε γραφική παράσταση σε μια θέση DR. Ενώ οι εκτιμώμενες θέσεις είναι κατά προσέγγιση, είναι πιο ακριβείς από μια απλή θέση DR. (Estimated Position, 2022)

- να παρέχουν ένα σήμα επίγειας πλοήγησης που είναι δύσκολο να διακοπεί ως συμπλήρωμα και εφεδρικό για δορυφορικά συστήματα και να ενθαρρύνουν τη χρήση του. (Humphrey, 2022)

4.2.8 Δορυφορικές Επικοινωνίες

Ο ανώτερος συνεργάτης της Pen Test Partners και ηθικός χάκερ Ken Munro πρότεινε σε μια δημοσίευση του τις παρακάτω πρακτικές όσον αφορά το σύστημα SATCOM. Οι λύσεις για το συγκεκριμένο σύστημα είναι οι εξής:

1. Δεν θα πρέπει να είναι διαθέσιμο από το δημόσιο Διαδίκτυο. Οι περισσότεροι - αλλά όχι όλοι - πάροχοι δορυφορικού Διαδικτύου και επικοινωνιών προσφέρουν έναν ιδιωτικό χώρο διευθύνσεων IP ως μέτρο για την αποτροπή πρόσβασης χάκερ στο σύστημα. Υπάρχουν διάφορες μέθοδοι για να εξακριβωθεί εάν τα τερματικά satcom του σκάφους είναι δημόσια ή ιδιωτικά. Ο πιο γρήγορος τρόπος είναι να πληκτρολογήσει κανείς τη διεύθυνση IP σε ένα πρόγραμμα περιήγησης σε έναν υπολογιστή που είναι συνδεδεμένος μέσω δημόσιας σύνδεσης. Εάν ο χώρος διευθύνσεων IP για το σύστημα satcom είναι ιδιωτικός, δεν πρέπει να υπάρχει πρόσβαση στη διεπαφή ιστού του τερματικού. Εναλλακτικά, μπορεί να γίνει επικοινωνία με τον πάροχο διαδικτύου για τον έλεγχο. Τέλος, η εκτέλεση μιας σάρωσης θύρας στο σύστημα θα βοηθήσει στην εύρεση ανοιχτών θυρών όπου θα μπορούσαν να κάνουν το σύστημα ευάλωτο σε επιθέσεις. Υπάρχουν πολλές διαδρομές προς ένα πλοίο, αλλά το satcom box είναι η μόνη διαδρομή που υπάρχει σχεδόν πάντα στο διαδίκτυο (Munro, Hacking vessel satcoms, 2022).
2. Αλλαγή προεπιλεγμένων κωδικών πρόσβασης διαχειριστή με πιο σύνθετους. Παραδόξως, αυτό είναι «μακράν το πιο κοινό πρόβλημα», σύμφωνα με τον κ. Munro. Τις περισσότερες φορές, όταν εγκαθίσταται το δορυφορικό τερματικό, το πρόγραμμα εγκατάστασης δεν αλλάζει τους προεπιλεγμένους κωδικούς, με αποτέλεσμα να σπάνε εύκολα.
3. Οι ενημερώσεις λογισμικού του συστήματος είναι ζωτικής σημασίας για την ασφάλεια στον κυβερνοχώρο. Μέρος της ενσωματωμένης διαδικασίας θα πρέπει να είναι η διασφάλιση ότι το λογισμικό ενημερώνεται κάθε φορά που ο κατασκευαστής δημοσιεύει μια ενημέρωση. Για να γίνει αυτό με μη αυτόματο τρόπο, θα πρέπει να γίνεται τακτικός έλεγχος των σελίδων ενημέρωσης λογισμικού του προμηθευτή του τερματικού, καθώς οι επιδιορθώσεις ασφαλείας συχνά κρύβονται στο αρχείο καταγραφής αλλαγών και δεν είναι εύκολο να βρεθούν. Για μείωση χρόνου και προσπάθειας μπορεί να χρησιμοποιηθεί μια υπηρεσία ειδοποίησης ενημέρωσης κώδικα. Οι ενημερώσεις συνήθως περιλαμβάνουν διορθώσεις για ελαττώματα ασφαλείας, επομένως όσο πιο ξεπερασμένο είναι το λογισμικό, τόσο πιο ευάλωτο είναι σε επιθέσεις. (Munro, Satellite communications equipment security, 2022)

Για την αποτροπή πρόσβασης οποιουδήποτε μη εξουσιοδοτημένου χρήστη και πόσο μάλλον με δικαιώματα root όσον αφορά το VSAT, έχουν δοθεί ορισμένες προτάσεις από τον Andrew Tierney στο Defcon28. Αρχικά, το σύστημα αυτό θα έπρεπε να το εγκαθιστά η ίδια η ναυτιλιακή εταιρία και όχι ένα τρίτο συμβαλλόμενο μέρος. Στην συνέχεια, θα πρέπει να αλλάζουν οι κωδικοί πρόσβασης, καθώς και να γίνεται έλεγχος της τοπολογίας γεγονός που ισχύει για όλα τα συστήματα (Defcon28, 2022).

4.3 Ναυτιλιακά Σεμινάρια για την Κυβερνοασφάλεια

Μία ενδεικτική εικόνα για το τι συμβαίνει στην πραγματικότητα μπορούμε να έχουμε από ορισμένα σεμινάρια που πραγματοποιήθηκαν, καθώς και από τα ερωτηματολόγια που ακολούθησαν. Στο διαδικτυακό σεμινάριο της Riviera Maritime Media με θέμα «Maritime cyber risk mitigation strategies: intelligence and countermeasures» στις 29 Μαρτίου 2022, ο διευθυντής πληροφορικής του ομίλου Columbia Shipmanagement (CSM) Alexander Oswald εξήγησε τις στρατηγικές της εταιρείας για την προστασία του διαχειριζόμενου στόλου της.

Η εκπαίδευση του χερσαίου προσωπικού, των ναυτικών , όπως και των εμπλεκόμενων διευθυντών- στελεχών είναι σημαντικοί παράγοντες για την ασφάλεια στον κυβερνοχώρο. Η CSM διεξάγει μια μετρήσιμη εκστρατεία ευαισθητοποίησης και εκπαίδευσης για όλες τις επιχειρηματικές λειτουργίες και αξιολογεί την ικανότητα των ανθρώπων να εντοπίζουν απειλές στον κυβερνοχώρο. Οι αξιολογήσεις κινδύνου είναι επίσης σημαντικές για την κατανόηση των τρωτών σημείων και των κενών στην ασφάλεια.

«Η υποδομή πληροφορικής πρέπει να αξιολογείται διαρκώς για τυχόν κίνδυνους», είπε ο κ. Oswald, προσθέτοντας ότι οι ναυτιλιακές εταιρείες πρέπει να έχουν ειδικούς, έτοιμους να υποστηρίξουν τον μετριασμό των κινδύνων στον κυβερνοχώρο και να βελτιώσουν την ασφάλεια. Καλό θα είναι να εξεταστεί το ενδεχόμενο χρήσης ενός κέντρου λειτουργίας ασφαλείας (Security Operation Center - SOC) για ανίχνευση προτύπων και απειλών όλο το 24ωρο. «Δημιουργήστε ένα δίκτυο πληροφοριών κινδύνου, συνδέοντας με ειδικούς για να καλύψετε όλες τις πλευρές από το σχεδιασμό, την παρακολούθηση, την εγκληματολογία και την ασφάλιση. Να είστε προετοιμασμένοι για την αναπόφευκτη επίθεση. Είναι σημαντικό να υπάρχει αντιμετώπιση περιστατικών και ένα σχέδιο επιχειρηματικής συνέχειας» είπε καταλήγωντας ο κ. Oswald.

Ο διευθυντής IT Carisbrooke Shipping Daniel Lewandowski συμφώνησε ότι οι τρεις κύριοι παράγοντες στην ασφάλεια στον κυβερνοχώρο είναι οι άνθρωποι, οι διαδικασίες και οι τεχνολογίες. «Χρησιμοποιούμε εργαλεία, νοημοσύνη και αυτοματισμό για να μετρήσουμε την εκπαίδευση των ανθρώπων. Στη συνέχεια προσαρμόζουμε τις στρατηγικές εκπαίδευσης και διδάσκουμε στους ανθρώπους να ακολουθούν καθοδήγηση και διαδικασίες». Η Carisbrooke διαθέτει προγράμματα για την εξάλειψη πιθανών κινδύνων για το προσωπικό της, συμπεριλαμβανομένων των φίλτρων email μέσω μηχανικής εκμάθησης που αναγνωρίζει το περιεχόμενο και τα μοτίβα. Χρησιμοποιεί την πλατφόρμα Seagull της Ocean Technologies Group για εκπαίδευση πληρωμάτων και περιεχόμενο κυβερνοασφάλειας και έχει αναπτύξει το δικό της υλικό για τη διαχείριση και την ασφάλεια των κινδύνων στον κυβερνοχώρο.

Στη συνέχεια παρατίθενται ερωτήσεις και απαντήσεις από τα ερωτηματολόγια που διεξήχθησαν. Ορισμένες από αυτές ήταν αν υπάρχει ασφαλιστική κάλυψη στον κυβερνοχώρο για γραφείο και στόλο, με το 43% να απαντάει θετικά, το 42% αρνητικά και οι λοιποί είχαν μόνο σε ένα μέρος. Αν υπάρχει πιθανότητα υιοθέτησης SOC με το 57% να είναι υπό εξέταση. Και αν διεξάγεται εκστρατεία ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο των εργαζομένων, με το 72% να είναι θετικοί, το 8% αρνητικοί και οι υπόλοιποι να προετοιμάζονται για αυτήν. (Wingrove, Using intelligence to mitigate cyber risks, 2022)

Ακόμη ένα διαδικτυακό σεμινάριο από τον ίδιο όμιλο έλαβε χώρα στις 30 Μαρτίου 2022 με θέμα «How to harden maritime IT and OT to withstand cyber attacks». Σε αυτό αξιοσημείωτη είναι η συμβουλή που έδωσε στις ναυτιλιακές εταιρίες ο διευθυντής της Varuna Marine Services Sanjeev Wewerinke-Singh για την κατασκευή χαρτών δικτύου για τον εντοπισμό τρωτών σημείων και περιοχών για τη βελτίωση της ασφάλειας. Μερικά από τα ζητήματα στον κυβερνοχώρο που θα μπορούσαν να επηρεάσουν το ΟΤ περιλαμβάνουν «αστοχία συστήματος λόγω σφαλμάτων λογισμικού, δυσλειτουργία λόγω συμβάντος και απώλεια ή χειραγώγηση δεδομένων εξωτερικών αισθητήρων που είναι κρίσιμα για τις λειτουργίες του πλοίου» εξήγησε.

Μερικές από τις προκλήσεις στην εφαρμογή της ασφάλειας στον κυβερνοχώρο σε πλοία περιλαμβάνουν τη χρήση παλαιού τύπου συστημάτων πληροφορικής και ΟΤ που δεν υποστηρίζονται πλέον σε πλοία ηλικίας 15-20 ετών. «Αυτά θα μπορούσαν ακόμα να βασίζονται σε απαρχαιωμένα λειτουργικά συστήματα», είπε ο κ. Wewerinke, καθώς η ομάδα του εντόπισε ορισμένα ΟΤ του πλοίου που εργάζονται σε λειτουργικά συστήματα Microsoft Windows 7 και παλαιότερα. Μια άλλη πρόκληση είναι οι πολλαπλοί ενδιαφερόμενοι φορείς που εκμεταλλεύονται και ναυλώνουν ένα πλοίο, «με αποτέλεσμα την έλλειψη λογοδοσίας για τα συστήματα και το δίκτυο».

Είπε ότι η διαχείριση του κυβερνοκινδύνου θα είναι συγκεκριμένη για την εταιρεία και το πλοίο. «Θα πρέπει να καθοδηγούνται από τις απαιτήσεις των σχετικών εθνικών, διεθνών και κρατών σημαίας κανονισμών και κατευθυντήριων γραμμών». Η ασφάλεια στον κυβερνοχώρο πρέπει επίσης να περιλαμβάνει χαρτογράφηση δικτύου για τον εντοπισμό τρωτών σημείων μεταξύ υποσυστημάτων και εξοπλισμού από διάφορους προμηθευτές, ενσωματώνοντας ανάλυση διαδρομής οποιουδήποτε περιστατικού, συνεχή σάρωση δικτύου και παρακολούθηση για

σφάλματα και πιθανές απειλές. Οι εταιρείες πρέπει «να γνωρίζουν πώς προστατεύονται τα τελικά σημεία του δικτύου και να έχουν καλύτερη ορατότητα», είπε ο κ. Wewerinke. Ο έλεγχος των συνδέσεων και των διαχωρισμών και η διασφάλιση της συνεχούς ενημέρωσης ή της ενημέρωσης του λογισμικού είναι επίσης ζωτικής σημασίας.

Σε αυτό το σεμινάριο δύο αξιοσημείωτες ερωτήσεις που απαντήθηκαν ήταν για την ύπαρξη σχεδίων αντιμετώπισης περιστατικών ασφάλειας στον κυβερνοχώρο και ειδικών ομάδων για την κάλυψη της ασφάλειας στα OT και IT συστήματα. Στην πρώτη λίγο παραπάνω από το μισό (70%) απάντησαν θετικά ενώ στην δεύτερη ακριβώς οι μισοί. (Wingrove, How to harden maritime IT and OT, 2022). Σε μία άλλη δημοσίευσή του κλείνει λέγοντας ότι πολλά πλοία που επιθεωρήθηκαν για ζητήματα στον κυβερνοχώρο διαπιστώθηκαν ότι ήταν γεμάτα κακόβουλο λογισμικό και απροσδόκητες συνδέσεις OT/IT, αυξάνοντας τους κινδύνους. Πάντα θα υπάρχουν επιθέσεις και κενά ασφαλείας που πρέπει να αντιμετωπιστούν. Η δοκιμή σχεδίων απόκρισης συμβάντων βοηθά τους ιδιοκτήτες να ανταποκρίνονται και να ανακάμπτουν από συμβάντα στον κυβερνοχώρο, διασφαλίζοντας τη λειτουργική συνέχεια. (Wingrove, Go beyond compliance for cyber security, 2022)

Μπορούμε να πούμε πως υπάρχουν πολλά επίπεδα ασφάλειας στον κυβερνοχώρο που μπορούν να υιοθετήσουν οι οργανισμοί και οι εταιρείες, αλλά δεν πρέπει να είναι μόνο για λόγους συμμόρφωσης, όπως δήλωσε ο εκτελεστικός διευθυντής του Maritime Transportation System - Information Sharing and Analysis Center (ISAC), Scott Dickerson. Πρόσθεσε επίσης ότι «κανένας κανονισμός, οδηγία ή κατευθυντήρια γραμμή δεν περιγράφει με ακρίβεια ποιο είναι το τρέχον προφίλ κινδύνου για έναν οργανισμό. Η συμμόρφωση δεν ισοδυναμεί με την ασφάλεια ή την αποτελεσματική διαχείριση κινδύνων». Υπάρχουν απαιτήσεις από τον IMO και τις περιφερειακές αρχές, όπως η ΕΕ, και καθοδήγηση από βιομηχανικούς οργανισμούς, όπως η BIMCO. Αλλά αυτά θα πρέπει να θεωρηθούν ως το ελάχιστο για την ασφάλεια στον κυβερνοχώρο.

Το μέγεθος ενός οργανισμού δεν έχει σημασία. Καθένας κινδυνεύει από απειλές στον κυβερνοχώρο και πρέπει να κατανοήσει τα τρωτά σημεία του και να τα ενισχύσει. «Καμία οργάνωση εκεί έξω, κυβέρνηση ή πολιτικός, από όσο γνωρίζω δεν έχει αποτρέψει με επιτυχία όλες τις επιθέσεις», είπε ο κ. Dickerson. Μέρος της θεραπείας είναι η ανταλλαγή πληροφοριών σχετικά με απειλές και επιθέσεις στον κυβερνοχώρο στη ναυτιλία και στα λιμάνια. Το Maritime Transportation System ISAC είναι μια πλατφόρμα για την ανώνυμη ανταλλαγή δεδομένων, με τον ιστότοπό του www.mtsisac.org. (Wingrove, Compliance does not equal security or effective risk management, 2022)

Εν κατακλείδι, τα περιστατικά στον κυβερνοχώρο μπορούν να θέσουν σε κίνδυνο τόσο τις λειτουργίες του οργανισμού όσο και τις ανθρώπινες ζωές. Ένα είναι σίγουρο ότι οι χειριστές δεν θα μπορούν να αμυνθούν μόνοι τους. Όπως και σε πολλές άλλες ψηφιακές εξελίξεις, οι ειδικοί προτείνουν συνεργασία και ανθεκτικότητα για την εύρεση των σωστών απαντήσεων. Μελέτη που διεξήχθη από το Ponemon Institute και χρηματοδοτήθηκε από την IBM Resilient διαπίστωσε ότι οι οργανισμοί δεν είναι έτοιμοι για το GDPR. Το 77% των ερωτηθέντων δεν έχει επίσημο σχέδιο αντιμετώπισης περιστατικών ασφάλειας στον κυβερνοχώρο (CSIRP) Οι περισσότερες χώρες που συμμετείχαν στην έρευνα δεν αναφέρουν εμπιστοσύνη στην ικανότητά τους να συμμορφωθούν με τον GDPR. Σύμφωνα με τον Οδηγό Βέλτιστης Πρακτικής TMSA 3, οι εταιρείες θα πρέπει να εφαρμόζουν διαδικασίες σχετικά με τα στοιχεία ασφαλείας που αφορούν εγκαταστάσεις στην ξηρά. Η ασφάλεια στον κυβερνοχώρο στη ναυτιλιακή βιομηχανία θα πρέπει να θεωρείται ως μέρος μιας ολιστικής προσέγγισης καθ' όλη τη διάρκεια του κύκλου ζωής ενός πλοίου. (Safety4Sea T. e., 10 steps to maritime cyber security, 2022)

4.4 Αναζητήσεις Shodan

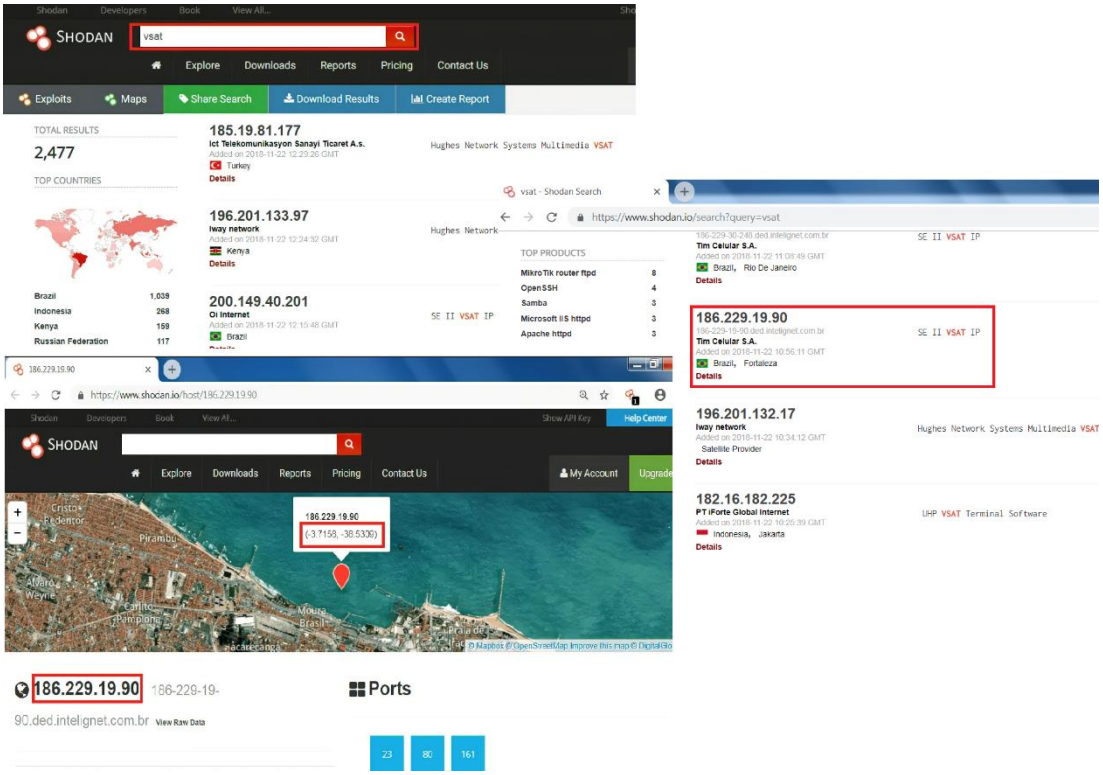
Σε προηγούμενο κεφάλαιο αναφέρθηκε ότι ένας ανεξάρτητος ερευνητής κυβερνοασφάλειας (x0rz) κατάφερε να εισέλθει στο σύστημα δορυφορικών επικοινωνιών ενός πλοίου χρησιμοποιώντας την μηχανή αναζήτησης Shodan. Αρχικά να δούμε τι είναι το Shodan. Είναι μια μηχανή αναζήτησης που συλλέγει πληροφορίες για όλες τις συσκευές που συνδέονται απευθείας στο διαδίκτυο. Εάν μια συσκευή είναι απευθείας συνδεδεμένη στο διαδίκτυο, τότε το Shodan ζητά από αυτήν διάφορες πληροφορίες που είναι διαθέσιμες στο κοινό. Το μεγαλύτερο μέρος των

δεδομένων λαμβάνεται από banner, τα οποία είναι μεταδεδομένα σχετικά με ένα λογισμικό που εκτελείται σε μια συσκευή. Οι πληροφορίες που λαμβάνονται από αυτές τις υπηρεσίες εφαρμόζονται σε πολλούς τομείς, όπως στην ασφάλεια δικτύου, στην έρευνα αγοράς, στον κυβερνορίσκο, στην παρακολούθηση της χρήσης των έξυπνων συσκευών και των ransomware. (What is Shodan?, 2022)

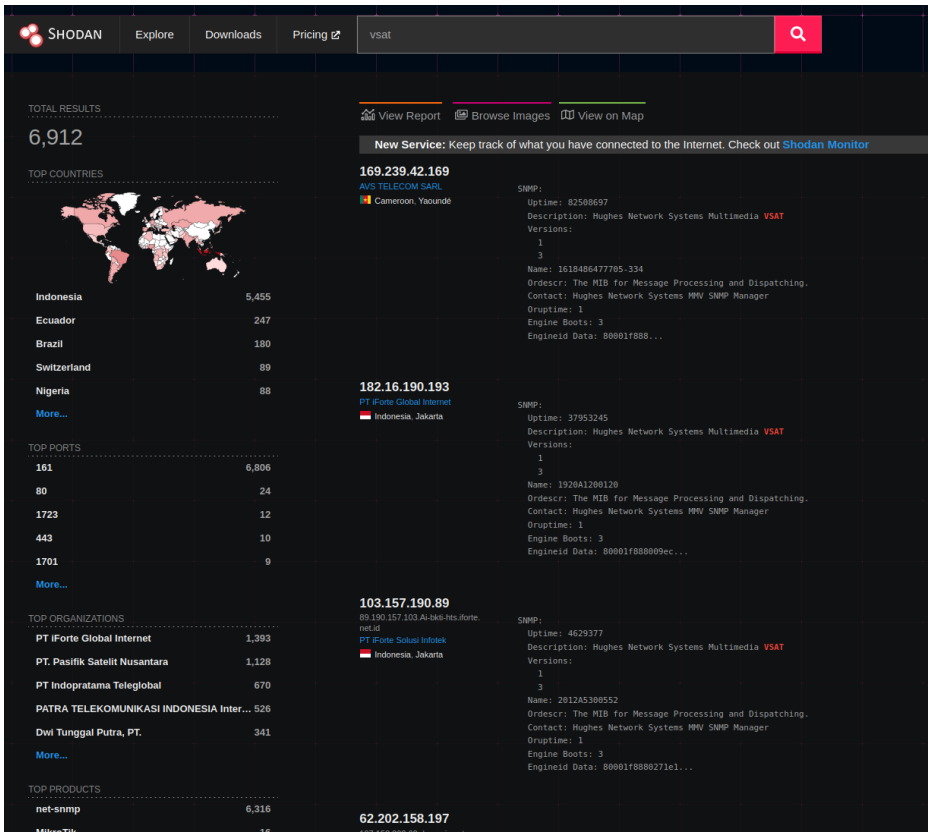
Το Shodan είναι ένας σαρωτής που εντοπίζει συσκευές συνδεδεμένες μέσω διαδικτύου δείχνοντας και τη φυσική τοποθεσία των συνδεδεμένων συσκευών. Αναπτύχθηκε από τον John Matherly το 2009 και σε αντίθεση με άλλες μηχανές αναζήτησης, αναζητά συγκεκριμένες πληροφορίες που μπορεί να είναι ανεκτίμητες για τους χάκερ. Για αυτό και κάποιοι το έχουν χαρακτηρίσει ως «την πιο επικίνδυνη μηχανή αναζήτησης στον κόσμο». Το απόρρητο των χρηστών μπορεί να παραβιαστεί διότι ένας κακόβουλος χρήστης μπορεί να κάνει ping σχεδόν σε οποιαδήποτε συσκευή χωρίς την άδεια τους. Κάποιες από τις αναζητήσεις που είχαν γίνει κατά καιρούς είχαν να κάνουν με κάμερες ασφαλείας (μην ξεχνάμε και στην ναυτιλία χρησιμοποιούνται CCTV συστήματα για την ασφάλεια 3.4.4) αλλά και συστήματα εποπτικού ελέγχου και απόκτησης δεδομένων (Supervisory control and data acquisition - SCADA) (π.χ. γεννήτριες 3.4.1). Ωστοσο, προσφέρει πολλές δυνατότητες για αναζήτηση με τους περισσότερους να το χρησιμοποιούν για την εύρεση τρωτών σημείων σε μαθήματα ηθικής πειρατείας.

Να σημειωθεί επίσης πως πολλοί από αυτούς τους ιστοτόπους και τις διεπαφές χρησιμοποιούν προεπιλεγμένους κωδικούς πρόσβασης. Στην περίπτωση αποφυγής πρόβλεψης, υπάρχουν πολλοί πόροι στον ιστό που αναφέρουν τους προεπιλεγμένους κωδικούς πρόσβασης ή ακόμα μπορούν να βρεθούν στις οδηγίες χρήσης όταν έχει συμβεί κάποιο λάθος και χρειάζεται επανεκκίνηση (OCCUPYTHEWEB, 2022). Όσον αφορά τη χρήση του Shodan, αρχικά πρέπει να γίνει εγγραφή. Δεν είναι απαραίτητη, καθώς η εφαρμογή μπορεί να χρησιμοποιηθεί και χωρίς αυτήν, αλλά δεν παρέχει τις ίδιες δυνατότητες σε έναν επισκέπτη από ό,τι σε έναν εγγεγραμμένο χρήστη, πόσο μάλλον σε μέλη που πληρώνουν για την χρήση του. Η περιήγηση μπορεί να ξεκινήσει σε οποιονδήποτε ιστότοπο/διεύθυνση IP, απλώς πληκτρολογώντας το όνομα-στόχου και θα εμφανιστούν οι λεπτομέρειές του. Υπάρχουν πολλές λέξεις-κλειδιά για αναζήτηση στο Shodan, για την εν λόγω όμως εργασία χρησιμοποιήθηκε ό,τι έχει να κάνει με τη ναυτιλία και τα συστήματά της.

Η ναυτιλία είναι πλέον πάντα ενεργή, συνδεδεμένη μέσω VSAT, GSM/LTE ακόμη και Wi-Fi. Υπάρχουν πολυάριθμα συστήματα με πρόσβαση του πληρώματος στο διαδίκτυο συνδυασμένα με ηλεκτρονικά συστήματα πλοήγησης, ECDIS, πρόωση, διαχείριση φορτίου κ.λπ. που παρέχουν πολλαπλά σημεία επαφής. Το VSAT (Very-Small-Aperture Terminal) χρησιμοποιεί IPv4 προκειμένου να επιτευχθεί η επικοινωνία του πλοίου με τον υπόλοιπο κόσμο με την χρήση δορυφόρων. Όπως το Shodan κάνει ping σε όλες τις διευθύνσεις IP μέσω του διαδικτύου, έτσι και αυτή η διαδικασία περιλαμβάνει επίσης τις IP που σχετίζονται με την επικοινωνία VSAT στο σκάφος. Αναζητώντας λοιπόν αυτήν την λέξη στο Shodan, ο συγγραφέας το 2018 δείχνει να υπάρχουν 2.477 αποτελέσματα, σχολιάζοντας «φαίνεται ότι υπάρχουν πολλές μη προστατευμένες IP πλοίων και ανοιχτές θύρες», ενώ σήμερα φαίνεται να έχουν αυξηθεί σε 6.912 όπως φαίνεται στις παρακάτω εικόνες. (Gill, 2022)

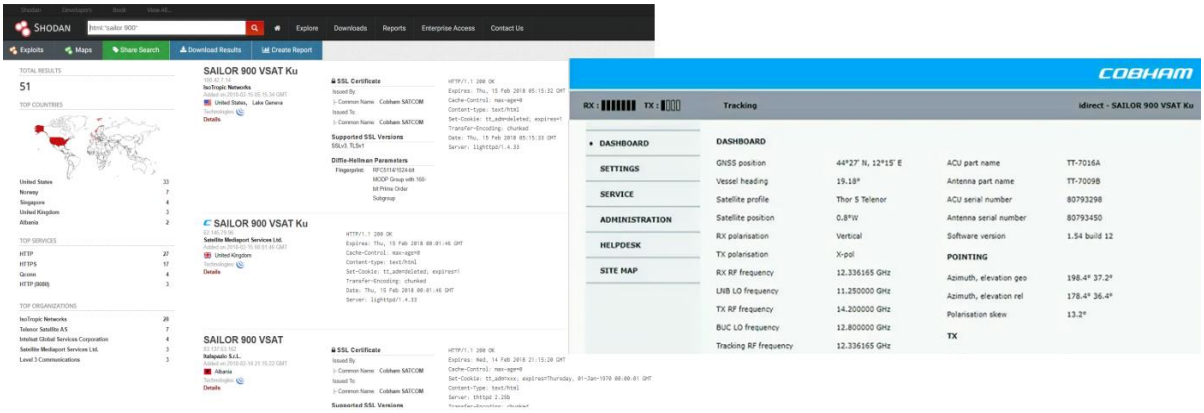


Εικόνα 66 - Αναζητήσεις με VSAT. (Gill, 2022)



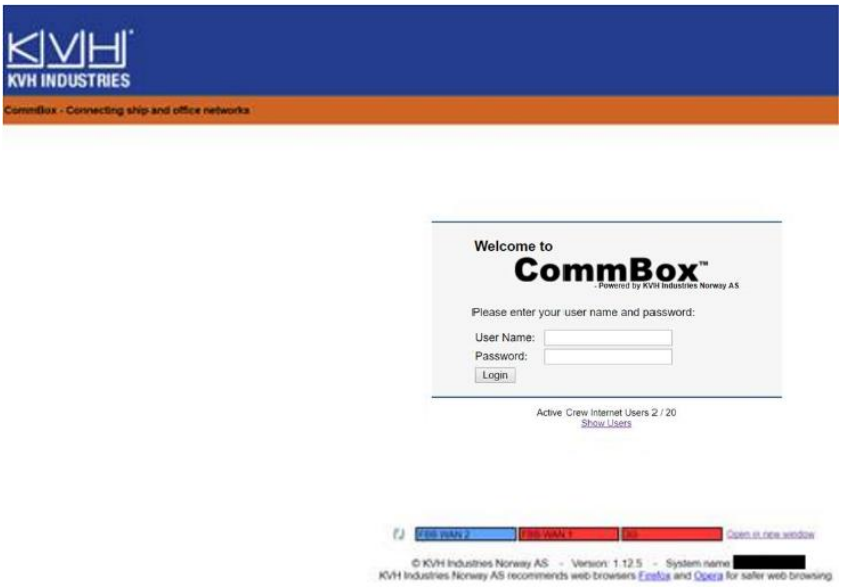
Εικόνα 67 - Αναζήτηση VSAT

Εκτός από τον συγκεκριμένο χρήστη και άλλοι έχουν καταφέρει μέσω αυτής της πλατφόρμας να εισβάλουν στα συστήματα του πλοίου. Ο Ken Munro με τη βοήθεια της διαδικτυακής πλατφόρμας Shodan, αναζητώντας μερικές από τις εφαρμογές των πλοίων, κατάφερε και εντόπισε μερικά τρωτά σημεία. Ένα από αυτά ήταν η αναζήτηση για τα τερματικά satcom. Μεγάλες μάρκες στον χώρο των θαλάσσιων satcoms, όπως οι Inmarsat, Telenor και Cobham, μπορούν να εντοπιστούν χρησιμοποιώντας το Shodan. Ένα ενδιαφέρον εύρημα ήταν για το σύστημα Cobham «Sailor 900», του οποίου οι λεπτομέρειες της δορυφορικής κεραίας δεν είχαν έλεγχο ταυτότητας και αναμενόμενα οι κωδικοί ήταν οι προεπιλεγμένοι admin/1234. Τώρα πάντως στο Shodan δεν υπάρχουν αποτελέσματα με την συγκεκριμένη αναζήτηση, γεγονός που δείχνει ότι μάλλον το πρόβλημα έχει επιλυθεί.



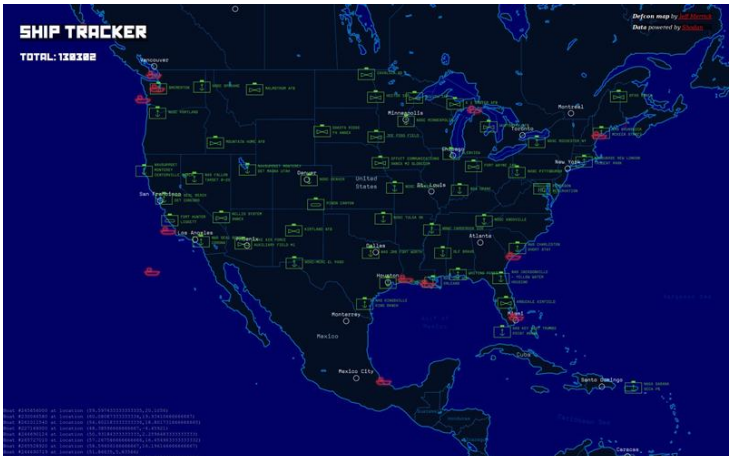
Εικόνα 68 - Εύρημα Sailor 900 (Munro, Hacking, tracking, stealing & sinking ships, 2022)

Η αναζήτησή του δεν σταμάτησε εκεί. Με τις λέξεις κλειδιά «html:commbox» αυτό που βρήκε ήταν μια ωραία συλλογή τερματικών KVH CommBox, τα οποία χρησιμοποιούνται για την αυτοματοποιημένη λειτουργία μεταφοράς αρχείων από και προς τα πλοία, σαν να ήταν μέρος του δικτύου γραφείου. Αυτό που εντόπισε ήταν η απουσία του TLS (Transport Layer Security) καθώς και κάτω από την σύνδεση ανέγραφε «Εμφάνιση Χρηστών». Από εκεί μπορούσε να δημιουργήσει μία λίστα με όλα τα μέλη του πληρώματος με αποτέλεσμα να πέσουν θύματα phishing. (Munro, OSINT from ship satcoms, 2022) Με μία επιτυχημένη τέτοια επίθεση, μπορεί να ληφθεί ο έλεγχος του φορητού υπολογιστή του μέλους αυτού και στην συνέχεια να καταφέρει να συνδεθεί σε άλλες πιο ενδιαφέρουσες συσκευές. Άλλος τρόπος θα μπορούσε να είναι η χειραγώγηση των διαπιστευτηρίων του στο commbox. Αυτό θα μπορούσε να αποτελέσει προβληματισμό για τη ναυτιλία (Munro, Hacking vessel satcoms, 2022).



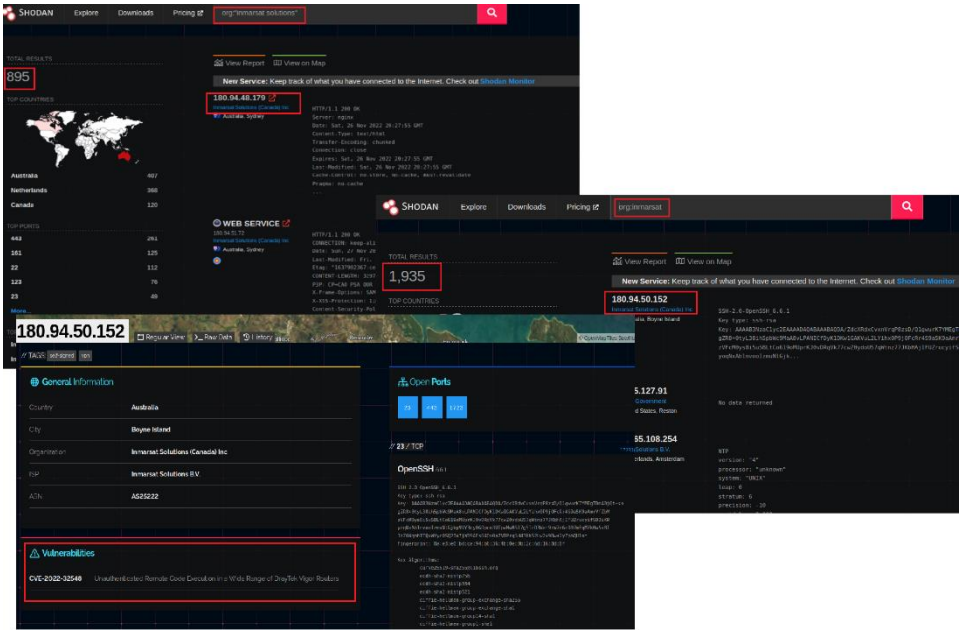
Εικόνα 69 - Αναζήτηση CommBox (Munro, OSINT from ship satcoms, 2022)

Σε ένα άλλο άρθρο ο Munro αναφέρει ότι το Shodan κυκλοφόρησε έναν γραφικό ιχνηλάτη πλοίων που με μερικές τροποποιήσεις θα «αλλάξει το παιχνίδι στη ναυτική ασφάλεια». Πιστεύει πως το Shodan Ship Tracker απλώς παρουσιάζει δεδομένα AIS, όπως κάνουν και άλλες μηχανές αναζήτησης. Αν όμως μπορούν να συνδυαστούν τα δεδομένα AIS με του Shodan τότε θα μπορούσε να υπάρξει ένας χάρτης με πλοία και ευπάθειες σε πραγματικό χρόνο κάνοντας έτσι την επιλογή ενός δυνητικά ευάλωτου πιο εύκολη. (Munro, Tracking & hacking ships with Shodan & AIS, 2022)



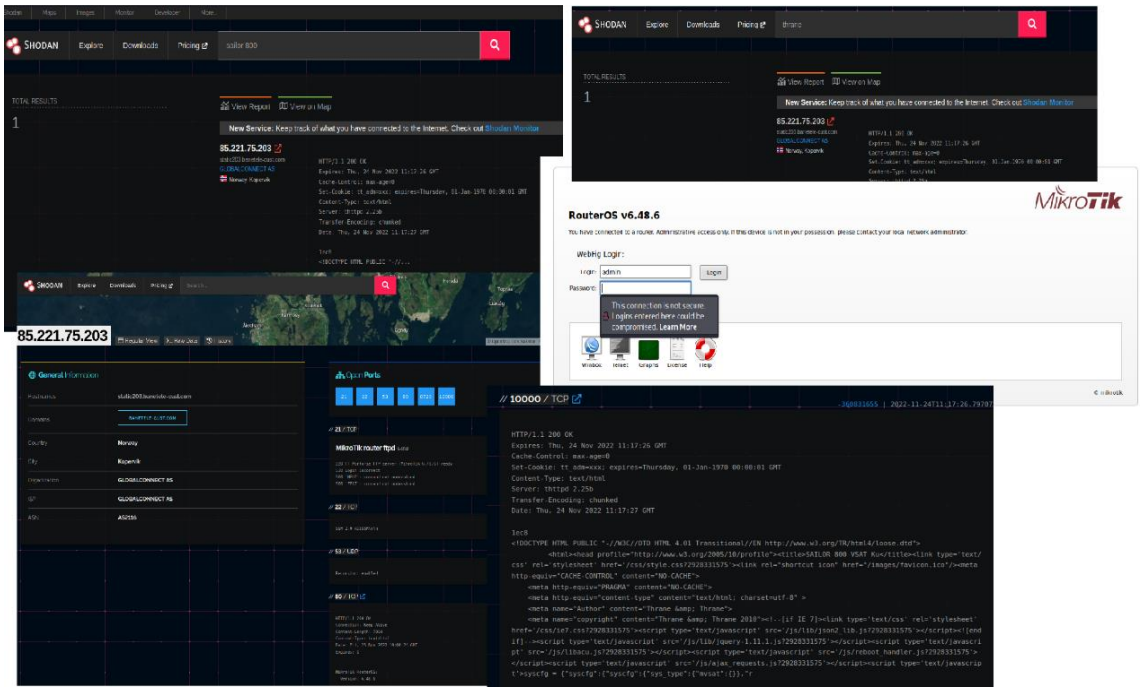
Εικόνα 70 - Γραφικός Ιχνηλάτης Shodan . (Tracking & hacking ships with Shodan & AIS)

Ακόμη, δηλώνει ότι αν γίνει αναζήτηση στο Shodan με τις λέξεις «org:"Inmarsat Solutions"» θα φανούν αρκετές συνδέσεις. Και όπως φαίνεται στην παρακάτω εικόνα με αυτά τα κριτήρια βρίσκονται 895 αποτελέσματα, ενώ 1.935 χωρίς το «Solutions» και ανοίγοντας την πρώτη κοινή IP αναφέρονται και ευπάθειες CVE-2022-32548.



Εικόνα 71 - Αναζήτηση Inmarsat

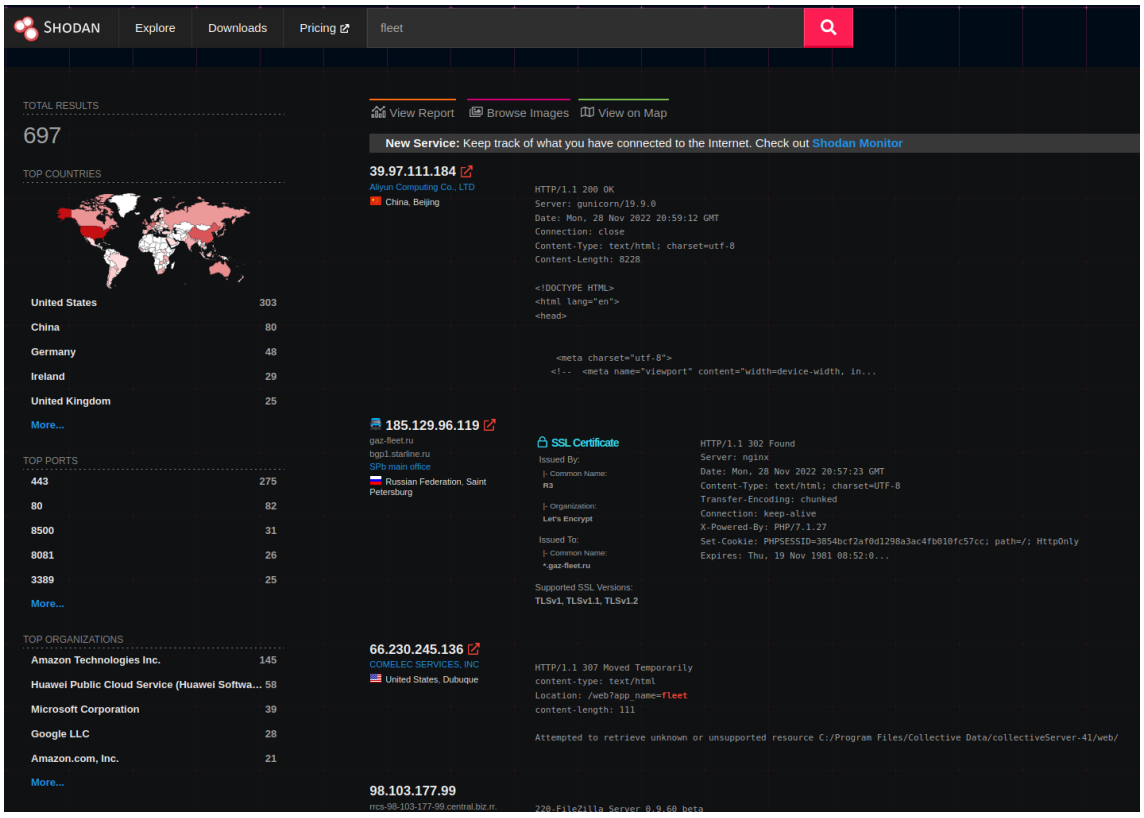
Στο ίδιο άρθρο αναφέρει και διαφορετικές εκδόσεις όπως την Thrane η οποία είναι και αυτή για δορυφορική επικοινωνία. Ψάχνοντας με αυτήν, το Shodan επιστρέφει ένα αποτέλεσμα όπως φαίνεται και στην ακόλουθη εικόνα. Στην θύρα 10000 TCP αναγράφεται και ο τίτλος sailor 800.



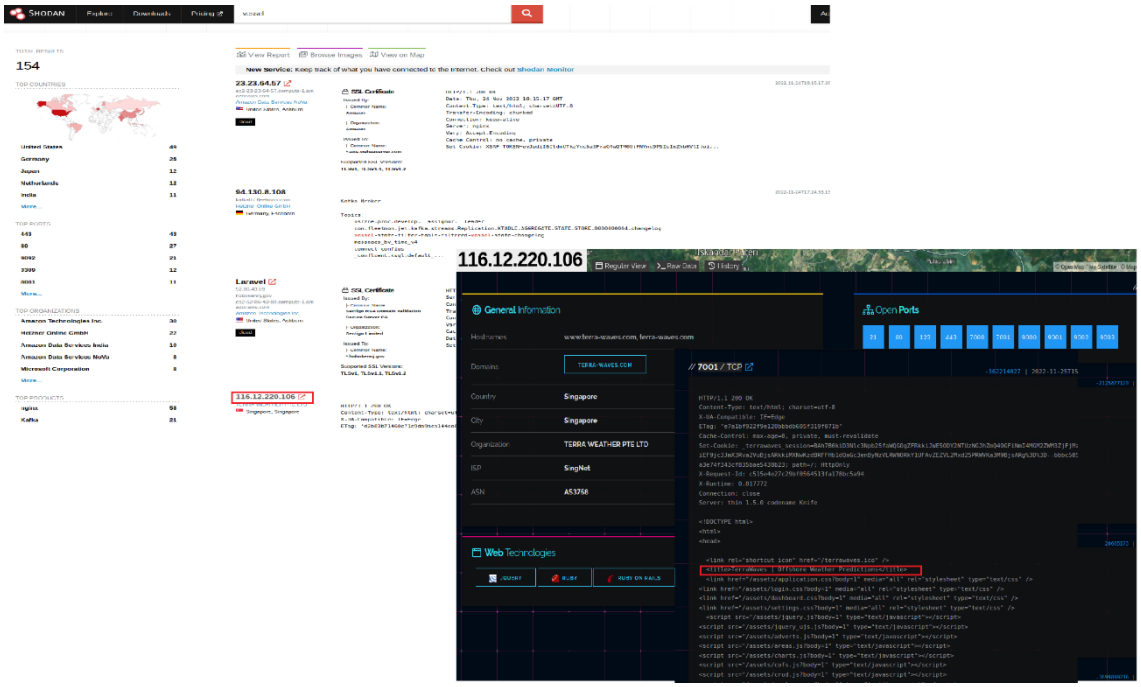
Εικόνα 72 - Αναζήτηση Thrane / Sailor 800

Μια άλλη ομάδα ερευνητών κυβερνοασφάλειας ανακάλυψε ότι η διαμόρφωση των συστημάτων δορυφορικής κεραίας ορισμένων πλοίων μπορεί να αποτελέσει το αίτιο για επιθέσεις. Τα προεπιλεγμένα διαπιστευτήρια σύνδεσης, τα οποία βρίσκονται εύκολα στο διαδίκτυο, παραμένουν αμετάβλητα σε τουλάχιστον ορισμένες από αυτές τις συσκευές που εντόπισαν στο Shodan. Οποιοσδήποτε που μπορεί να αποκτήσει πρόσβαση στο εν λόγω σύστημα θα μπορούσε να αλλάξει χειροκίνητα τις συντεταγμένες GPS ενός πλοίου ή, ενδεχομένως, ακόμη και να σπάσει πλήρως το σύστημα πλοήγησης του σκάφους, ανεβάζοντας νέο υλικολογισμικό. (Morse, 2022)

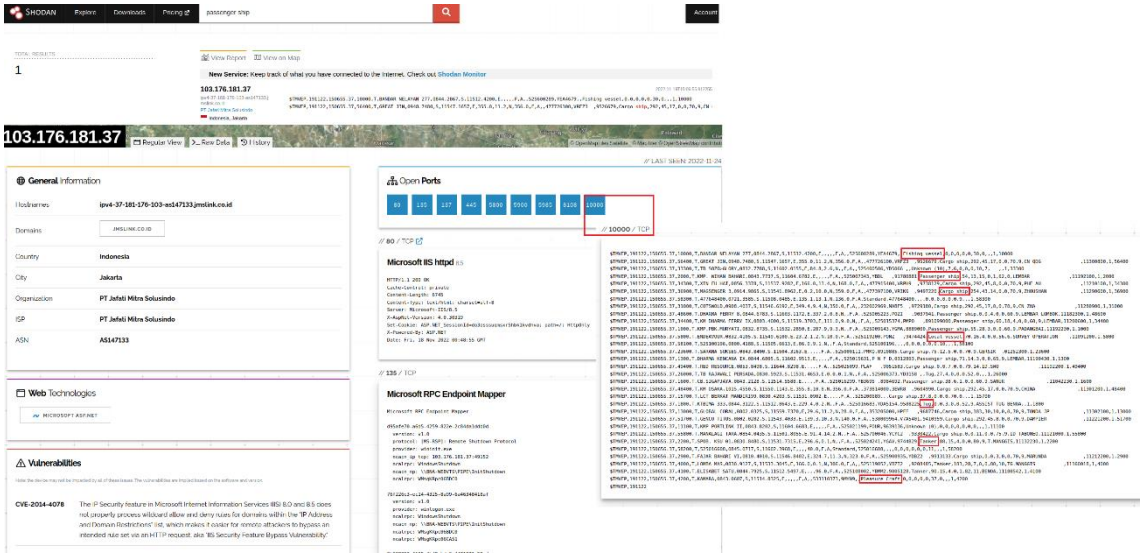
Στην συνέχεια θα ακολουθήσει φωτογραφικό υλικό με αναζητήσεις χρησιμοποιώντας λέξεις κλειδιά των συστημάτων αλλά και γενικά της ναυτιλίας όπως είναι Cobham vessel, AIS vessel, BWMS, passenger ship κ.α. για να δούμε γενικά τι αποτελέσματα εμφανίζει. Στις λεζάντες των εικόνων αναγράφεται η αντίστοιχη αναζήτηση. Ενδιαφέρουσες είναι οι αναζητήσεις «Vessel» μιας που εμφανίζει και πληροφορίες για Offshore Weather Prediction (πιθανόν σενάριο για Faking Weather Forecasts 2.2.3), «passenger ship» καθώς στην θύρα της 10000 φαίνονται να αναγράφονται και άλλα είδη πλοίων.



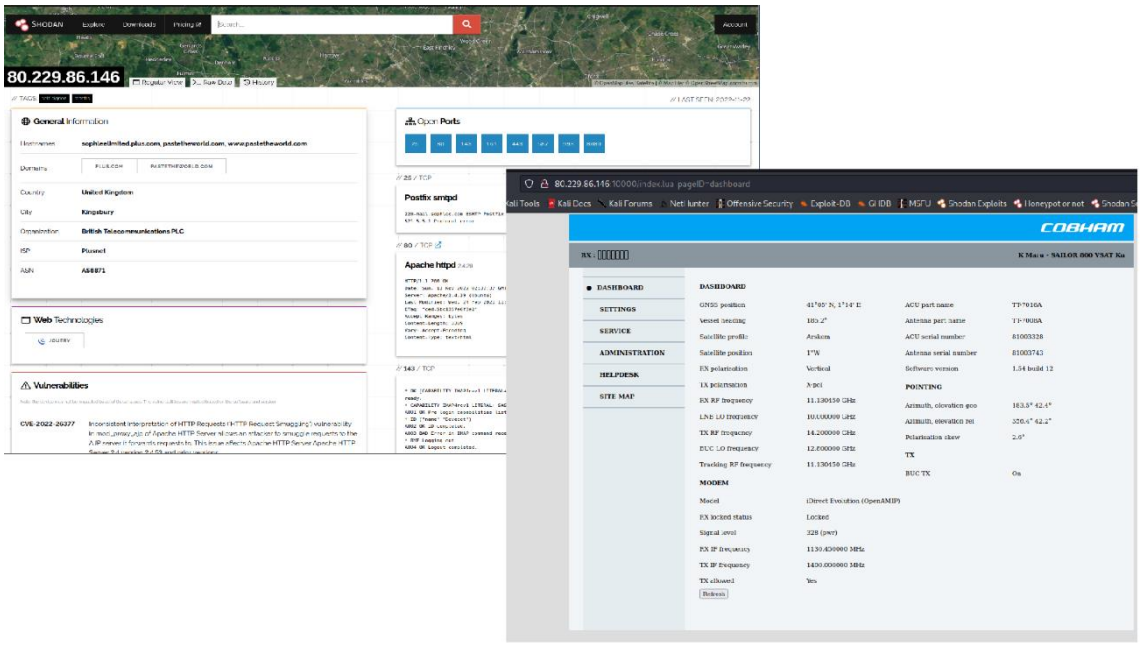
Εικόνα 73 – Fleet



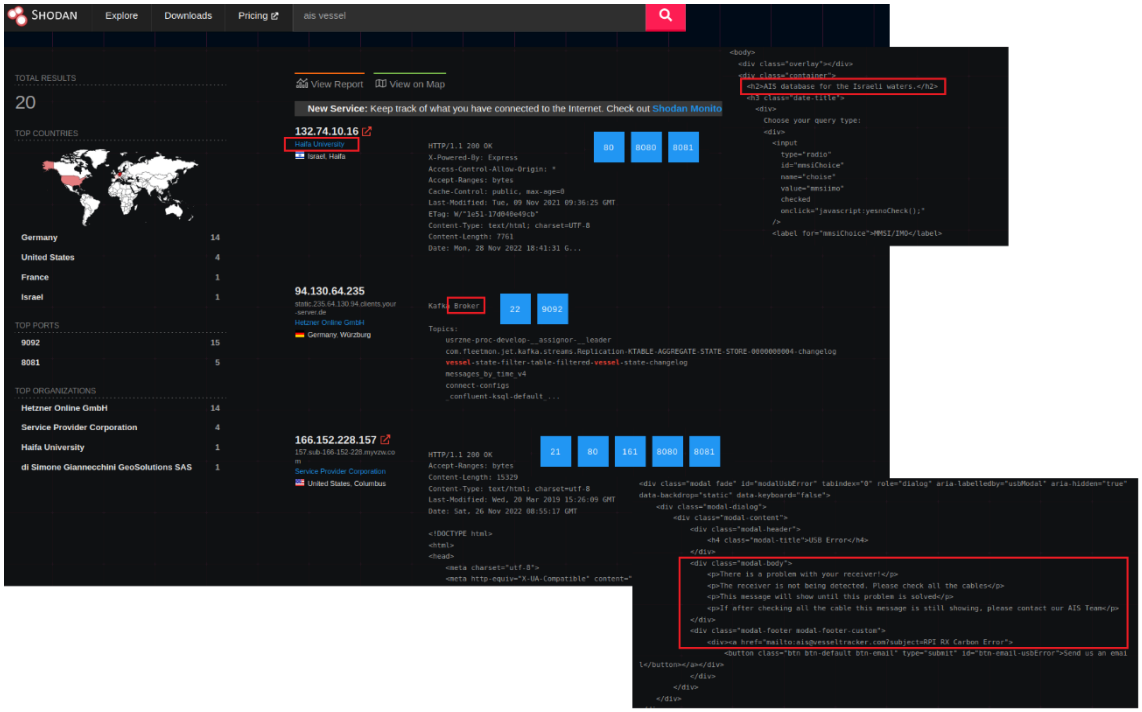
Εικόνα 74 - Vessel



Εικόνα 75 - Passenger ship

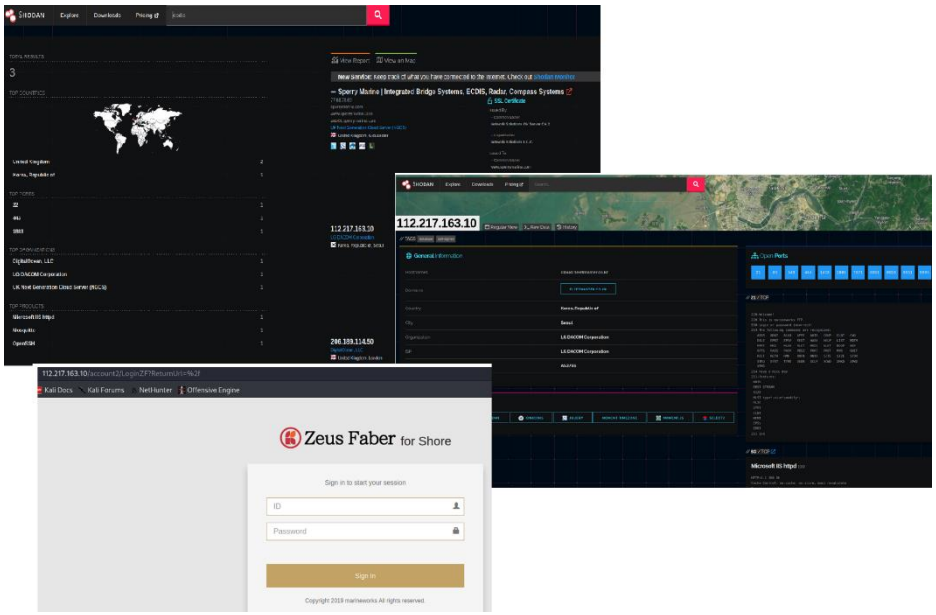


Εικόνα 76 - Cobham Vessel

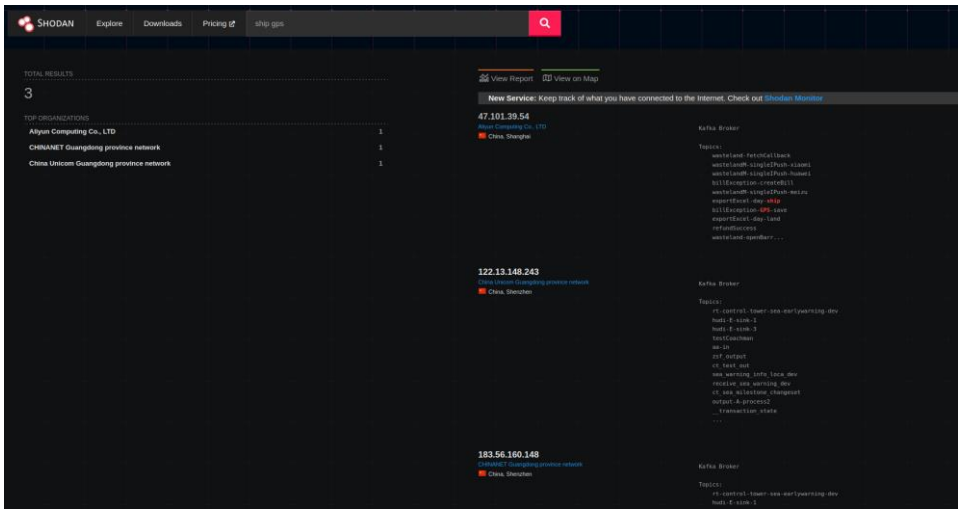


Εικόνα 77 – AIS Vessel

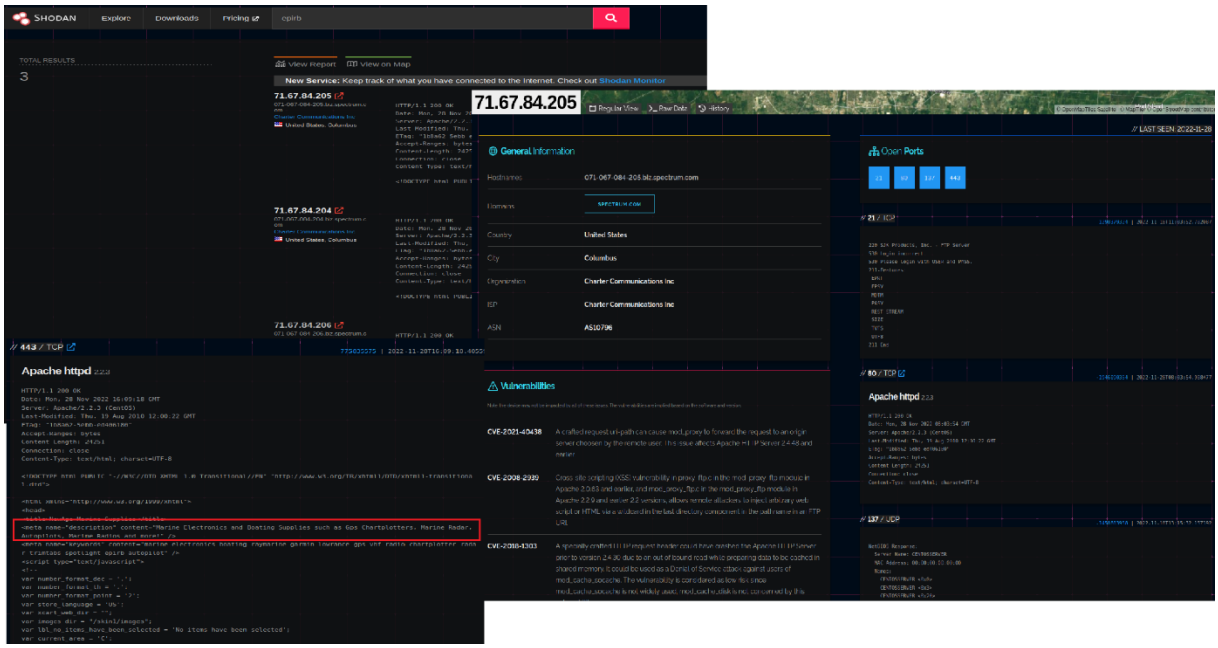
Με την παραπάνω αναζήτηση «AIS Vessel» τα πρώτα τρία αποτελέσματα ήταν διαφορετικά αλλά πιθανόν εξίσου σημαντικά. Το πρώτο αφορά ένα πανεπιστήμιο και το έφερε σαν αποτέλεσμα λόγω του «AIS Database for Israel Water», το δεύτερο αφορά Broker και το βρήκε λόγω «vessel state» και το τελευταίο ανέγραφε «There is a problem with the receiver… please contact AIS team».



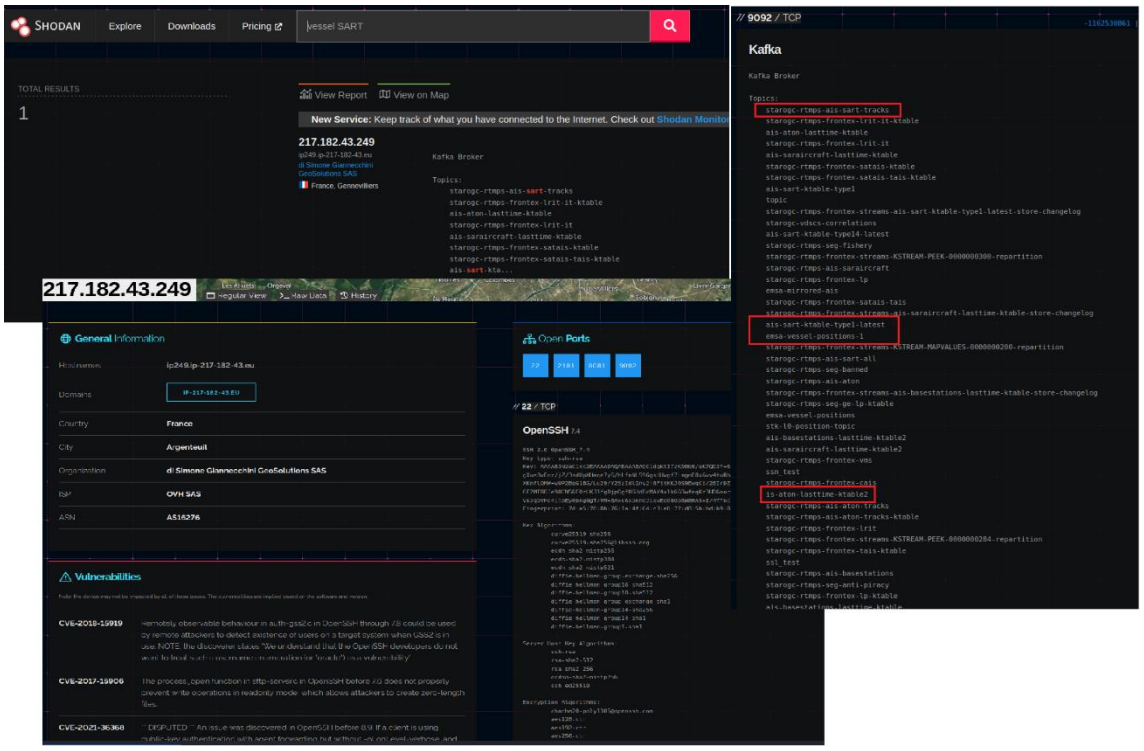
Εικόνα 78 – ECDIS



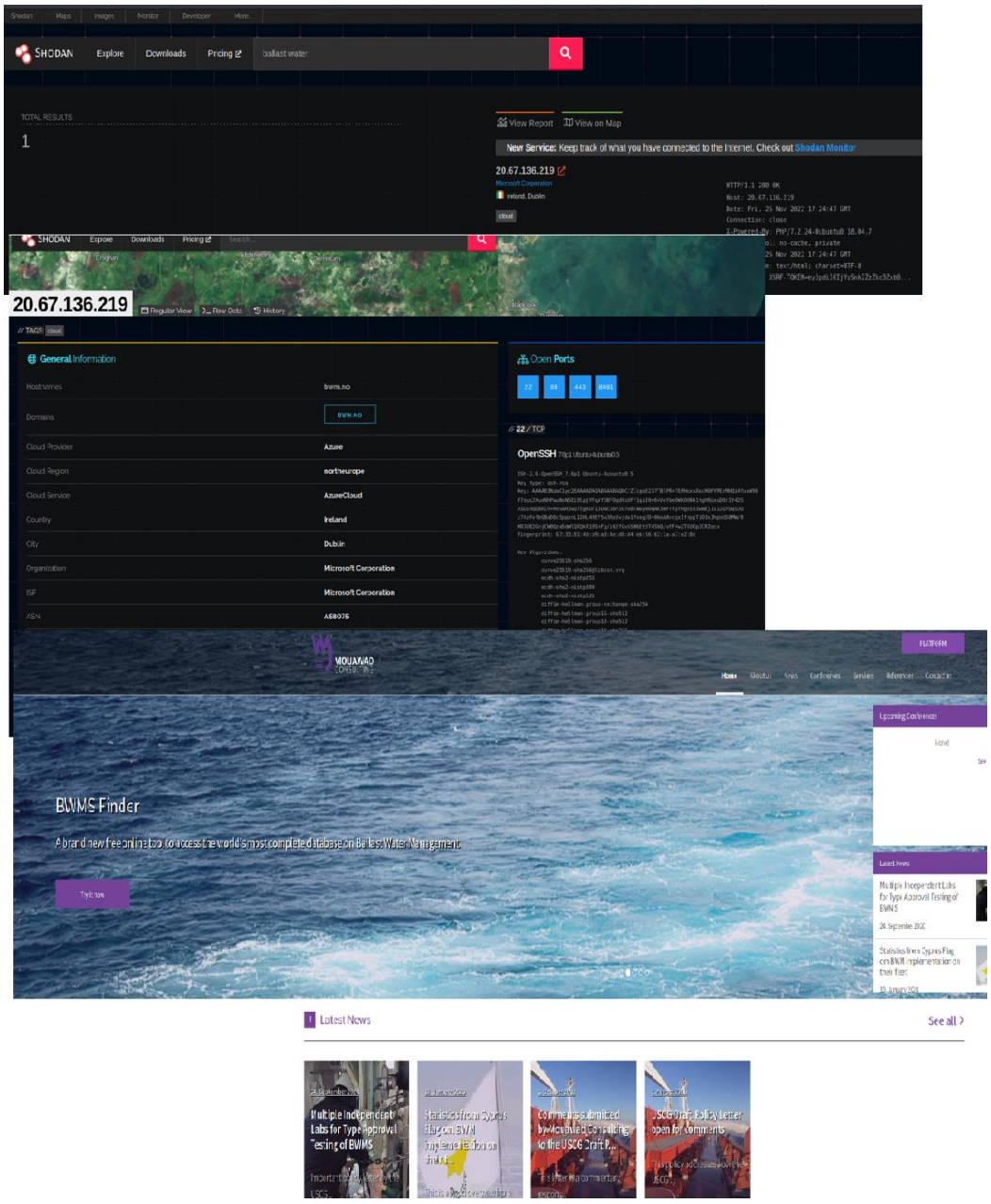
Εικόνα 79 - Ship GPS



Εικόνα 80 – EPIRB



Εικόνα 81 - Vessel SART



Εικόνα 82 - Ballast water

Κεφάλαιο 5: Συμπεράσματα

Ο σκοπός της παρούσας εργασίας ήταν να καταστήσει κατανοητό την ανάγκη ύπαρξης ασφαλείας σε ζητήματα κυβερνοχώρου στον τομέα της Ναυτιλιακής Βιομηχανίας. Η τεχνολογία έχει εισέλθει για τα καλά στην ναυτιλία, καθώς προσπαθεί να αξιοποιήσει όσον το δυνατό περισσότερα τεχνολογικά επιτεύγματα με σκοπό να διασφαλίσει την βελτιστοποίηση της λειτουργικής αποτελεσματικότητας. Όπως για παράδειγμα η άμεση επικοινωνία πλοίου - γραφείου αλλά και η χρήση δορυφορικών συστημάτων για την ψυχαγωγία του πληρώματος. Εκτός αυτών η δρομολόγηση καιρού, ο προγραμματισμός ταξιδιού, η κατανάλωση καυσίμου, ο έλεγχος εκπομπών και η προγνωστική συντήρηση είναι δημοφιλείς επιλογές για βελτιωμένη εμπορική απόδοση.

Ο αναγνώστης μέσα από την ανάλυση των συστημάτων των πλοίων και τον εντοπισμό των ευάλωτων σημείων τους καλείται να συνειδητοποιήσει την σπουδαιότητα της κυβερνοασφάλειας μιας που η απειλή είναι κάθε άλλο εκτός από πιθανή. Τα πλοία, οι πλατφόρμες, οι δορυφόροι και οι χερσαίες εγκαταστάσεις διασυνδέονται ολοένα και περισσότερο, εκθέτοντάς τα σε πληθώρα τεχνολογικών απειλών. Στην πραγματικότητα δεν υπάρχει τρόπος για το δίκτυο ενός πλοίου να «γνωρίσει» το επίπεδο ανθεκτικότητάς του στον κυβερνοχώρο. Όπως αποδεικνύεται και από τα περιστατικά που έχουν συμβεί, η εξάλειψη των επιθέσεων δεν είναι εφικτή αλλά ο μετριασμός τόσο αυτών όσο και του αντικτύπου τους είναι. Για αυτό είναι σημαντικό κάθε οργανισμός να έχει πραγματοποιήσει μία εκτίμηση κινδύνου προκειμένου να γνωρίσει το πιθανόν κόστος και να είναι όσο το δυνατόν πιο καλά προετοιμασμένος σε περίπτωση κυβερνοεπίθεσης.

Το Σύστημα Θαλάσσιων Μεταφορών είναι αρκετά σύνθετο με πολλά μέρη να εμπλέκονται και να χρειάζεται να συνεργαστούν και να επικοινωνούν μεταξύ τους. Οι ναυπηγοί και οι κατασκευαστές εξοπλισμού πλοίων πρέπει επίσης να κατανοούν τις απειλές και να εφαρμόζουν τα κατάλληλα μέτρα. Για την ασφαλή ναυσιπλοΐα, θα πρέπει να τηρούνται οι κανονισμοί κυβερνοασφάλειας που επιβάλλονται από τον IMO καθώς και οι οδηγίες των κυβερνήσεων. Είναι ανάγκη να αυξηθεί η ευαισθητοποίηση σχετικά με τις διάφορες απειλές που διατρέχουν τα συστήματα που χρησιμοποιούνται τόσο για τις επικοινωνίες αλλά κυριότερα τα λειτουργικά συστήματα που αφορούν την πρόωση του πλοίου αλλά και την πλοήγησή του.

Η πολυεπίπεδη προσέγγιση, η πρόσβαση με βάση την ανάγκη και την εξουσιοδότηση, οι περιμετρικές άμυνες όπως τα τείχη προστασίας και το ενημερωμένο λογισμικό μπορούν να εμποδίσουν σημαντικά την πρόσβαση ενός εισβολέα στα συστήματα ενός πλοίου, αποτρέποντας ταυτόχρονα την εξάπλωση κακόβουλου λογισμικού. Να μην ξεχνάμε όμως ότι η ναυτιλία είναι συνεχώς συνδεδεμένη στο διαδίκτυο όπως φαίνεται και από τα ευρήματα της πλατφόρμας αναζήτησης Shodan, γεγονός που καθιστά αναγκαία και την τμηματοποίηση των δικτύων και το διαχωρισμό των συστημάτων. Και φυσικά δεν πρέπει να υποβαθμίζεται ο ανθρώπινος παράγοντας. Η συνεχής εκπαίδευση και η ευαισθητοποίηση των ατόμων που βρίσκονται στην εταιρία αλλά και στο πλοίο είναι άκρως απαραίτητη.

Προσωπική επιδίωξη είναι αυτή η εργασία να αποτελέσει το κινητήριο έναυσμα για περαιτέρω δραστηριοποίηση επί της κυβερνοασφάλειας δεδομένου ότι η πρόοδος στον τομέα της πληροφορικής και της ναυτιλιακής βιομηχανίας εξελίσσεται διαρκώς και ανοίγει νέα άβατα «μονοπάτια». Για παράδειγμα, η τεχνητή νοημοσύνη ενσωματώνει ναυτιλιακά Logistics και τεχνολογία επικοινωνίας, η ρομποτική χρησιμοποιείται για χειρισμό περιουσιακών στοιχείων, επιθεώρηση, συντήρηση και ανάπτυξη αισθητήρων, τα cloud για την ανταλλαγή δεδομένων, η εικονική πραγματικότητα για εκπαίδευση, μηχανική και επιθεώρηση αλλά και drones για περιβαλλοντική παρακολούθηση, χαρτογράφηση, και για υπηρεσίες έκτακτης ανάγκης. (Mishra, 2022)

Μία ακόμη τεχνολογική τάση είναι η χρήση Blockchain, που έχει αναφερθεί για την χρήση του σε ασφάλιση εγγράφων, αποκλεισμού κλοπής προσωπικών δεδομένων, κρυπτογράφηση και αποτροπή μη εξουσιοδοτημένης πρόσβασης. Στη ναυτιλιακή βιομηχανία μπορεί να χρησιμοποιηθεί, μεταξύ άλλων, και για την παρακολούθηση της κίνησης των αγαθών σε όλα τα στάδια, για συμβόλαια και γενικά για μετάβαση στην ψηφιακή τεχνολογία και την αυτοματοποίηση της επεξεργασίας των εγγράφων. Αυτά θα εξοικονομήσουν χρόνο και θα μειώσουν το κόστος που

σχετίζεται με τον εκτελωνισμό και τη μεταφορά των εμπορευμάτων αλλά μπορεί να επιφέρουν απροσδόκητους κινδύνους (Prinston, 2022).

Καταλήγοντας, ενόσω αυξάνεται η αυτοματοποίηση, θα απαιτούνται μεγαλύτερες αποδόσεις για την υποστήριξη μικρότερου πληρώματος και την προστασία των συστημάτων καθώς αυξάνεται η κυκλοφορία δεδομένων που κινείται μεταξύ πλοίου και ακτής. Για παράδειγμα, με λιγότερη ανθρώπινη παρέμβαση, τα απρόσμενα προβλήματα μπορεί να χρειαστεί να αντιμετωπιστούν εξ αποστάσεως, καθιστώντας την ανθεκτικότητα του πλοίου στη σύνδεση της ξηράς πιο κρίσιμη από ποτέ. Με μηχανήματα, αισθητήρες, συστήματα και δίκτυα διασυνδεδεμένα και συνδεδεμένα στο Διαδίκτυο, οποιαδήποτε ευπάθεια στην ασφάλεια στον κυβερνοχώρο μπορεί να προκαλέσει μια σοβαρή ρωγμή στην θωράκιση ενός αυτόνομου πλοίου εάν δεν διαχειριστεί σωστά και έγκαιρα. Για το λόγο αυτό, είναι χρήσιμο να μελετηθούν και να αξιολογηθούν διαφορετικές αρχιτεκτονικές δικτύων, εστιάζοντας στις ιδιαιτερότητες της ναυτιλιακής βιομηχανίας και να προταθούν λύσεις στον κυβερνοχώρο λαμβάνοντας παράλληλα υπόψιν την έλλειψη σαφήνειας σχετικά με την ανάληψη ευθυνών σε περιπτώσεις κυβερνοεπίθεσης.

(Jo, Choi, You, Cha, & Lee, 2022) (McNally, 2022) (Bothur, Zheng, & Valli, 2022) (Co, 2022)

Βιβλιογραφία

12 Iacs Recommendations On Cyber Safety Mark Step Change In Delivery Of Cyber Resilient Ships. (2022, 10 06). Ανάκτηση από IACS: https://iacs.org.uk/news/12-iacs-recommendations-on-cyber-safety-mark-step-change-in-delivery-of-cyber-resilient-ships/

(2022, 10 04). Ανάκτηση από NIST: https://www.nist.gov/cybersecurity

(2022, 10 06). Ανάκτηση από BIMCO: https://www.bimco.org/about-us-and-our-members

(2022, 10 06). Ανάκτηση από CISA: https://www.cisa.gov/about-cisa

ABS. (2022, 10 06). Ανάκτηση από https://ww2.eagle.org/en.html

Advanced Polymer Coatings. (2022, 04 23). Ανάκτηση από https://www.adv-polymer.com/blog/maritime-cybersecurity#ch4

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022, 08 19). *Cybersecurity Challenges in the Maritime Sector*. Ανάκτηση από MDPI: https://www.mdpi.com/2673-8732/2/1/9/htm

Allen, J., Firch, J., & MBA. (2022, 11 14). *Social Engineering: What Is It And Why Is It Effective?* Ανάκτηση από PurpleSec: https://purplesec.us/learn/why-social-engineering-works/#Prevent

ANDERSSON, S., & LINSE, A. (2022, 08 14). *Investigation of the engine control room design, ergonomics, and function*. Ανάκτηση από Chalmers: https://odr.chalmers.se/bitstream/20.500.12380/301880/1/andersson_linse_investigation_of_the_engine_control_room_design_ergopnomics_and_function.pdf

Andrej Androjna, M. P. (2022, 06 16). *AIS Data Vulnerability Indicated by a Spoofing Case-Study*. Ανάκτηση από https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwicnuXfiav4AhWZlP0HHd7CAcc4ChAWegQIARAB&url=https%3A%2F%2Fwww.mdpi.com%2F2076-3417%2F11%2F11%2F5015%2Fpdf%3Fversion%3D1622447004&usg=AOvVaw0z2Xia8d6KKNTdaAaU5E5j

Anish. (2022, 08 18). *What is Ship Security Alert System (SSAS)?* Ανάκτηση από Marine Insight: https://www.marineinsight.com/marine-piracy-marine/what-is-ship-security-alert-system-ssas/

Area41. (2020, 08 29). Ανάκτηση από https://www.youtube.com/watch?v=GMWoS7v3qFo&ab_channel=DEFCONSwitzerland

Asket. (2022, 02 06). Ανάκτηση από https://www.asket.co.uk/post/2017/11/26/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-asketoperati

Auto-Maskin DCU 210E RP 210E and Marine Pro Observer App. (2022, 09 27). Ανάκτηση από CERT Coordination Center: https://www.kb.cert.org/vuls/id/176301

AUTO-MASKIN DCU 210E/RP-210E/MARINE PRO OBSERVER ANDROID APP INFORMATION DISCLOSURE. (2022, 09 27). Ανάκτηση από VulDb: https://vuldb.com/?id.125078

Averous, J. (2022, 10 24). *How Hardware Infrastructure Can Be Vulnerable to Hacking*. Ανάκτηση από The fourth revolution blog: https://thefourthrevolution.org/wordpress/archives/7249?doing_wp_cron=1666636397.4358489513397216796875

awake . (2021, 05 02). Ανάκτηση από https://awakesecurity.com/glossary/credential-theft/

Ballast Water Management - DNV. (2022, 08 10). Ανάκτηση από DNV: https://www.dnv.com/maritime/ballast-water-management/index.html

Ballast Water Management - IMO. (2022, 08 10). Ανάκτηση από IMO: https://www.imo.org/en/OurWork/Environment/Pages/BallastWaterManagement.aspx

BAPLIE. (2022, 08 09). Ανάκτηση από RBS: https://rbs-tops.com/glossary/baplie-bayplan-including-empties/

Baraniuk, C. (2022, 09 24). *How hackers are targeting the shipping industry*. Ανάκτηση από BBC: https://www.bbc.com/news/technology-40685821

Baumann, I. (2022, 06 05). *IMO and the GNSS*. Ανάκτηση από Inside GNSS: https://insidegnss.com/imo-and-the-gnss/

Bhattacharjee, S. (2022, 07 11). *Marine Radars and Their Use in the Shipping Industry*. Ανάκτηση από Marine Insight: https://www.marineinsight.com/marine-navigation/marine-radars-and-their-use-in-the-shipping-industry/

Bhattacharjee, S. (2022, 07 10). *What is Electronic Chart Display and Information System (ECDIS)?* Ανάκτηση από Marine Insight: https://www.marineinsight.com/marine-navigation/what-is-electronic-chart-display-and-information-system-ecdis/

BigThink. (2022, 06 26). Ανάκτηση από https://bigthink.com/strange-maps/circle-spoofing/

Board, U. N. (2022, 06 13). *GNSS Spoofing - A Technology Re/evolution*. Ανάκτηση από https://www.gps.gov/governance/advisory/meetings/2018-12/goward.pdf

Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2022, 07 24). *A novel cyber-risk assessment method for ship systems*. Ανάκτηση από ScienceDirect: https://www.sciencedirect.com/science/article/pii/S0925753520303052

Bothur, D., Zheng, G., & Valli, C. (2022, 11 30). *A critical analysis of security vulnerabilities and countermeasures in a smart ship system*. Ανάκτηση από Edith Cowan University: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1209&context=ism

Boyes, H., & Isbell, R. (2022, 10 06). *Code of Practice Cyber Security for Ships*. Ανάκτηση από The Institution of Engineering and Technology: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf

Brooke, L. (2022, 10 09). *Data Manipulation Attacks And How To Counter Them*. Ανάκτηση από US Cybersecurity: https://www.uscybersecurity.net/data-manipulation-attacks/

Buckbee, M. (2021, 05 02). *What is a Man-in-the-Middle Attack: Detection and Prevention Tips*. Ανάκτηση από varonis: https://www.varonis.com/blog/man-in-the-middle-attack/

Canadian Center for Cyber Security. (2021, 04 18). Ανάκτηση από https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

cargo plan stowage plan. (2022, 08 09). Ανάκτηση από wartsila: https://www.wartsila.com/encyclopedia/term/cargo-plan-stowage-plan

Carrier sense multiple access with collision detection. (2022, 08 08). Ανάκτηση από wikipedia: https://en.wikipedia.org/wiki/Carrier-sense_multiple_access_with_collision_detection

CGCYBER. (2022, 10 06). Ανάκτηση από Unites States Coast Guard: https://www.dco.uscg.mil/Our-Organization/CGCYBER/

Champers, S. (2022, 09 24). *Ship's satellite communication system hacked with ease*. Ανάκτηση από Splash247: https://splash247.com/ships-satellite-communication-system-hacked-ease/

Chroni, E. (2021, 04 18). *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020 – 2025.* Athens: Ministry of Digital Goverment Hellenic Republiv. Ανάκτηση από https://mindigital.gr/wp-content/uploads/2020/12/ΕΘΝΙΚΗ-ΣΤΡΑΤΗΓΙΚΗ-ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ-2020-2025.pdf

Cimpanu, C. (2022, 09 27). *Ships infected with ransomware, USB malware, worms*. Ανάκτηση από ZD Net: https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms/

cisco. (2021, 04 18). Ανάκτηση από https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~types-of-cyber-attacks

CloudFlare. (2021, 04 22). Ανάκτηση από https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

CNBlogs. (2022, 05 02). Ανάκτηση από https://www.cnblogs.com/pengdonglin137/p/5020143.html

Co, C. &. (2022, 11 30). *The impact of technological change on thes hipping industry*. Ανάκτηση από Imarest: https://www.imarest.org/policy-news/thought-leadership/1010-technology-in-shipping/file

Collaborate with Us: Government Organizations. (2022, 10 04). Ανάκτηση από NIST: https://www.nccoe.nist.gov/get-involved/collaborate-us-government-organizations

Comma-separated values. (2022, 08 09). Ανάκτηση από wikipedia: https://en.wikipedia.org/wiki/Comma-separated_values

COMMITTEE, N. C. (2022, 07 10). *CYBER SECURITY NEWS LETTER*. Ανάκτηση από https://www.sfmx.org/wp-content/uploads/2017/03/Cyber-Security-Newsletter-2014-1.pdf

computer hope. (2021, 05 03). Ανάκτηση από https://www.computerhope.com/jargon/d/datamani.htm

contrast security. (2021, 05 03). Ανάκτηση από https://www.contrastsecurity.com/knowledge-hub/glossary/application-attacks

Cyber Law. (2022, 07 24). Ανάκτηση από https://cyberlaw.ccdcoe.org/wiki/Operation_Orchard/Outside_the_Box_(2007)

Cyber Safety And Security. (2022, 11 13). Ανάκτηση από Bureau Veritas: https://www.bureauveritas.gr/digital/maritime-industry-40/cyber-safety-security

Cyber Security International Legislation. (2022, 05 02). Ανάκτηση από https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj3pr_4tMH3AhWD7rsIHcQ5DQkQFnoECAgQAQ&url=https%3A%2F%2Fvm.ee%2Fsites%2Fdefault%2Ffiles%2Fcontent-editors%2Fweb-static%2F017%2FCyber_Security_Threat_from_the_Net.ppt&usg=AOvVaw27tuKt

Cybersecurity. (2022, 11 13). Ανάκτηση από ICC: https://iccwbo.org/global-issues-trends/digital-growth/cybersecurity/

Cybersecurity in the Maritime Sector: ENISA Releases New Guidelines for Navigating Cyber Risk. (2022, 10 06). Ανάκτηση από ENISA: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-maritime-sector-enisa-releases-new-guidelines-for-navigating-cyber-risk

Cyclic redundancy check. (2022, 08 08). Ανάκτηση από wikipedia: https://en.wikipedia.org/wiki/Cyclic_redundancy_check

Cyclic redundancy check. (2022, 12 07). Ανάκτηση από Wikipedia: https://en.wikipedia.org/wiki/Cyclic_redundancy_check

Dead reckoning. (2022, 12 07). Ανάκτηση από Wikipedia: https://en.wikipedia.org/wiki/Dead_reckoning

Defcon28. (2022, 02 03). Ανάκτηση από https://www.youtube.com/watch?v=0yoMhWURaCI&ab_channel=HackTheSea

Degnarain, N. (2022, 09 18). *Could Oil Ship Wakashio Been Hacked Before Mauritius Spill?* Ανάκτηση από Forbes: https://www.forbes.com/sites/nishandegnarain/2020/10/26/could-mol-chartered-mauritius-oil-spill-ship-wakashio-have-been-hacked/?sh=5d10e5507fbb

digicert. (2021, 05 15). Ανάκτηση από https://www.websecurity.digicert.com/security-topics/difference-between-virus-worm-and-trojan-horse

Digital Yacht. (2022, 07 11). Ανάκτηση από https://digitalyacht.net/2014/04/03/cpa-and-tcpa-alarms-explained/

Digitizing Engine Control Systems for Operational Efficiency. (2022, 08 14). Ανάκτηση από MOXA: https://www.moxa.com/en/case-studies/digitizing-engine-control-systems-for-operational-efficiency

Dinesh Sathyamoorthy, S. S. (2022, 06 18). *Evaluating the Effect of Global Positioning System (GPS) Satellite Clock Error via GPS Simulation*. Ανάκτηση από https://iopscience.iop.org/article/10.1088/1755-1315/37/1/012013/pdf

DNV. (2021, 04 30). Ανάκτηση από https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/index.html

DNV. (2021, 04 30). Ανάκτηση από https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/ism-guidance.html

ELECTRICALFUNABOLG. (2022, 06 18). Ανάκτηση από https://electricalfundablog.com/global-positioning-system-gps/

E-nautilia. (2022, 03 13). Ανάκτηση από https://e-nautilia.gr/sustimata-eoikoinonias-pou-xrisimopoiountai-sto-xoro-tis-nautilias/

enisa. (2021, 04 22). Ανάκτηση από https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets

Enisa. (2021, 05 02). Ανάκτηση από https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing

(2021). *ENISA Threat Landscape - The year in review.* ENISA.

eset. (2021, 04 24). Ανάκτηση από https://www.eset.com/gr/ransomware/

Estimated Position. (2022, 12 07). Ανάκτηση από TDGil: https://tdgil.com/estimated-position/

europa.eu. (2021, 04 18). Ανάκτηση από https://europa.eu/european-union/about-eu/agencies/enisa_el

European Commision. (2021, 04 29). Ανάκτηση από https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

European Commission. (2021, 04 29). Ανάκτηση από https://digital-strategy.ec.europa.eu/en/policies/nis-directive

European Commission. (2021, 04 29). Ανάκτηση από https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

European Commission. (2021, 04 29). Ανάκτηση από https://ec.europa.eu/jrc/en/science-update/european-cybersecurity-taxonomy

Firch, J., & MBA. (2022, 11 14). *9 Common Types Of Malware (And How To Prevent Them)*. Ανάκτηση από PurpleSec: https://purplesec.us/common-malware-types/#Prevent

First EU-report on Maritime Cyber Security. (2022, 10 06). Ανάκτηση από ENISA: https://www.enisa.europa.eu/news/enisa-news/first-eu-report-on-maritime-cyber-security

France24. (2022, 02 06). Ανάκτηση από https://www.france24.com/en/live-news/20220203-european-oil-port-terminals-hit-by-cyberattack

Gard. (2022, 04 23). Ανάκτηση από https://www.gard.no/Content/25634225/Cyber%20Security_Presentation%20(ID%2014 18279).pdf

Garmin. (2022, 07 11). Ανάκτηση από https://www8.garmin.com/manuals/webhelp/gpsmap7400-7600/EL-GR/GUID-C4C5ACFC-BA5A-485C-8E51-179A71C0015A.html

GeoTab. (2022, 06 18). Ανάκτηση από https://www.geotab.com/blog/what-is-gps/

Ghamdi, M. S. (2022, 07 10). *Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS)*. Ανάκτηση από https://www.mdpi.com/2077-1312/7/10/350?type=check_update&version=2

Gill, J. (2022, 11 23). *Find Webcams, Databases, Boats In The Sea Using Shodan*. Ανάκτηση από Information Security Newspaper:

https://www.securitynewspaper.com/2018/11/27/find-webcams-databases-boats-in-the-sea-using-shodan/

Global Fishing Watch. (2022, 05 07). Ανάκτηση από https://globalfishingwatch.org/data/ais-for-safety-and-tracking-a-brief-history/

Global, O. T. (2022, 06 18). *LinkedIn*. Ανάκτηση από https://www.linkedin.com/pulse/maritime-industry-over-reliant-gps-ocean-time-marine-global?trk=portfolio_article-card_title

GNSS Market Report. (2022, 06 05). Ανάκτηση από EUSPA: https://www.euspa.europa.eu/sites/default/files/Maritime_0.pdf

Gonidec, Y. L. (2022, 11 16). *Cyber Risk And Ships: Practical Issues Following Bimco Guideline*. Ανάκτηση από IUMI: https://iumi.com/images/documents/genua-2016-program/7_yohan_le_gonidec_1474365158.pdf

GPS gov. (2022, 06 18). Ανάκτηση από https://www.gps.gov/applications/marine/

gpsd. (2022, 05 15). Ανάκτηση από https://gpsd.gitlab.io/gpsd/AIVDM.html

Grind GIS. (2022, 06 18). Ανάκτηση από https://grindgis.com/gps/application-of-gps-in-marine

Gronholt-Pedersen, J. (2022, 10 04). *Maersk says global IT breakdown caused by cyber attack*. Ανάκτηση από Reuters: https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19I1NO

Guard, U. S. (2022, 08 13). *Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels*. Ανάκτηση από United States Coast Guard: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf

guru99. (2021, 04 24). Ανάκτηση από https://www.guru99.com/potential-security-threats-to-your-computer-systems.html

Η CMA CGM, το τελευταίο θύμα κυβερνοεπίθεσης στη ναυτιλία . (2022, 09 22). Ανάκτηση από Ναυτικά Χρονικά: https://www.naftikachronika.gr/2020/09/28/h-cma-cgm-to-teleftaio-thyma-kyvernoepithesis-sti-naftilia/

Hamilton, M. K. (2022, 10 09). *4 Tips for Cruise Ship Cybersecurity*. Ανάκτηση από Critical Insight: https://www.criticalinsight.com/resources/news/article/4-tips-for-cruise-ship-cybersecurity

HEXAGON. (2022, 06 13). Ανάκτηση από https://en.calameo.com/read/00191579602f9b13b088e?authid=9leJ1niQkK75

HHVFerry. (2022, 07 30). Ανάκτηση από https://www.hhvferry.com/zenobia.html

Hoegh Osaka ship was 'unstable' when it left Southampton port. (2022, 07 30). Ανάκτηση από BBC: https://www.bbc.com/news/uk-england-hampshire-35823182

how to plan cargo containers stowage on container ship. (2022, 08 09). Ανάκτηση από marine nsight: https://www.marineinsight.com/guidelines/how-to-plan-cargo-containers-stowage-on-container-ship/

Hub, P. (2020, 12 13). Cyber Security.

Human Machine Interface Systems for Marine Applications. (2022, 08 17). Ανάκτηση από eao: https://www.mouser.com/pdfDocs/eao-ta-hmi-marine-applications-en.pdf

Humphrey, C. (. (2022, 11 14). *How to Steal a Ship - Part 2*. Ανάκτηση από The Maritime Executive: https://maritime-executive.com/editorials/how-to-steal-a-ship-part-2

IACS adopts two new Unified Requirements on cyber resilience of Ships. (2022, 10 06). Ανάκτηση από Marine Regulations: https://www.marineregulations.news/iacs-adopts-two-new-unified-requirements-urs-on-cyber-resilience-of-ships/

IAPH launches Cybersecurity Guidelines for Ports and Port Facilities as part of industry call to action to digitalize the maritime transport chain. (2022, 06 10). Ανάκτηση από World Port Sustainability Program: https://sustainableworldports.org/iaph-launches-cybersecurity-guidelines-for-ports-and-port-facilities-as-part-of-industry-call-to-action-to-digitalize-the-maritime-transport-chain/

ICC Cyber Security . (2022, 11 13). Ανάκτηση από ICC: http://www2.hgk.hr/icc/datoteke/ICC-Cyber-Security-Guide-for-Business.pdf

IGuru. (2022, 05 02). Ανάκτηση από https://iguru.gr/national-intelligence-service-nis-cert/

IHS Markit | 2018 Maritime Cyber Security Results. (2021, 05 02). Ανάκτηση από https://www.bimco.org/news/priority-news/20180924-cyber-security-survey

Ilcev, D. S. (2022, 06 12). *Architecture of the global navigation satellite system for maritime applications*. Ανάκτηση από https://core.ac.uk/download/pdf/295538331.pdf

IMO. (2021, 04 30). Ανάκτηση από https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

IMO. (2022, 04 22). Ανάκτηση από https://www.imo.org/en/KnowledgeCentre/ConferencesMeetings/Pages/SOLAS.aspx

imperva. (2021, 04 20). Ανάκτηση από https://www.imperva.com/learn/application-security/phishing-attack-scam/

imperva. (2021, 05 03). Ανάκτηση από https://www.imperva.com/learn/ddos/ddos-attacks/

Inductive Automation. (2022, 08 28). Ανάκτηση από https://www.inductiveautomation.com/resources/article/what-is-hmi

Insider. (2022, 06 13). Ανάκτηση από https://www.businessinsider.com/gnss-hacking-spoofing-jamming-russians-screwing-with-gps-2019-4

insurance quality. (2021, 04 17). Ανάκτηση από iqbrokers: https://iqbrokers.gr/υπηρεσίες-cyber-security-τι-είναι-η-κυβερνοασφά/

International Labour Conference. (2022, 04 23). Ανάκτηση από https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---normes/documents/normativeinstrument/wcms_090250.pdf

International Maritime Bureau. (2022, 11 13). Ανάκτηση από ICC: https://www.icc-ccs.org/icc/imb

International Maritime Organization - MSC-FAL.1/Circ.3 "Guidelines On Maritime Cyber Risk Management". (2021, 04 30). Ανάκτηση από https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

International Reference Guideline For The Implementation Of Transport EDI Messages. (2022, 08 09). Ανάκτηση από ITIGG: https://www.transnetportterminals.net/About/EDI%20Documents/COPARN_D95B.pdf

Intertanko. (2022, 06 15). Ανάκτηση από https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf

investopedia. (2021, 04 24). Ανάκτηση από https://www.investopedia.com/terms/c/cryptojacking.asp

Investopedia. (2021, 04 22). Ανάκτηση από https://www.investopedia.com/terms/i/identitytheft.asp

Iran Telecommunication Research Center - Cyber Crime Legislation. (2022, 05 02). Ανάκτηση από https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/CybersecurityASPCOE/cybersecurity/Tafazzoli-cybercrime%20legislations.pdf

Iran's secret cyber files on how cargo ships and petrol stations could be attacked. (2022, 07 30). Ανάκτηση από IFMAT: https://www.ifmat.org/07/27/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked/

Isalos,net. (2020, 08 29). Ανάκτηση από https://www.isalos.net/2019/11/cyber-risk-sti-naftilia-pragmatikos-kindynos-i-enas-akoma-mythos/

Isalos.net. (2022, 04 23). Ανάκτηση από https://www.isalos.net/2019/11/m-servos-ta-ploia-metatrepontai-stadiaka-se-plota-diktya-ypologiston/

ISO/IEC 27001 - Information Security Management. (2021, 04 30). Ανάκτηση από https://www.iso.org/standard/73906.html

IT News. (2022, 02 05). Ανάκτηση από https://www.itnews.com.au/news/shipbuilder-austal-was-hacked-with-stolen-creds-sold-on-dark-web-546165

ITU. (2022, 05 02). Ανάκτηση από https://www.itu.int/en/ITU-D/Cybersecurity/Pages/legislation.aspx

Jo, Y., Choi, O., You, J., Cha, Y., & Lee, D. H. (2022, 07 30). *Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework*. Ανάκτηση από MDPI: https://www.mdpi.com/1424-8220/22/5/1860

Junior, W. C., Moraes, C. C., Albuquerque, C. E., Machado, R. C., & Sá, A. O. (2022, 07 24). *A Triggering Mechanism for Cyber-Attacks in Naval Sensors and Systems*. Ανάκτηση από National Center for Biotechnology Information: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8124306/pdf/sensors-21-03195.pdf

Kalfigkopoulos, N. (2022, 11 23). *Why the maritime industry must get on board with the NIS Directive*. Ανάκτηση από PWC: https://pwc.blogs.com/cyber_security_updates/2018/12/why-the-maritime-industry-must-get-on-board-with-the-nis-directive.html

Kapalidis, C. (2022, 09 22). *4 Cases of Cyber Security Failures in Shipping History*. Ανάκτηση από Linkedin: https://www.linkedin.com/pulse/4-cases-cyber-security-failures-shipping-history-chronis-kapalidis

KaranC. (2022, 08 18). *How Ship Security Reporting System (SSRS) helps to Improve Maritime Security?* Ανάκτηση από Marine Insight: https://www.marineinsight.com/marine-piracy-marine/how-ship-security-reporting-system-ssrs-helps-to-improve-maritime-security/

kaspersky. (2021, 04 22). Ανάκτηση από https://www.kaspersky.com/resource-center/definitions/data-breach

kaspersky. (2021, 05 03). Ανάκτηση από https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

Kessler, G. (2022, 09 14). *Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity*. Ανάκτηση από TransNav: https://www.transnav.eu/Article2_Protected_AIS:_A_Demonstration_of_Capability_Scheme_to_Provide_Authentication_and_Message_Integrity_Kessler,54,1002.html

Kessler, G. (2022, 08 08). *The CAN Bus in the Maritime Environment – Technical Overview and Cybersecurity Vulnerabilities*. Ανάκτηση από TransNav: https://www.transnav.eu/Article_The_CAN_Bus_in_the_Maritime_Environment_%e2%80%93_Technical_Overview_and_Cybersecurity_Vulnerabilities_Kessler,59,1145.html

Kessler, G. C., & Zorri, D. M. (2022, 10 03). *Cross Domain IW Threats to SOF Maritime Missions: Implications for U.S. SOF*. Ανάκτηση από Joint Special Operations University: https://www.hsdl.org/?view&did=857850

Krile, S., Kezić, D., & Dimc, F. (2022, 11 16). *NMEA Communication Standard for Shipboard Data Architecture*. Ανάκτηση από https://hrcak.srce.hr/file/162159

lawspot. (2021, 04 29). Ανάκτηση από https://www.lawspot.gr/nomika-nea/kyvernoasfaleia-stin-eyropaiki-enosi-hrisimes-plirofories-me-aformi-ti-nea-praxi-gia-tin

leaf. (2021, 04 28). Ανάκτηση από https://leaf-it.com/10-ways-prevent-cyber-attacks/

Leyden, J. (2022, 08 08). *Container ship loading plans are 'easily hackable'*. Ανάκτηση από The Register: https://www.theregister.com/2017/11/20/container_ship_loading_software_mischief/

Lloyd's Register. (2021, 04 30). Ανάκτηση από https://www.lr.org/en/cyber-safe-for-marine/

Lloyd's Register. (2022, 04 23). Ανάκτηση από Cyber-enabled ships - ShipRight procedure: https://www.lr.org/en/cyber-safe-for-marine/

Lloyd's Register. (2022, 04 23). Ανάκτηση από Cyber-enabled ships - Guidance Document: https://www.lr.org/en/cyber-safe-for-marine/

Lund, M. H. (2022, 05 01). *An Attack on an Integrated Navigation System.* Ανάκτηση από http://www.mass-lund.no/publications/Necesse.pdf

Mallam, S. C., & Lundh, M. (2022, 08 14). *Ship Engine Control Room Design: Analysis of Current Human Factors & Ergonomics Regulations & Future Directions*. Ανάκτηση από Researchgate: https://www.researchgate.net/publication/273296895_Ship_Engine_Control_Room_Design

Man, Y., Lundh, M., & MacKinnon, S. N. (2022, 08 17). *Managing unruly technologies in the engine control room: from problem patching to an architectural thinking and standardization*. Ανάκτηση από WMU Journal of Maritime Affairs: https://link.springer.com/content/pdf/10.1007/s13437-018-0159-y.pdf

Manuals Lib. (2022, 08 10). Ανάκτηση από https://www.manualslib.com/manual/2505300/Elite-Seascape-80.html?page=42

Marine Digital. (2022, 05 01). Ανάκτηση από https://marine-digital.com/article_21types_of_navigation_equipment

marine insight. (2021, 04 30). Ανάκτηση από https://www.marineinsight.com/marine-navigation/what-is-integrated-bridge-system-ibs-on-ships/

Marine Insight. (2022, 05 01). Ανάκτηση από https://www.marineinsight.com/marine-navigation/what-is-bridge-navigational-watch-alarm-system-bnwas/

Maritime Cyber Readiness Branch. (2022, 10 06). Ανάκτηση από United States Coast Guard: https://www.dco.uscg.mil/Our-Organization/CGCYBER/Maritime-Cyber-Readiness-Branch/

Maritime Industry 4.0. (2022, 11 13). Ανάκτηση από Bureau Veritas: https://www.bureauveritas.gr/maritime-industry-40

Maritime Modal Sector Coordinating Council Charter . (2022, 10 06). Ανάκτηση από CISA: https://www.cisa.gov/sites/default/files/publications/maritime_scc_charter_2019_4.26.19.pdf

McNally, M. (2022, 08 09). *Cybersecurity for the Increasingly Connected Ship*. Ανάκτηση από The maritime executive: https://www.maritime-executive.com/editorials/cybersecurity-for-the-increasingly-connected-ship

MD5 Hash Generator. (2022, 12 07). Ανάκτηση από Dans Tools: https://www.md5hashgenerator.com/

MDPI. (2022, 04 23). Ανάκτηση από Towards a Cyber-Physical Range for the Integrated Navigation System (INS).: https://www.mdpi.com/2077-1312/10/1/107

Mednikarov, B., Tsonev, Y., & Lazarov, A. (2022, 07 10). *Analysis of Cybersecurity Issues in the Maritime Industry*. Ανάκτηση από https://isij.eu/article/analysis-cybersecurity-issues-maritime-industry

Microsoft SMB Protocol and CIFS Protocol Overview. (2022, 12 07). Ανάκτηση από Microsoft: https://learn.microsoft.com/en-us/windows/win32/fileio/microsoft-smb-protocol-and-cifs-protocol-overview

Mishra, B. (2022, 11 30). *Emerging Technology Trends in Shipping and Maritime Industry*. Ανάκτηση από SeaNews: https://seanews.co.uk/shipping-news/emerging-technology-trends-in-shipping-and-maritime-industry/

MIT Technology Review. (2022, 06 26). Ανάκτηση από https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/

Modius, S. (2022, 09 24). *Quora*. Ανάκτηση από How many generators does it take to power a ship?: https://www.quora.com/How-many-generators-does-it-take-to-power-a-ship

MonoNews. (2022, 02 05). Ανάκτηση από https://www.mononews.gr/business/shipping/kivernoepithesi-tin-imera-tou-halloween-se-ellinikes-naftiliakes-eteries-epesan-ta-sistimata-

epikinonias?fbclid=IwAR3AFs5G3ZCjwXJQ-Uj5ZXIxfOV4lewPJJzOSF6U1qQutCNt1-qXHVSduUc

Morse, J. (2022, 11 23). *Remotely hacking ships shouldn't be this easy, and yet*. Ανάκτηση από Mashable: https://mashable.com/article/hacking-boats-is-fun-and-easy

Munro, K. (2022, 09 23). *Container theft, the legal system and poor maritime security*. Ανάκτηση από Pen Test Partners: https://www.pentestpartners.com/security-blog/container-theft-the-legal-system-and-poor-maritime-security/

Munro, K. (2022, 11 24). *Hacking vessel satcoms*. Ανάκτηση από Maritime Security Review: http://www.marsecreview.com/2017/10/hacking-vessel-satcoms/

Munro, K. (2022, 11 26). *Hacking, tracking, stealing & sinking ships*. Ανάκτηση από Pen Test Partners: https://static1.squarespace.com/static/57a8878837c58153c1897c2c/t/5aea9a516d2a733ad7bfa487/1525324384558/10KenMunro_Ham18.pdfhttps://static1.squarespace.com/static/57a8878837c58153c1897c2c/t/5aea9a516d2a733ad7bfa487/1525324384558/10KenMunro_Ham18.pdf

Munro, K. (2022, 02 02). *Hacking, tracking, stealing and sinking ships*. Ανάκτηση από Pen Test Partners: https://www.pentestpartners.com/security-blog/hacking-tracking-stealing-and-sinking-ships/

Munro, K. (2022, 08 09). *Making prawn espressos, or hacking ships by deciphering BAPLIE EDIFACT messaging*. Ανάκτηση από Pen Test Partners: https://www.pentestpartners.com/security-blog/making-prawn-espressos-or-hacking-ships-by-deciphering-baplie-edifact-messaging/

Munro, K. (2022, 02 02). *OSINT from ship satcoms*. Ανάκτηση από Pen Test Partners: https://www.pentestpartners.com/security-blog/osint-from-ship-satcoms/

Munro, K. (2022, 10 09). *Satellite communications equipment security*. Ανάκτηση από Pen Test Partners: https://www.pentestpartners.com/security-blog/satellite-communications-equipment-security/

Munro, K. (2022, 08 09). *Sinking bulk carrier ships by hacking HSMS*. Ανάκτηση από Pen Test Partners: https://www.pentestpartners.com/security-blog/sinking-bulk-carrier-ships-by-hacking-hsms/

Munro, K. (2022, 08 09). *Sinking container ships by hacking load plan software*. Ανάκτηση από Pen Test Partners: https://www.pentestpartners.com/security-blog/sinking-container-ships-by-hacking-load-plan-software/

Munro, K. (2022, 10 09). *Tactical Advice for Maritime Cyber Security – Top 10*. Ανάκτηση από Pen Test Partners: https://www.pentestpartners.com/security-blog/tactical-advice-for-maritime-cyber-security-top-10/

Munro, K. (2022, 11 23). *Tracking & hacking ships with Shodan & AIS*. Ανάκτηση από Pen Test Partners: https://www.pentestpartners.com/security-blog/tracking-hacking-ships-with-shodan-ais/

Naval Dome exposes vessel vulnerabilities to cyber attack. (2022, 08 03). Ανάκτηση από SeaTrade Maritime News: https://www.seatrade-maritime.com/asia/naval-dome-exposes-vessel-vulnerabilities-cyber-attack

Navipedia. (2022, 05 21). Ανάκτηση από https://gssc.esa.int/navipedia/index.php/AIS-VTS

NDTV. (2022, 05 02). Ανάκτηση από https://www.ndtv.com/india-news/kerala-boat-hit-and-run-cargo-ship-sailor-arrested-470800

Network, M. N. (2022, 09 22). *Real Life Incident: Ships Wedged Together After Collision*. Ανάκτηση από Marine Insight: https://www.marineinsight.com/case-studies/real-life-incident-ships-wedged-together-after-collision/

Newman, D. A. (2020, 07 30). *The Zenobia Shipwreck*. Ανάκτηση από Atlas Obscura: https://www.atlasobscura.com/places/the-zenobia-shipwreck-larnaca-cyprus

Nicaise, V. (2022, 02 06). *Cybermarétique: a short history of cyberattacks against ports*. Ανάκτηση από Stormshield: https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/

NIST. (2022, 08 28). Ανάκτηση από https://csrc.nist.gov/glossary/term/human_machine_interface

NIST Framework for Improving Critical Infrastructure Cybersecurity. (2021, 04 30). Ανάκτηση από https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

OAS - International legal frameworks for combating cybercrime: the UNODC perspective. (2022, 05 02). Ανάκτηση από https://www.oas.org/juridico/PDFs/cyb9_unodc_Dec16_v1.pdf

OCCUPYTHEWEB. (2022, 11 26). *How to Find Vulnerable Targets Using Shodan—The World's Most Dangerous Search Engine*. Ανάκτηση από Null bite: https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerable-targets-using-shodan-the-worlds-most-dangerous-search-engine-0154576/

Offshore Energy. (2022, 02 06). Ανάκτηση από https://www.offshore-energy.biz/ports-increasingly-targeted-by-cyberattacks-as-maritime-incidents-surge/

Osler, D. (2022, 09 23). *One ship is hacked every day on average*. Ανάκτηση από Lloyds List: https://lloydslist.maritimeintelligence.informa.com/LL1137457/One-ship-is-hacked-every-day-on-average

Paper: Cyber security by design. (2022, 11 13). Ανάκτηση από DNV GL: https://www.dnv.com/maritime/publications/paper-security-by-design-complex-vessels.html

Patsakis, C., & Chrysanthou, A. (2022, 12 07). *Analysing the fall 2020 Emotet campaign*. Ανάκτηση από arxiv: https://arxiv.org/pdf/2011.06479.pdf

Pavur, J., Moser, D., Strohmeier, M., Lenders, V., & Martinovic, I. (2022, 07 10). *A Tale of Sea and Sky On the Security of Maritime VSAT Communications*. Ανάκτηση από IEEE Xplore: https://ieeexplore.ieee.org/document/9152624

preveil. (2021, 05 02). Ανάκτηση από https://www.preveil.com/blog/public-and-private-key/

Prinston, P. (2022, 11 30). *Top 4 Trending Technologies in the Maritime Industry*. Ανάκτηση από SeaRates: https://www.searates.com/gr/blog/post/it-technologies-in-the-marine-industry

propeller. (2022, 06 18). Ανάκτηση από https://www.propelleraero.com/blog/satellite-navigation-systems-the-difference-between-gnss-and-gps/

PURPLESEC. (2021, 04 28). Ανάκτηση από https://purplesec.us/prevent-cyber-attacks/

RayMarine. (2022, 05 07). Ανάκτηση από https://www.raymarine.com/uploadedFiles/Blog/Raymarine_Blog/AutomaticIdentificationSystem.pdf

Reasearch Gate. (2022, 05 21). Ανάκτηση από https://www.researchgate.net/figure/Satellite-based-AIS-architecture_fig1_274545049

Reports, M. (2022, 09 22). *Real Life Accident: Officer Of The Watch Ignores Lookout's Warning, Ship Collides with Sailboat*. Ανάκτηση από Marine Insight: https://www.marineinsight.com/case-studies/officer-of-the-watch-ignores-lookouts-warning-ship-collides-with-sailboat/

Republic Of The Marshall Islands - Maritime Cyber Risk Management Resources. (2021, 05 02). Ανάκτηση από https://www.register-iri.com/wp-content/uploads/SS-200-Maritime-Cyber-Risk-Management-Resources.pdf

Resilient Navigation and Timing Foundation. (2022, 02 06). Ανάκτηση από https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-ihs-fairplay/

RESOLUTION MSC.252(83). (2022, 05 01). Ανάκτηση από https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.252(83).pdf

Resolution Msc.428(98) - Maritime Cyber Risk Management In Safety Management Systems. (2021, 04 30). Ανάκτηση από https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

Risk Assessment. (2022, 10 08). Ανάκτηση από Canadian Centre for Occupational Health & Safety: https://www.ccohs.ca/oshanswers/hsprograms/risk_assessment.html

Roberts, F. S., Egan, D., Nelson, C., Whytlaw, R., Center, C., & University, R. (2022, 08 19). *Combined Cyber and Physical Attacks on the Maritime Transportation System*. Ανάκτηση από NATO MARITIME INTERDICTION OPERATIONAL TRAINING CENTRE: https://nmiotc.nato.int/wp-content/uploads/2019/10/NMIOTC-18-2019-A-Internet.pdf

Robinson, E. (2022, 09 21). *Hacked – a real life story of exploiting vessel VSAT*. Ανάκτηση από Smart Maritime Network: https://smartmaritimenetwork.com/2020/05/25/hacked-a-real-life-story-of-exploiting-vessel-vsat/

Robinson, E. (2022, 09 21). *We hacked a ship. The owner is liable.* Ανάκτηση από Digital Ship: https://thedigitalship.com/news/maritime-satellite-communications/item/6597-we-hacked-a-ship-the-owner-is-liable

Rules on Cyber Security for the Classification of Marine Units. (2022, 11 13). Ανάκτηση από Bureau Veritas: https://erules.veristar.com/dy/data/bv/pdf/659-NR_2020-09.pdf

Rundle, J. (2022, 08 13). *Coast Guard Details February Cyberattack on Ship*. Ανάκτηση από The Wall Street Journal: https://www.wsj.com/articles/coast-guard-details-february-cyberattack-on-ship-11564133401

S.Žuškin, D. S. (2022, 07 10). *ECDIS Possibilities for BWE Adoption*. Ανάκτηση από Research Gate: https://www.researchgate.net/figure/ECDIS-system-architecture-with-BWE-application_fig1_320325392

Safety4Sea. (2018, December). σ. 37.

safety4sea. (2022, 06 13). Ανάκτηση από https://safety4sea.com/iran-seizes-british-flagged-oil-tanker-in-strait-of-hormuz/

Safety4Sea. (2022, 02 06). Ανάκτηση από https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/

Safety4Sea, T. e. (2022, 11 14). *10 steps to maritime cyber security*. Ανάκτηση από Safety4Sea: https://safety4sea.com/10-steps-to-maritime-cyber-security/

Safety4Sea, T. e. (2022, 09 24). *Easy hacking on the AIS system puts global shipping at risk*. Ανάκτηση από Safety4Sea: https://safety4sea.com/easy-hacking-on-the-ais-system-puts-global-shipping-at-risk/

Safety4Sea, T. e. (2022, 09 24). *Holland America, Princess report cyber security breach*. Ανάκτηση από Safety4Sea: https://safety4sea.com/holland-america-princess-report-cyber-security-breach/

Safety4Sea, T. E. (2022, 11 14). *How to handle data breaching*. Ανάκτηση από Safety4Sea: https://safety4sea.com/how-to-handle-data-breaching/

Safety4Sea, T. E. (2022, 11 14). *How to identify phishing emails*. Ανάκτηση από Safety4Sea: https://safety4sea.com/how-to-identify-phishing-emails/

Safety4Sea, T. E. (2022, 11 16). *INMARSAT: Cyber Risk Management after IMO 2021*. Ανάκτηση από Safety4Sea: https://safety4sea.com/inmarsat-cyber-risk-management-after-imo-2021/

Safety4Sea, T. e. (2022, 09 24). *Two Iranians behind Port of San Diego cyber attack*. Ανάκτηση από Safety4Sea: https://safety4sea.com/two-iranians-behind-port-of-san-diego-cyber-attack/

Safety4Sea, T. e. (2022, 09 24). *US MARAD: GPS interference incidents reported in the eastern Mediterranean Sea*. Ανάκτηση από Safety4Sea: https://safety4sea.com/us-marad-gps-interference-incidents-reported-in-the-eastern-mediterranean-sea/

Safety4Sea, T. E. (2022, 09 24). *Vessel loses control, causes triple collision and crane crash*. Ανάκτηση από Safety4Sea: https://safety4sea.com/vessel-loses-control-causes-triple-collision-and-crane-crash/

Santamarta, R. (2022, 05 02). *IOActive*. Ανάκτηση από https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/

Sea News. (2020, 07 18). Ανάκτηση από https://seanews.co.uk/shipping/information-technology-and-modern-communication-in-shipping/

Sea Rates. (2022, 05 01). Ανάκτηση από https://www.searates.com/gr/blog/post/5-examples-of-information-technology-and-modern-communication-in-shipping

Semantic Scholar. (2022, 04 22). Ανάκτηση από https://www.semanticscholar.org/paper/A-systems-approach-to-governance-in-Maritime-System-Mansouri-Gorod/fd37bc4bfa3f6a25d5764be217391181b4c695cb

ShipOwners. (2021, 04 30). Ανάκτηση από https://www.shipownersclub.com/media/2019/01/TMSA-3-Cyber-Security-On-board-ships-1217.pdf

Silgado, D. M. (2022, 09 23). *Cyber-attacks: a digital threat reality affecting the maritime* . Ανάκτηση από World Maritime University: https://commons.wmu.se/cgi/viewcontent.cgi?article=1662&context=all_dissertations

sucuri. (2021, 05 03). Ανάκτηση από https://docs.sucuri.net/definitions/attacks/brute-force/password-guessing-brute-force-attacks/

Swanagan, M., CISSP, CISA, & CISM. (2022, 11 14). *How To Prevent Cyber Attacks*. Ανάκτηση από PurpleSec: https://purplesec.us/resources/prevent-cyber-attacks/#Prevent

Swanagan, M., CISSP, CISA, & CISM. (2022, 11 14). *How To Prevent Network Attacks + (19 Types Of Attacks Explained)*. Ανάκτηση από PurpleSec: https://purplesec.us/resources/prevent-cyber-attacks/network/

Swanagan, M., CISSP, CISA, & CISM. (2022, 11 14). *How To Prevent Wireless Attacks + (15 Types Of Attacks Explained)*. Ανάκτηση από PurpleSec: https://purplesec.us/resources/prevent-cyber-attacks/wireless/#Packet

Swanbeck, S. (2022, 09 23). *Coast Guard Commandant Addresses Cybersecurity Vulnerabilities on Offshore Oil Rigs*. Ανάκτηση από CSIS: https://www.csis.org/blogs/strategic-technologies-blog/coast-guard-commandant-addresses-cybersecurity-vulnerabilities

Team, G. (2022, 06 18). *What is GPS?* Ανάκτηση από Geotab: https://www.geotab.com/blog/what-is-gps/

Tests Show Ease of Hacking ECDIS, Radar and Machinery. (2022, 08 03). Ανάκτηση από THE MARITIME EXECUTIVE: https://maritime-executive.com/article/tests-show-ease-of-hacking-ecdis-radar-and-machinery

the capacity group. (2021, 04 28). Ανάκτηση από https://capcoverage.com/index.php/10-ways-to-prevent-cyber-attacks/

The Guidelines On Cyber Security Onboard Ships. (2021, 04 30). Ανάκτηση από https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ANNEX%20Guidelines%20on%20Cyber%20Security%20Onboard%20Ships%20v.4.pdf

The Hindu. (2022, 05 02). Ανάκτηση από https://www.thehindu.com/news/national/tamil-nadu/voyage-data-recorder-of-prabhu-daya-may-have-been-tampered-with/article2982183.ece

The News. (2022, 06 18). Ανάκτηση από https://www.portsmouth.co.uk/news/defence/gps-data-showing-navy-warship-charging-at-russian-naval-base-was-fake-says-mod-3287074

The times of India. (2022, 05 02). Ανάκτηση από https://timesofindia.indiatimes.com/city/chennai/lost-voice-data-recorder-may-cost-india-italian-marines-case/articleshow/18942389.cms

The University of Texas. (2020, 08 29). Ανάκτηση από https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/

The Windows Club. (2021, 04 18). Ανάκτηση από https://www.thewindowsclub.com/cyber-attacks-definition-types-prevention

Threat Post. (2022, 02 05). Ανάκτηση από https://threatpost.com/hacker-capsize-ship-sea/142077/

tictac laboratories. (2021, 04 18). Ανάκτηση από https://tictac.gr/cyber-security-ti-einai/

UNEDIFACT. (2022, 08 09). Ανάκτηση από Unece: https://unece.org/trade/uncefact/introducing-unedifact

upguard. (2021, 04 18). Ανάκτηση από https://www.upguard.com/blog/cyber-threat

USA issues a Cybersecurity Alert. (2022, 10 06). Ανάκτηση από Marine Regulations: https://www.marineregulations.news/usa-issues-a-cybersecurity-alert/

USNI news. (2022, 06 18). Ανάκτηση από https://news.usni.org/2021/06/21/positions-of-two-nato-ships-were-falsified-near-russian-black-sea-naval-base

VERMAS. (2022, 08 09). Ανάκτηση από RBS: https://rbs-tops.com/glossary/vermas/

vmware. (2021, 04 24). Ανάκτηση από https://www.vmware.com/topics/glossary/content/cyber-espionage

Voytenko, M. (2022, 09 23). *Cargo ship with containers capsized at Iskenderun port*. Ανάκτηση από FleetMon: https://www.fleetmon.com/maritime-news/2022/39569/cargo-ship-containers-capsized-iskenderun-port-vid/

Wagner, E., Lundh, M., & Grundevik, P. (2022, 08 17). *Engine Control Rooms - Human Factors* . Ανάκτηση από Chalmers: https://research.chalmers.se/publication/167457/file/167457_Fulltext.pdf

Walton, R. (2022, 09 24). *Sophisticated hackers could crash the US power grid, but money, not sabotage, is their focus*. Ανάκτηση από Utility Dive: https://www.utilitydive.com/news/sophisticated-hackers-could-crash-the-us-power-grid-but-money-not-sabotag/603764/

What is Shodan? (2022, 11 26). Ανάκτηση από Shodan: https://help.shodan.io/the-basics/what-is-shodan

White Hat Security. (2021, 04 24). Ανάκτηση από https://www.whitehatsec.com/glossary/content/information-leakage

Wikipedia. (2020, 07 18). Ανάκτηση από https://el.wikipedia.org/wiki/Χωρητικότητα_πλοίου

Wikipedia. (2020, 07 18). Ανάκτηση από https://en.wikipedia.org/wiki/Maritime_call_sign

Wikipedia. (2020, 07 18). Ανάκτηση από https://en.wikipedia.org/wiki/Maritime_Mobile_Service_Identity

Wikipedia. (2020, 07 18). Ανάκτηση από https://en.wikipedia.org/wiki/X_band#Radar

Wikipedia. (2020, 08 29). Ανάκτηση από https://el.wikipedia.org/wiki/Jamming

Wikipedia. (2020, 08 29). Ανάκτηση από https://el.wikipedia.org/wiki/Spoofing

Wikipedia. (2020, 08 28). Ανάκτηση από https://el.wikipedia.org/wiki/Global_System_for_Mobile_Communications

Wikipedia. (2020, 08 28). Ανάκτηση από https://en.wikipedia.org/wiki/NMEA_2000

wikipedia. (2021, 04 20). Ανάκτηση από https://en.wikipedia.org/wiki/Browser_exploit

wikipedia. (2021, 04 20). Ανάκτηση από https://en.wikipedia.org/wiki/Drive-by_download

wikipedia. (2021, 04 20). Ανάκτηση από https://en.wikipedia.org/wiki/Watering_hole_attack

wikipedia. (2021, 04 20). Ανάκτηση από https://en.wikipedia.org/wiki/Email_spam

wikipedia. (2021, 05 02). Ανάκτηση από https://en.wikipedia.org/wiki/IHS_Markit

wikipedia. (2021, 05 02). Ανάκτηση από https://en.wikipedia.org/wiki/MAC_address

wikipedia. (2021, 05 02). Ανάκτηση από https://en.wikipedia.org/wiki/Internet_Protocol

wikipedia. (2021, 05 02). Ανάκτηση από https://el.wikipedia.org/wiki/Packet_sniffer

wikipedia. (2021, 05 02). Ανάκτηση από https://en.wikipedia.org/wiki/Domain_Name_System

wikipedia. (2021, 05 02). Ανάκτηση από https://en.wikipedia.org/wiki/HTTPS

wikipedia. (2021, 05 02). Ανάκτηση από https://en.wikipedia.org/wiki/Unicode

wikipedia. (2021, 05 02). Ανάκτηση από https://en.wikipedia.org/wiki/Certificate_authority

Wikipedia. (2021, 02 14). Ανάκτηση από https://el.wikipedia.org/wiki/Κυβερνοχώρος

Wikipedia. (2021, 04 18). Ανάκτηση από https://en.wikipedia.org/wiki/Cyberattack#cite_note-2

wikipedia. (2022, 04 22). Ανάκτηση από https://en.wikipedia.org/wiki/SOLAS_Convention

Wikipedia. (2022, 02 03). Ανάκτηση από https://el.wikipedia.org/wiki/IPTV

Wikipedia. (2022, 05 15). Ανάκτηση από https://en.wikipedia.org/wiki/Navigational_aid

Wilhoit, M. B. (2022, 05 07). *n0secure - A security evaluation of AIS*. Ανάκτηση από https://www.n0secure.org/wp-content/uploads/2016/06/wp-a-security-evaluation-of-ais.pdf

Wingrove, M. (2022, 07 24). *'Impregnable' radar breached in simulated cyber attack*. Ανάκτηση από Riviera: https://www.rivieramm.com/news-content-hub/news-content-hub/impregnable-radar-breached-in-simulated-cyber-attack-25158

Wingrove, M. (2022, 10 23). *ACCIDENT REPORT: Ship damaged due to incorrect ECDIS use*. Ανάκτηση από Riviera: https://www.rivieramm.com/news-content-hub/news-content-hub/accident-report-ship-damaged-due-to-incorrect-ecdis-use-26796

Wingrove, M. (2022, 11 16). *Compliance does not equal security or effective risk management*. Ανάκτηση από Riviera: https://www.rivieramm.com/news-content-hub/news-content-hub/compliance-does-not-equal-security-or-effective-risk-management-60830

Wingrove, M. (2022, 10 09). *Go beyond compliance for cyber security*. Ανάκτηση από Riviera: https://www.rivieramm.com/opinion/go-beyond-compliance-for-cyber-security-72098

Wingrove, M. (2022, 10 09). *How to harden maritime IT and OT*. Ανάκτηση από Riviera: https://www.rivieramm.com/news-content-hub/how-to-harden-maritime-it-and-ot-70469

Wingrove, M. (2022, 10 09). *Using intelligence to mitigate cyber risks*. Ανάκτηση από Riviera: https://www.rivieramm.com/news-content-hub/use-intelligence-for-cyber-risk-mitigation-70454

Zero-day (0day) exploit. (2022, 10 09). Ανάκτηση από Imperva: https://www.imperva.com/learn/application-security/zero-day-exploit/

Zorz, Z. (2022, 09 21). *Critical flaws in maritime comms system could endanger entire ships*. Ανάκτηση από Help Net Security: https://www.helpnetsecurity.com/2017/10/26/critical-flaws-maritime-comms-system/

Zorz, Z. (2022, 09 21). *The dismal state of SATCOM security*. Ανάκτηση από Help Net Security: https://www.helpnetsecurity.com/2014/04/17/the-dismal-state-of-satcom-security/

ΑΔΑΕ. (2022, 05 02). Ανάκτηση από http://www.adae.gr/i-adae/paroysiasi/

Αρχή Προστατίας Δεδομένων. (2022, 05 02). Ανάκτηση από https://www.dpa.gr/

ΕΕΤΤ. (2022, 05 02). Ανάκτηση από https://www.eett.gr/opencms/opencms/EETT/EETT/AboutEETT/

Ελληνική Αστυνομία. (2022, 05 02). Ανάκτηση από http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194&Itemid=378&lang

Ελληνική Δημοκρατία - Υπουργείο Ψηφιακής Διακυβέρνησης. (2022, 05 02). Ανάκτηση από https://mindigital.gr/wp-content/uploads/2020/12/Εθνική-Στρατηγική-Κυβερνοασφάλειας.pdf

Ελληνική Δημοκρατία. (2022, 05 02). Ανάκτηση από https://mindigital.gr/kyvernoasfaleia

Ευρωπαϊκό Συμβούλιο. (2021, 04 29). Ανάκτηση από https://www.consilium.europa.eu/el/policies/cybersecurity/

Η χρήση και η αξιοποίηση του Διαδικτύου και των εφαρμογών του στη σύγχρονη Εμπορική Ναυτιλία. (2017). Στο Σ. Α. Μανομενίδου Χριστίνα. ΝΕΑ ΜΗΧΑΝΙΩΝΑ.

IMO. (2022, 05 07). Ανάκτηση από https://www.imo.org/en/OurWork/Safety/Pages/AIS.aspx

KEMEA. (2022, 05 02). Ανάκτηση από http://www.kemea.gr/el/to-kemea/sxetika-me-to-kemea

Παπανικολάου, Α. Δ. (2009). Μελέτη Πλοίου - Μεθοδολογίες Προμελέτης Τεύχος 1. Αθήνα: Εκδόσεις Συμεών.

Σπανός, Σ. (2022, 11 23). *Κυβερνοασφάλεια στη Ναυτιλία : Συγκριτική μελέτη*. Ανάκτηση από ISONIKE: https://isonike.com/?q=node/120

TrustNet. (2021, 04 20). Ανάκτηση από https://www.trustnetinc.com/web-application-attacks/